



配置和管理 OnCommand Insight

NetApp
April 01, 2024

目录

配置和管理	1
设置Insight	1
Insight安全性	86
支持智能卡和证书登录	99
为智能卡和证书登录配置数据仓库	110
为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.5至7.3.9)	111
为智能卡和证书登录配置Cognos (OnCommand Insight 7.3.10及更高版本)	112
导入Cognos和DWH的CA签名SSL证书(Insight 7.3.5至7.3.9)	114
导入Cognos和DWH的CA签名SSL证书(Insight 7.3.10及更高版本)	116
导入SSL证书	118
业务实体层次结构	120
定义标注	123
正在查询资产	136
Insight数据源管理	143
设备解析	237
维护Insight	254
监控您的环境	275

配置和管理

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：

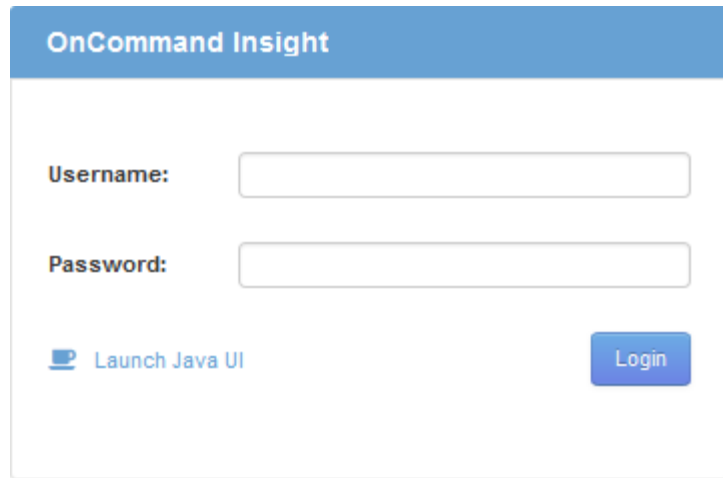
- 在Insight服务器上打开Insight：

`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。

The image shows a login dialog box for OnCommand Insight. It has a blue header bar with the text "OnCommand Insight". Below the header, there are two input fields: "Username:" and "Password:". Below the password field, there is a link that says "Launch Java UI" with a small icon of a laptop. To the right of the "Launch Java UI" link is a blue button labeled "Login".

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登录名将为用户DOMAIN\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。

LDAP

LDAP integration enables authentication of users via LDAP (or ActiveDirectory). This is done by assigning these users to LDAP groups. The groups are used to identify the user permissions.

☒ Enable LDAP

Please provide credentials for a user authorized for directory lookup queries.

LDAP servers:

User:

Password:

[Show more](#) ▼

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。

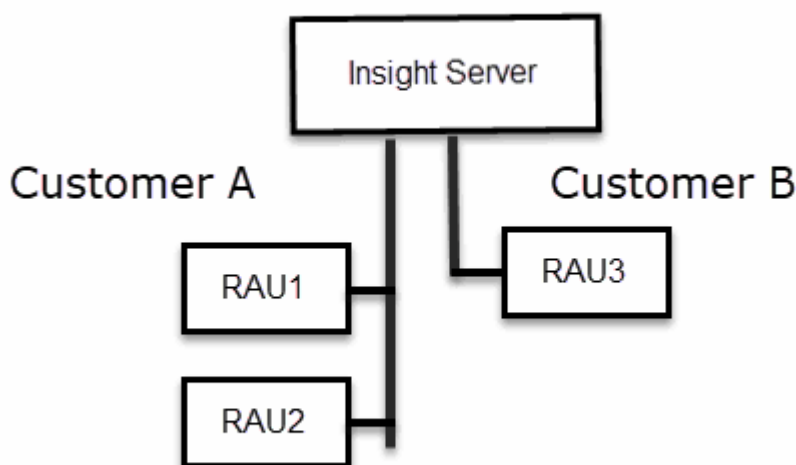
升级和安装注意事项

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SMTP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服务器配置的数据仓库 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。

Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="••••••••"/>
Advanced ▼	
<input type="button" value="Save"/>	<input type="button" value="Cancel"/>
<input type="button" value="Test"/>	<input type="button" value="Remove"/>

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。

Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="....."/>
Server user name:	<input type="text" value="dwh_internal"/>
Server password:	<input type="password" value="....."/>
HTTPS port:	<input type="text" value="443"/>
TCP port:	<input type="text" value="3306"/>

Basic ^

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。

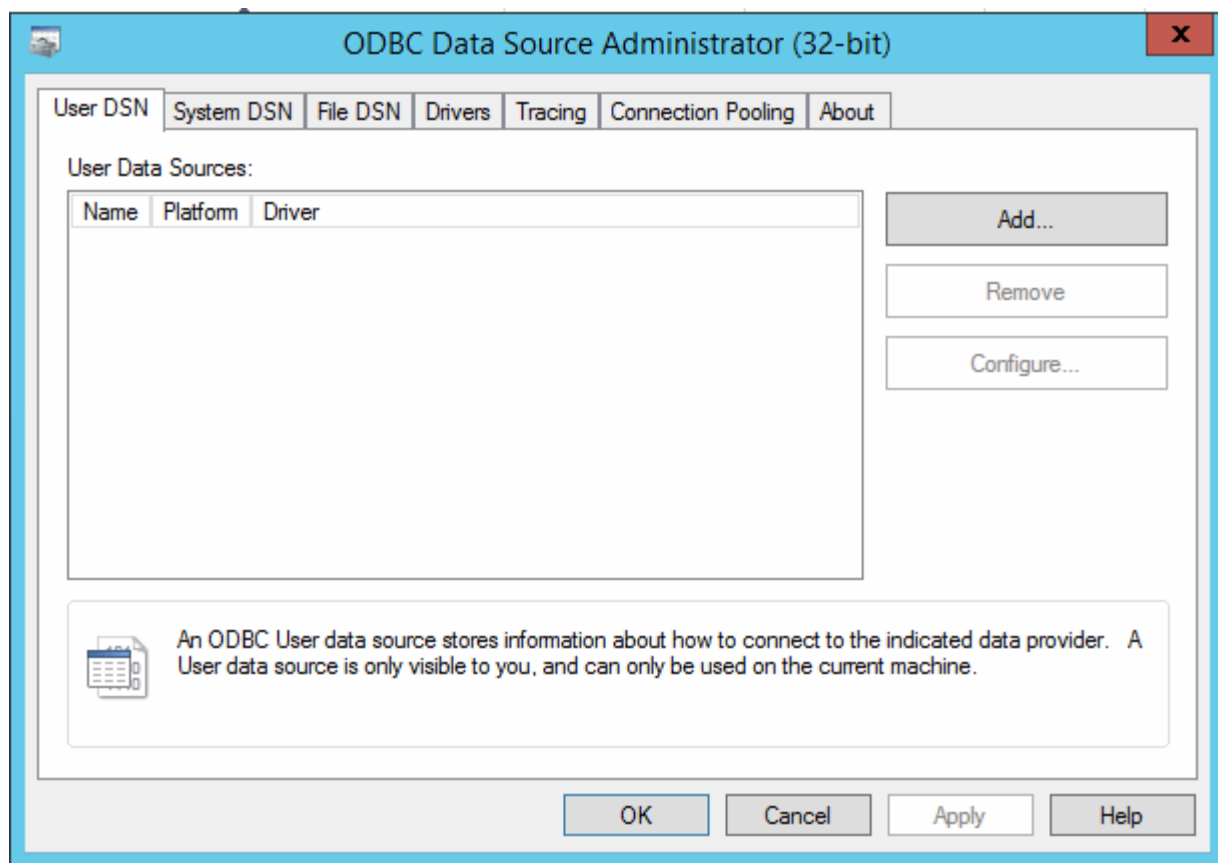
开始之前

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

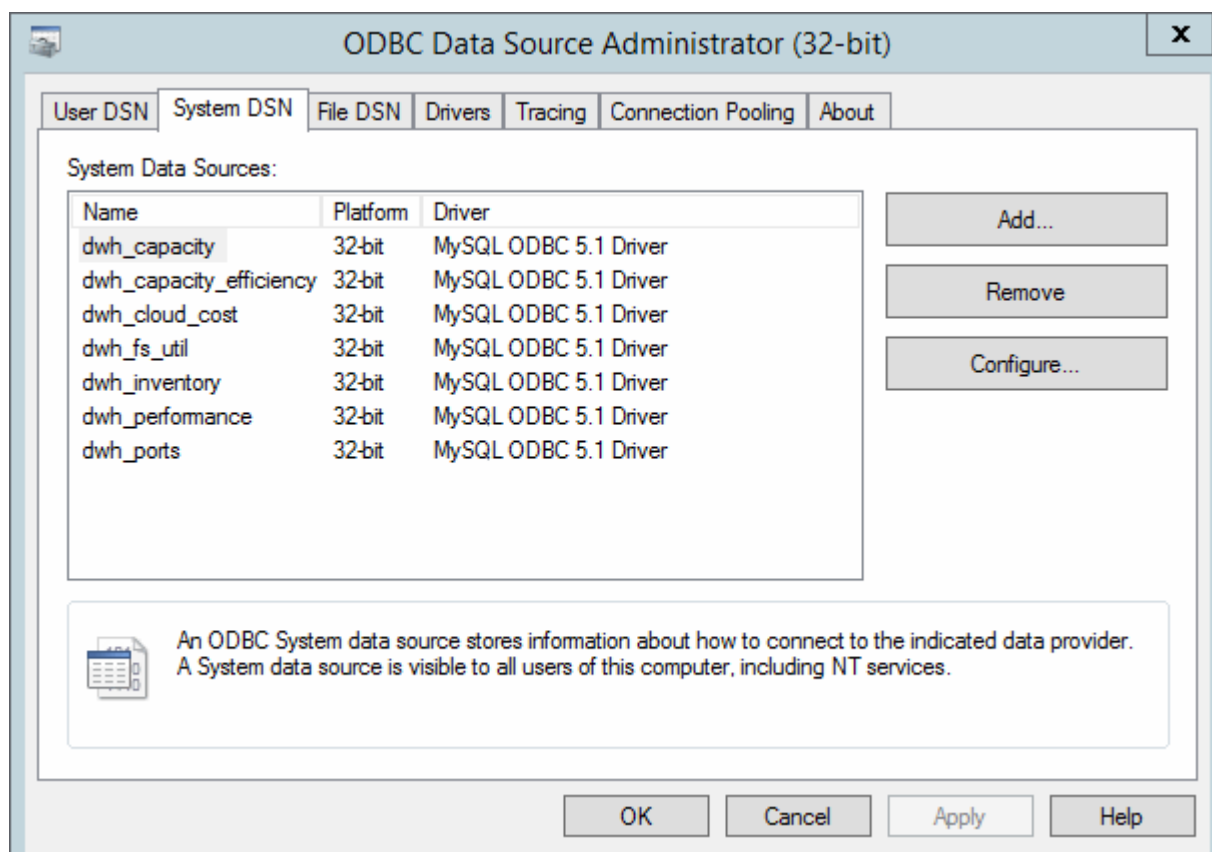
1. 远程登录到托管该数据仓库的服务器。
2. 访问ODBC管理工具、网址为 C:\Windows\SysWOW64\odbcad32.exe

系统将显示"ODBC数据源管理员"屏幕。



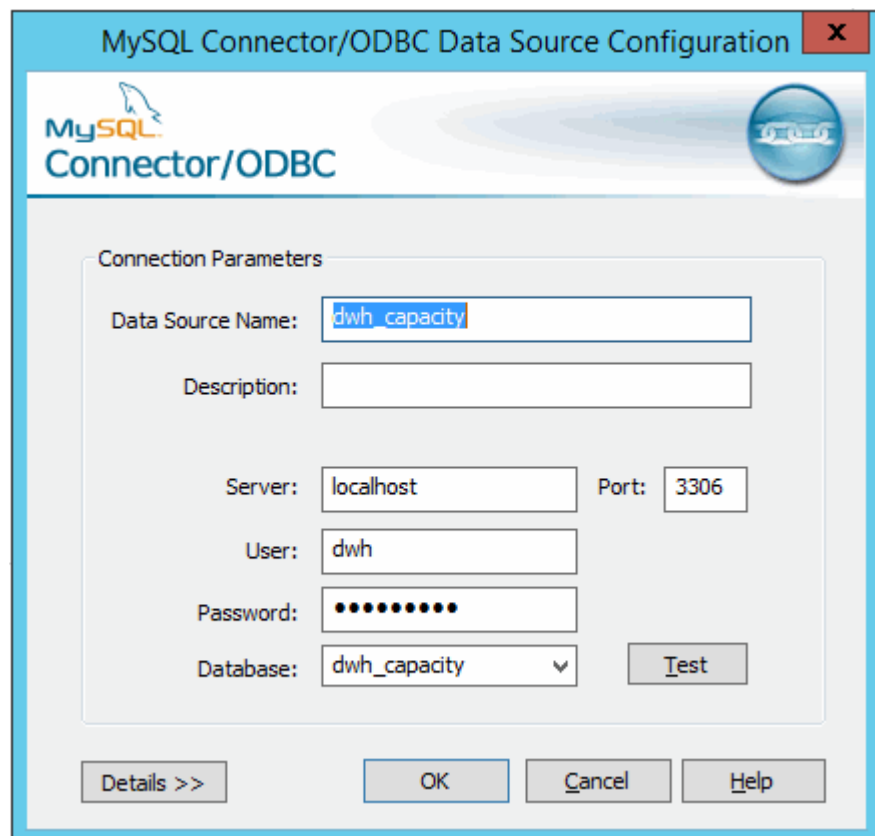
3. 单击*系统DSN*

此时将显示系统数据源。



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

此时将显示Data Source Configuration屏幕。



The image shows the 'MySQL Connector/ODBC Data Source Configuration' dialog box. It has a title bar with the MySQL logo and a close button. The main area is titled 'Connection Parameters' and contains several input fields: 'Data Source Name' (containing 'dwh_capacity'), 'Description' (empty), 'Server' (containing 'localhost'), 'Port' (containing '3306'), 'User' (containing 'dwh'), 'Password' (masked with dots), and 'Database' (a dropdown menu showing 'dwh_capacity'). There is a 'Test' button next to the Database dropdown. At the bottom, there are buttons for 'Details >>', 'OK', 'Cancel', and 'Help'.

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、为用户提供了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OnCommand 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OnCommand 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OnCommand 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OnCommand 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OnCommand 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。

- 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
- 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 当系统提示您输入密码时、输入 `NoPassWordSet`。

- 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OnCommand 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。

- 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
- 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 当系统提示您输入密码时、输入 `NoPassWordSet`。
- 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:

- 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OnCommmand 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OnCommand 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.truststore -storepass changeit -alias cognos3rdca`

15. 重新启动SANSscreen 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SANSscreen 证书或无法创建DWH备份。

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

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

c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.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OnCommand 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\SANSscreen 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OnCommand 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OnCommand 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。

- 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。
- 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
- 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 当系统提示您输入密码时、输入 `NoPassWordSet`。
- 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:

- 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。
- 执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
- 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:

- 执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
- 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OnCommand 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OnCommand 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 ..\SANSscreen\cognos\analytics\configuration\cogstartup.xml。
2. 在下创建"certs"和"csk"文件夹的备份 ..\ SANSscreen\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\sansscreen\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"-storepasschangeit -alias cognoscrt

14. 重新启动SANSscreen 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 ..\SANSscreen\cognos\analytics\configuration 和 ..\SANSscreen\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\sansscreen\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.trustore -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 "%SANSSCREEN_HOME%cognos\analytics\bin\"`
- b. `"%SANSSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sansscreen.cer" -keystore "%SANSSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
- c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.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

如果要將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  Add 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 。如果可以为选定资产类型分配业务实体、您将看到菜单项*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  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`System-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`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  以添加其他级别。
6. 完成后、单击*保存*。

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 。

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  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 .

此时将显示添加标注对话框。

4. 单击*标注*、然后从列表选择一个标注。
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 .
- 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 。

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 [-username] [-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*并选择您在上面对添加的标注变量。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。

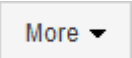
为查询选择资源时、系统会自动显示多个默认列；您可以随时删除这些列或添加新列。


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 、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。

- 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。

- 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 、然后从列表选择一个条件。
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 、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  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 、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 、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。

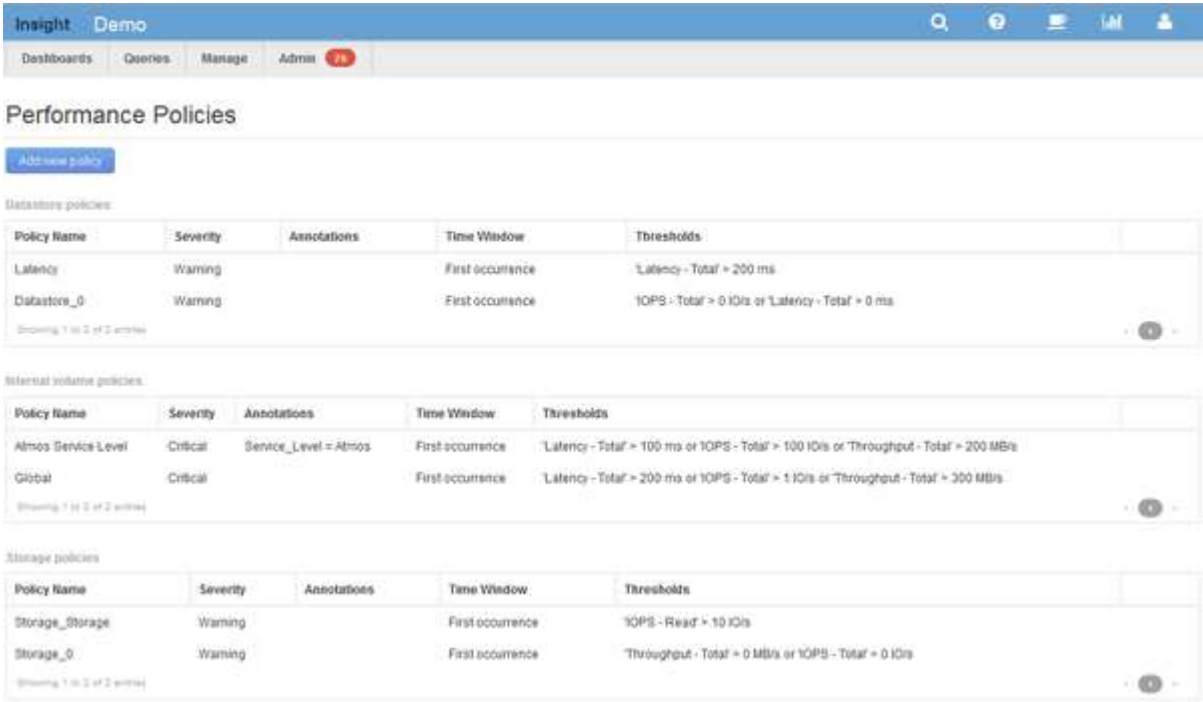
创建性能策略

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。

+

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。

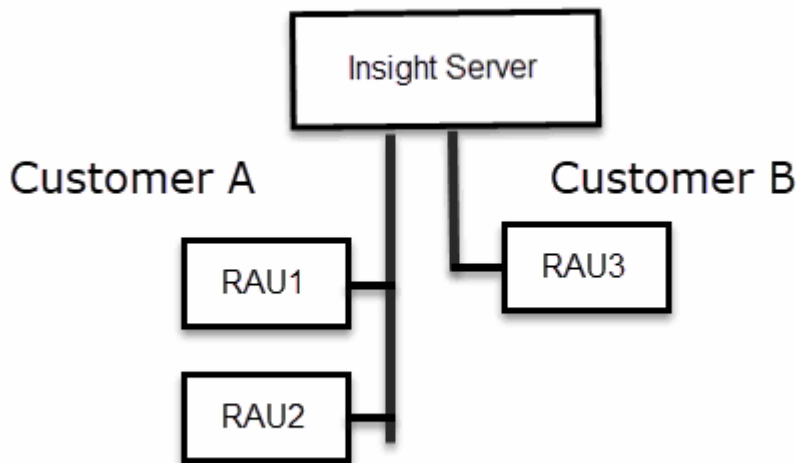
升级和安装注意事项

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SMTP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。

Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="••••••••"/>

Advanced 

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。

Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="....."/>
Server user name:	<input type="text" value="dwh_internal"/>
Server password:	<input type="password" value="....."/>
HTTPS port:	<input type="text" value="443"/>
TCP port:	<input type="text" value="3306"/>

Basic ^

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。

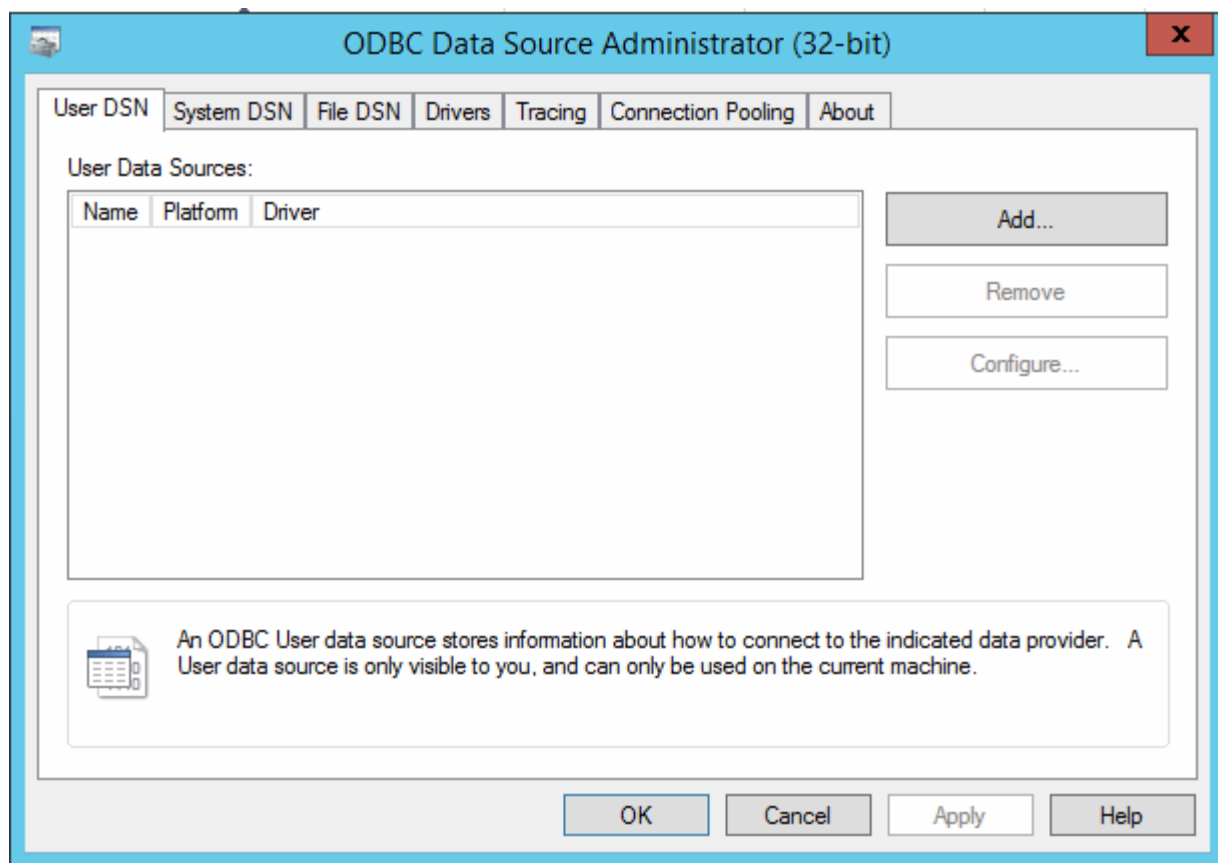
开始之前

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

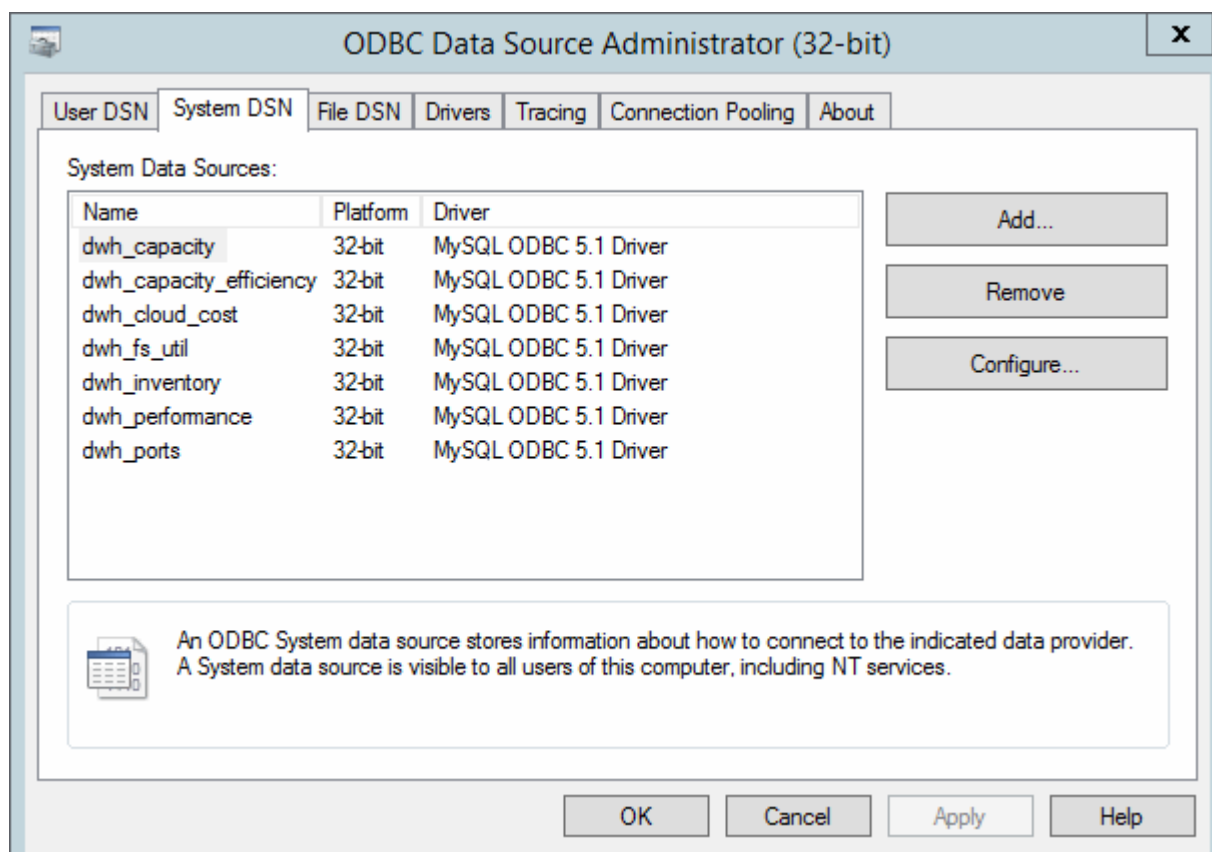
1. 远程登录到托管该数据仓库的服务器。
2. 访问ODBC管理工具、网址为 C:\Windows\SysWOW64\odbcad32.exe

系统将显示"ODBC数据源管理员"屏幕。



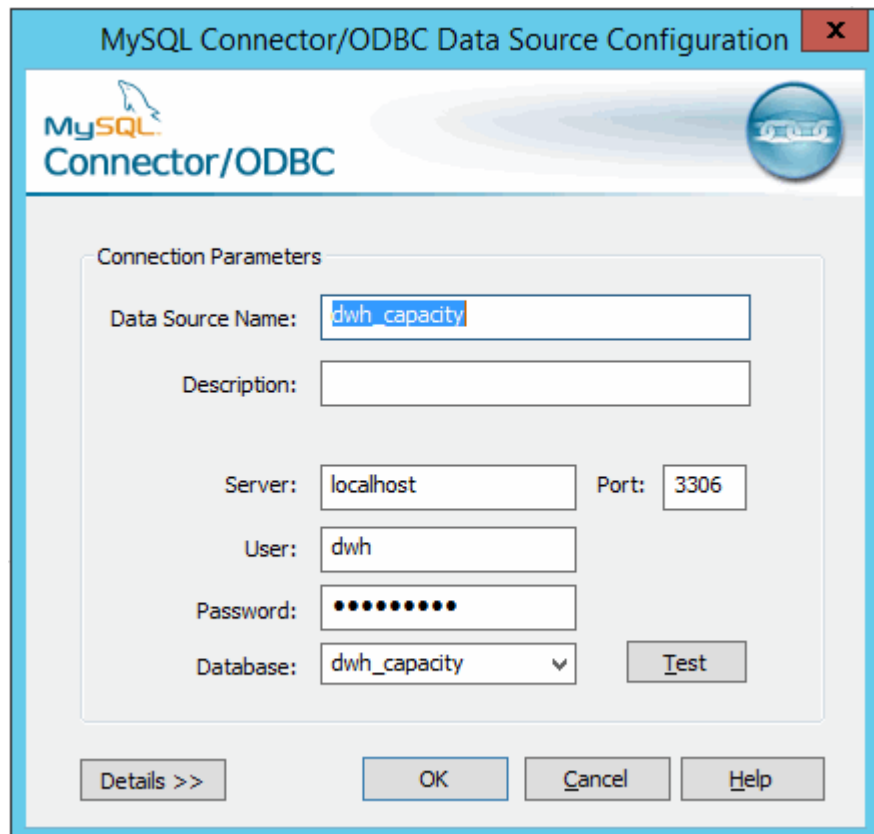
3. 单击*系统DSN*

此时将显示系统数据源。



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

此时将显示Data Source Configuration屏幕。



The image shows the 'MySQL Connector/ODBC Data Source Configuration' dialog box. It has a title bar with the MySQL logo and a close button. The main area is titled 'Connection Parameters' and contains several input fields: 'Data Source Name' (set to 'dwh_capacity'), 'Description' (empty), 'Server' (set to 'localhost'), 'Port' (set to '3306'), 'User' (set to 'dwh'), 'Password' (masked with dots), and 'Database' (set to 'dwh_capacity' with a dropdown arrow). There is a 'Test' button next to the Database field. At the bottom, there are buttons for 'Details >>', 'OK', 'Cancel', and 'Help'.

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、为用户提供了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OnCommand 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OnCommand 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OnCommand 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OnCommand 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OnCommand 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。

- 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
- 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 当系统提示您输入密码时、输入 `NoPassWordSet`。
- 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OnCommand 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。

- 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。
- 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
- 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 当系统提示您输入密码时、输入 `NoPassWordSet`。
- 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:

- 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OnCommmand 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\sansscreen\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\sansscreen\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.truststore -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 "%SANSSCREEN_HOME%cognos\analytics\bin\"

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

c. ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.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OnCommand 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OnCommand 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。

- 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
- 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 当系统提示您输入密码时、输入 `NoPassWordSet`。
- 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OnCommand 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。

- 在命令窗口中、转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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`
- 如果不存在合适的文件、请提供CA证书文件、通常为 `.pem` 文件
- 要将客户的CA与OnCommand Insight 可信CA结合使用、请转至 `..\SANscreen\cognos\analytics\configuration\certs\`
- 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。

- 当系统提示您输入密码时、输入 `NoPassWordSet`。
- 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:

- 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。
- 执行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
- 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:

- 执行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
- 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OnCommand 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OnCommand 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 ..\SANSscreen\cognos\analytics\configuration\cogstartup.xml。
2. 在下创建"certs"和"csk"文件夹的备份 ..\ SANSscreen\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\sansscreen\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OnCommand 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.trustore -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\sansscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
- c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.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。

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  Add 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 。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  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`System-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`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  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 。

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  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 。

此时将显示添加标注对话框。

4. 单击*标注*、然后从列表选择一个标注。
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 。
- 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 [-username] [-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 、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.

+


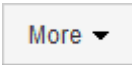
修改查询

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 、然后从列表选择一个条件。
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 、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  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 、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 、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。

Insight数据源管理

数据源是用于维护OnCommand Insight 环境的最关键的组件。由于它们是Insight的主要信息源、因此您必须保持数据源处于运行状态。

您可以通过选择一个数据源来检查与其状态相关的事件并注意可能导致问题的任何更改来监控网络中的数据源。

除了检查单个数据源之外、您还可以执行以下操作:

- 克隆数据源以在Insight中创建许多类似的数据源
- 编辑数据源信息
- 更改凭据
- 控制轮询
- 删除数据源
- 安装数据源修补程序
- 从修补程序安装新的数据源
- 为NetApp客户支持准备错误报告

在Insight中设置数据源

在尝试维护Insight环境时、数据源是最关键的组件。数据源可发现用于分析和验证的网络信息。您需要在Insight中配置数据源、以便可以在网络中对其进行监控。

对于每个数据源、定义该数据源的具体要求取决于相应设备的供应商和型号。在添加数据源之前、您需要所有设备的网络地址、帐户信息和密码、可能还需要以下附加详细信息:

- 交换机
- 设备管理工作站
- 具有IP连接的存储系统
- 存储管理工作站
- 运行管理软件的主机服务器、用于没有IP连接的存储设备

有关数据源定义的详细信息、请参见本节中的"供应商专用数据源参考"信息。

数据源支持信息

在规划配置时、您应确保Insight可以监控环境中的设备。为此、您可以查看数据源支持列表、了解有关操作系统、特定设备和协议的详细信息。某些数据源可能并非在所有操作系

统上都可用。

最新版本的数据源支持列表的位置

OnCommand Insight 数据源支持列表随每个Service Pack版本一起更新。文档的最新版本可在中找到 ["NetApp 支持站点"](#)。。

添加数据源

您可以使用添加数据源对话框快速添加数据源。

步骤

- 1. 在浏览器中打开OnCommand Insight 、然后以具有管理权限的用户身份登录。
- 2. 选择*管理*、然后选择*数据源*。
- 3. 单击*+添加*按钮。

此时将打开添加数据源向导。

- 4. 在*设置*部分中、输入以下信息：

字段	Description
Name	为此数据源输入唯一的网络名称。注意：数据源名称仅允许使用字母、数字和下划线(_)字符。
供应商	从下拉列表中选择数据源的供应商。
型号	从下拉列表中选择数据源的型号。
运行位置	选择本地、或者、如果您的环境中配置了RAU、则可以选择远程采集单元。
要收集的内容	对于大多数数据源、这些选项将为清单和性能。默认情况下、清单始终处于选中状态、不能取消选择。请注意、某些数据源可能具有不同的选项。您选择的收集选项会更改配置和高级配置部分中的可用字段。

- 5. 单击*配置*链接、然后输入选定数据收集类型的数据源所需的基本设置信息。
- 6. 如果此类数据源通常需要更详细的信息才能在网络中进行设置、请单击*高级配置*链接以输入追加信息。
- 7. 有关特定数据源所需或可用的配置或高级配置信息的详细信息、请参见 ["供应商专用数据源参考"](#)。
- 8. 单击*测试*链接以确保已正确配置数据源。
- 9. 单击 * 保存 * 。

您可以从电子表格将多个数据源导入到OnCommand Insight 中。如果您已在电子表格中维护发现设备、则此操作可能会很有用。此过程会添加新的数据源、但不能用于更新现有数据源。

关于此任务

OnCommand Insight 包含一个电子表格、可帮助您创建数据源。此电子表格具有以下属性：

- 该电子表格可用于Microsoft Excel 2003或更高版本。
- 每个选项卡都包含一种数据源类型、例如Brocade SSH/CLI。
- 每行表示要创建的新数据源的一个实例。

该电子表格包含一个宏、用于在OnCommand Insight 中创建新的数据源。

步骤

1. 在中找到电子表格
`<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip。`
2. 在电子表格的彩色单元格中输入数据源信息。
3. 删除空行。
4. 从电子表格中、运行 `CreateDataSources` 用于创建数据源的宏。
5. 当系统提示输入凭据时、输入OnCommand Insight 服务器管理用户名和密码。

结果将记录在采集日志中。

6. 此时将出现一个提示、询问当前运行宏的计算机是否已安装OnCommand Insight。

选择以下选项之一：

- 否：如果要创建必须在OnCommand Insight 计算机上运行的批处理文件、请选择"否"。从安装目录运行此批处理文件。
- 是：如果已安装OnCommand Insight 、并且不需要执行其他步骤来生成数据源信息、请选择"是"。

7. 要验证是否已添加数据源、请在浏览器中打开Insight。
8. 在Insight工具栏上、单击*管理*。
9. 检查"Data sources"列表中是否存在您导入的数据源。

通过修补程序添加新数据源

新数据源将作为修补程序文件发布、可以使用修补程序过程将这些文件加载到系统中。通过此过程、可以在OnCommand Insight 的计划版本之间使用新的数据源。

开始之前

您必须已上传要安装的修补程序文件。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 选择*修补程序*。
3. 选择*操作*>*安装服务包或修补程序*。
4. 在*安装Service Pack或Patch*对话框中、单击*浏览*以查找并选择您上传的修补程序文件。
5. 单击*修补程序摘要*对话框中的*下一步*。
6. 查看*请阅读*信息、然后单击*下一步*继续。
7. 在*安装*对话框中、单击*完成*。

克隆数据源

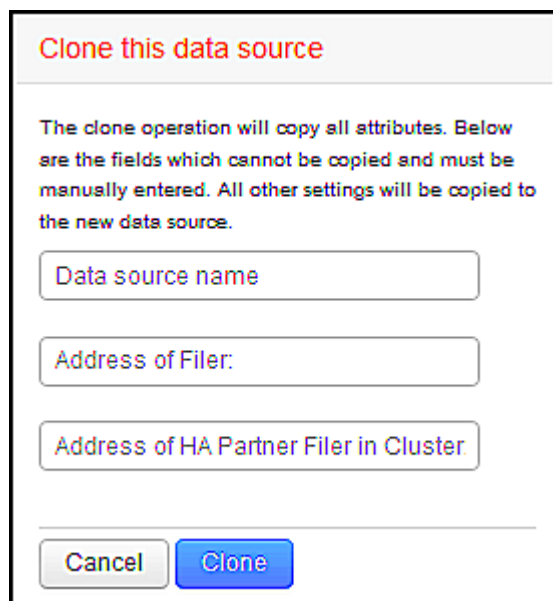
使用克隆工具，您可以快速添加与其他数据源具有相同凭据和属性的数据源。通过克隆，您可以轻松配置同一设备类型的多个实例。

步骤

1. 在Insight工具栏上、单击*管理*。

此时将打开数据源列表。
2. 突出显示包含要用于新数据源的设置信息的数据源。
3. 在突出显示的数据源右侧、单击*克隆*图标。

克隆此数据源对话框列出了必须为选定数据源提供的信息、如以下NetApp数据源示例所示：



Clone this data source

The clone operation will copy all attributes. Below are the fields which cannot be copied and must be manually entered. All other settings will be copied to the new data source.

Data source name

Address of Filer:

Address of HA Partner Filer in Cluster

Cancel Clone

4. 在字段中输入所需信息；这些详细信息无法从现有数据源复制。
5. 单击 * 克隆 *。

结果

克隆操作会复制所有其他属性和设置以创建新的数据源。

测试数据源配置

添加数据源时、您可以在保存或更新该数据源之前验证与设备通信的配置是否正确。

单击数据源向导中的*测试*按钮时、将检查与指定设备的通信。此测试将生成以下结果之一：

- PASSED：已正确配置数据源。
- 警告：测试未完成、可能是由于处理期间超时或采集未运行。
- failed：配置的数据源无法与指定设备通信。检查配置设置并重新测试。

供应商专用数据源参考

配置详细信息因所添加数据源的供应商和型号而异。

如果供应商的数据源需要高级Insight配置说明、例如特殊要求和特定命令、则本节将包含这些信息。

3PAR InServ数据源

OnCommand Insight 使用3PAR InServ (固件2.2.2+、SSH)数据源发现HP 3PAR StoreServ存储阵列的清单。

术语

OnCommand Insight 从3PAR InServ数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
物理磁盘	Disk
存储系统	存储
控制器节点	存储节点
通用配置组	存储池
虚拟卷	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- InServ 集群的 IP 地址或 FQDN
- 对于清单、InServ服务器的只读用户名和密码。
- 为了提高性能、InServ服务器的读写用户名和密码。
- 端口要求：22 (清单收集)、5988或5989 (性能收集)[注意：InServ OS 3.x+支持3PAR性能]
- 对于性能收集，请通过 SSH 登录到 3PAR 阵列来确认 SMI-S 已启用。

Configuration

字段	Description
集群 IP	InServ集群的IP地址或完全限定域名
用户名	InServ服务器的用户名
Password	InServ服务器使用的密码
SMI-S主机IP	SMI-S提供程序主机的IP地址
SMI-S 用户名	SMI-S Provider 主机的用户名
SMI-S 密码	SMI-S Provider 主机使用的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
排除设备	要排除的设备IP的逗号分隔列表
SSH进程等待超时(秒)	SSH进程超时(默认值为60秒)
SSH重试次数	SSH重试尝试次数
SSH横幅等待超时(秒)	SSH横幅等待超时(默认为20秒)
SMI-S端口	SMI-S Provider主机使用的端口
协议	用于连接到 SMI-S 提供程序的协议
SMI-S命名空间	SMI-S命名空间

性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
SMI-S连接重试次数	SMI-S连接重试尝试次数

Amazon AWS EC2数据源

OnCommand Insight 使用此数据源来发现Amazon AWS EC2的清单和性能。

前提条件：

要从 Amazon EC2 设备收集数据，您必须具有以下信息：

- 您必须具有IAM访问密钥ID
- 您必须拥有Amazon EC2云帐户的机密访问密钥
- 您必须具有 " 列表组织 " 权限
- 端口433 HTTPS
- EC2 实例可以报告为虚拟机，也可以报告为主机（不太自然）。EBS 卷既可以报告为虚拟机使用的虚拟磁盘，也可以报告为虚拟磁盘提供容量的数据存储库。

访问密钥由一个访问密钥 ID（例如，AKIIOSFODNN7EXAMPLE）和一个机密访问密钥（例如，wJALRXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY）组成。如果使用Amazon EC2 SDK、REST或查询API操作，则可以使用访问密钥对向EC@发出的编程请求进行签名。这些密钥随 Amazon 的合同一起提供。

如何配置此数据源

要配置Amazon AWS EC2数据源、您需要为AWS帐户提供AWS IAM访问密钥ID和机密访问密钥。

根据下表填写数据源字段：

配置：

字段	Description
AWS 地区	选择 AWS 区域
IAM 角色	仅在 AWS 中的 AU 上采集时使用。有关IAM角色的详细信息、请参见下文。
AWS IAM 访问密钥 ID	输入 AWS IAM 访问密钥 ID 。如果不使用 IAM 角色，则此为必填项。
AWS IAM 机密访问密钥	输入 AWS IAM 机密访问密钥。如果不使用 IAM 角色，则此为必填项。
我了解AWS会为我的API请求付费	选中此复选框可验证您是否了解AWS会为Insight轮询发出的API请求向您收费

高级配置：

字段	Description
包括其他区域	指定要包括在轮询中的其他区域。
跨帐户角色	用于访问不同 AWS 帐户中的资源的角色。
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为60分钟)
HTTP连接和套接字超时(秒)	HTTP连接超时(默认值为300秒)
包括AWS标记	选中此选项可在Insight标注中启用AWS标记支持
性能轮询间隔（秒）	性能轮询之间的时间间隔(默认值为1800秒)

将AWS标记映射到Insight标注

AWS EC2数据源包含一个选项、可用于使用AWS上配置的标记填充Insight标注。标注的名称必须与AWS标记完全相同。Insight将始终填充同名文本类型的标注、并"尽力"填充其他类型(数字、布尔值等)的标注。如果您的标注类型不同、而数据源无法填充、则可能需要删除此标注并将其重新创建为文本类型。

请注意、AWS区分大小写、而Insight不区分大小写。因此、如果您在Insight中创建了名为"owner"的标注、并在AWS中创建了名为"owner"、"owner"和"owner"的标记、则"owner"的所有AWS变体都将映射到Insight的"owner"标注。

相关信息：

"管理IAM用户的访问密钥"

包括其他区域

在 AWS Data Collector * 高级配置 * 部分中，您可以设置 * 包括额外区域 * 字段以包括其他区域，以逗号或分号分隔。默认情况下，此字段设置为 *。*_*，它会在所有美国 AWS 地区收集数据。要在 *all* 地区收集数据，请将此字段设置为 *。*_*。

如果 * 包括额外区域 * 字段为空，则数据收集器将收集在 * 配置 * 部分中指定的 * AWS 区域 * 字段中指定的资产。

从AWS子帐户收集

Insight支持在一个AWS数据收集器中收集AWS的子帐户。此收集的配置在 AWS 环境中执行：

- 您必须将每个子帐户配置为具有一个AWS角色、此角色允许主帐户ID从子帐户访问EC2详细信息。
- 每个子帐户都必须将角色名称配置为相同的字符串
- 在"跨帐户角色"字段的"Insight AWS Data Collector 高级配置"部分中输入此角色名称字符串。

最佳实践：强烈建议将AWS预定义的AmazonEC2ReadOnlyAccess策略分配给ECS主帐户。此外、在数据源中配置的用户应至少分配预定义的_AWSOrganizationsReadOnlyAccess__policy、以便查询AWS。

有关配置环境以允许Insight从AWS子帐户收集数据的信息、请参见以下内容：

"教程：使用 IAM 角色跨 AWS 帐户委派访问"

"AWS 设置：在您拥有的另一个 AWS 帐户中提供对 IAM 用户的访问权限"

"创建角色以将权限委派给 IAM 用户"

IAM 角色

使用IAM role_ security时、您必须确保您创建或指定的角色具有访问资源所需的适当权限。

例如，如果您创建了一个名为 _InstanceEE2ReadOnly" 的 IAM 角色，则必须设置此策略，以便为此 IAM 角色向所有 EC2 资源授予 EC2 只读列表访问权限。此外，您还必须授予 STS （安全令牌服务）访问权限，以便允许此角色跨帐户承担角色。

创建 IAM 角色后，您可以在创建新的 EC2 实例或任何现有 EC2 实例时附加此角色。

将 IAM 角色 _InstanceEE2ReadOnly" 附加到 EC2 实例后，您将能够通过实例元数据按 IAM 角色名称检索临时凭据，并使用它通过在此 EC2 实例上运行的任何应用程序访问 AWS 资源。



仅当采集单元在AWS实例中运行时、才能使用IAM角色。

Brocade Enterprise Fabric Connectivity Manager数据源

OnCommand Insight 使用Brocade Enterprise Fabric Connectivity Manager (EFCM)数据源发现Brocade EFCM交换机的清单。Insight支持EFCM 9.5、9.6和9.7版。

要求



从OnCommand Insight 7.3.11开始、此数据收集器不可用。

- EFCM 服务器的网络地址或完全限定域名
- EFCM 版本必须为 9.5 ， 9.6 或 9.7
- EFCM 服务器的 IP 地址
- EFCM 服务器的只读用户名和密码
- 已通过端口51512使用只读用户名和密码验证通过Telnet从Insight服务器对Connectrix交换机的访问

Configuration

* 字段 *	* 问题描述 *
EFC 服务器	EFC 服务器的 IP 地址或完全限定域名
用户名	交换机的用户名
Password	交换机使用的密码

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为15分钟)
网络结构名称	要由EFCM数据源报告的网络结构名称。留空以将网络结构名称报告为 WWN 。
通信端口	用于与交换机通信的端口
启用陷阱	选择此选项可在从设备收到 SNMP 陷阱时启用采集。如果选择启用陷阱，则还必须激活 SNMP 。
陷阱之间的最短时间（秒）	陷阱触发的两次采集尝试之间的最短时间(默认为15秒)
非活动区域集	除了在活动分区集上执行采集之外，要在其中执行采集的非活动分区集的逗号分隔列表
要使用的 NIC	指定在报告 SAN 设备时应在 RAU 上使用哪个网络接口
排除设备	要包括在轮询中或从轮询中排除的单元名称的逗号分隔列表
使用EFCM交换机别名作为Insight交换机名称	选择以使用EFCM交换机别名作为Insight交换机名称
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

Brocade FC交换机数据源

OnCommand Insight 使用Brocade FC交换机(SSH)数据源发现运行Factored Operating System (FOS)固件4.2及更高版本的Brocade或更名交换机设备的清单。支持 FC 交换机和访问网关模式下的设备。

术语

OnCommand Insight 从Brocade FC交换机数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
交换机	交换机
Port	Port

虚拟网络结构，物理网络结构	网络结构
分区	分区
逻辑交换机	逻辑交换机
LSAN 区域	IVR 区域



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 采集单元(本地或远程)将启动与Brocade交换机上的TCP端口22的连接、以收集清单数据。AU 还将启动与 UDP 端口 161 的连接，以收集性能数据。
- 网络结构中的所有交换机都必须具有 IP 连接。如果选中发现网络结构中的所有交换机复选框、OCI将标识网络结构中的所有交换机；但是、它需要通过IP连接到这些附加交换机才能发现它们。
- 网络结构中的所有交换机需要全局使用同一个帐户。您可以使用 PuTTY （开源终端模拟器）确认访问。
- 如果安装了Perform许可证、则端口161和162必须对网络结构中的所有交换机开放、以便进行SNMP性能轮询。
- SNMP 只读社区字符串

Configuration

字段	Description
交换机 IP	交换机的 IP 地址或完全限定域名
用户名	交换机的用户名
Password	交换机使用的密码
SNMP 版本	SNMP 版本
SNMP 社区字符串	用于访问交换机的 SNMP 只读社区字符串
SNMP 用户名	SNMP版本协议用户名(仅适用于SNMP v3)
SNMP 密码	SNMP版本协议密码(仅适用于SNMP v3)

高级配置

字段	Description
----	-------------

网络结构名称	数据源要报告的网络结构名称。留空以将网络结构名称报告为 WWN 。
排除设备	要从轮询中排除的设备 ID 的逗号分隔列表
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为15分钟)
超时(秒)	连接超时(默认为30秒)
横幅等待超时(秒)	SSH横幅等待超时(默认值为5秒)
管理域处于活动状态	选择是否使用管理域
检索 MPR 数据	选择此项可从多协议路由器(MPR)获取路由数据
启用陷阱	选择此选项可在从设备收到 SNMP 陷阱时启用采集。如果选择启用陷阱，则还必须激活 SNMP 。
陷阱之间的最短时间（秒）	陷阱触发的两次采集尝试之间的最短时间（默认值为 10 秒）
发现网络结构中的所有交换机	选择以发现网络结构中的所有交换机
选择偏向 HBA 而不是分区别名	选择是支持 HBA 别名还是分区别名
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
SNMP 身份验证协议	SNMP 身份验证协议（仅限 SNMP v3 ）
SNMP 隐私协议	SNMP隐私协议(仅限SNMP v3)
SNMP 隐私密码	SNMP 隐私密码（仅限 SNMP v3 ）
SNMP 重试	SNMP 重试尝试次数
SNMP 超时（毫秒）	SNMP 超时（默认为 5000 毫秒）

Brocade Sphereon/Intrepid交换机数据源

OnCommand Insight 使用Brocade Sphereon/Intrepid交换机(SNMP)数据源发现Brocade Sphereon或Intrepid交换机的清单。



从OnCommand Insight 7.3.11开始、此数据收集器不可用。

- 网络结构中的所有交换机都必须具有 IP 连接。如果选中发现网络结构中的所有交换机复选框、OCI将标识网络结构中的所有交换机；但是、它需要通过IP连接到这些附加交换机才能发现它们。
- 如果使用 SNMP V1 或 SNMP V2 ，则为只读社区字符串。
- 通过 HTTP 访问交换机以获取分区信息。
- 通过运行进行访问验证 snmpwalk 实用程序连接到交换机(请参见 <install_path>\bin\)。

Configuration

* 字段 *	* 问题描述 *
Sphereon 交换机	交换机的 IP 地址或完全限定域名
SNMP 版本	SNMP 版本
SNMP社区	用于访问交换机的 SNMP 只读社区字符串
用户名	交换机的 SMI-S 用户名（仅限 SNMP v3 ）
Password	交换机的 SMI-S 密码（仅限 SNMP v3 ）

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为15分钟)
SNMP 身份验证协议	SNMP 身份验证协议（仅限 SNMPv3 ）
SNMP 隐私协议	SNMP 隐私协议（仅限 SNMPv3 ）
SNMP 隐私密码	SNMP隐私密码
SNMP 重试次数	SNMP 重试尝试次数
SNMP 超时（毫秒）	SNMP 超时（默认为 5000 毫秒）
网络结构名称	数据源要报告的网络结构名称。留空以将网络结构名称报告为 WWN 。

启用陷阱	选择此选项可在从设备收到 SNMP 陷阱时启用采集。如果选择启用陷阱，则还必须激活 SNMP 。
两次陷阱之间的最短时间(秒)	陷阱触发的两次采集尝试之间的最短时间（默认值为 10 秒）
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

Cisco FC交换机固件(SNMP)数据源

OnCommand Insight 使用Cisco FC交换机固件2.0+(SNMP)数据源来发现Cisco MDS光纤通道交换机以及启用了FC服务的各种Cisco Nexus FCoE交换机的清单。此外、您还可以使用此数据源发现在NPV模式下运行的多种Cisco设备型号。

术语

OnCommand Insight 从Cisco FC交换机数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
交换机	交换机
Port	Port
VSAN	网络结构
分区	分区
逻辑交换机	逻辑交换机
名称服务器条目	名称服务器条目
VSAN 间路由（ Inter-VSAN Routing ， IVR ） 区域	IVR 区域



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 网络结构中一个交换机或单个交换机的 IP 地址
- 机箱发现，用于启用网络结构发现
- 如果使用 SNMP V2 ， 则为只读社区字符串
- 端口 161 用于访问设备

- 使用进行访问验证 snmpwalk 实用程序连接到交换机(请参见 <install_path>\>\bin\)

Configuration

字段	Description
Cisco 交换机 IP	交换机的 IP 地址或完全限定域名
SNMP 版本	要获取性能、需要使用SNMP v2或更高版本
SNMP 社区字符串	用于访问交换机的 SNMP 只读社区字符串（不适用于 SNMP v3）
用户名	交换机的用户名（仅限 SNMP v3）
Password	交换机使用的密码（仅限 SNMPv3）

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
SNMP 身份验证协议	SNMP 身份验证协议（仅限 SNMPv3）
SNMP 隐私协议	SNMP 隐私协议（仅限 SNMPv3）
SNMP 隐私密码	SNMP隐私密码
SNMP 重试	SNMP 重试尝试次数
SNMP 超时（毫秒）	SNMP 超时（默认为 5000 毫秒）
启用陷阱	选择以启用陷阱。如果启用陷阱，则还必须激活 SNMP 通知。
陷阱之间的最短时间（秒）	陷阱触发的两次采集尝试之间的最短时间（默认值为 10 秒）
发现所有光纤交换机	选择以发现网络结构中的所有交换机
排除设备	要从轮询中排除的设备 IP 的逗号分隔列表
包括设备	要包括在轮询中的设备 IP 的逗号分隔列表

检查设备类型	选择此项可仅接受那些明确将自己公布为 Cisco 设备的设备
主别名类型	<p>提供第一个首选项来解析别名。从以下选项中进行选择：</p> <ul style="list-style-type: none"> • 设备别名 <p>这是端口WWN (pWWN)的用户友好名称、可根据需要在所有配置命令中使用。Cisco MDS 9000 系列中的所有交换机都支持分布式设备别名服务（设备别名）。</p> <ul style="list-style-type: none"> • * 无 * <p>不报告任何别名</p> <ul style="list-style-type: none"> • *端口问题描述 * <p>一个问题描述 、用于帮助在端口列表中标识端口</p> <ul style="list-style-type: none"> • 分区别名(全部) <p>端口的一个用户友好名称、仅可用于分区配置</p> <ul style="list-style-type: none"> • 分区别名(仅活动) <p>端口的用户友好名称、仅可用于活动配置。这是默认值。</p>
二级别名类型	请提供第二个首选项来解析别名
三级别名类型	提供第三个首选项来解析别名
启用 SANTap 代理模式支持	选择 Cisco 交换机是否在代理模式下使用 SANTap 。如果您使用的是 EMC RecoverPoint ，则可能是 SANTap 。
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

EMC Celerra数据源

Celerra (SSH)数据源从Celerra存储收集清单信息。在配置方面、此数据源需要存储处理器的IP地址以及_read-ononly_用户名和密码。

术语

OnCommand Insight 从EMC Celerra数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此

资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Celerra网络服务器	存储
Celerra元数据卷/Celerra存储池	存储池
文件系统	内部卷
数据移动	控制器
数据移动器上挂载的文件系统	文件共享
CIFS 和 NFS 导出	共享
磁盘卷	后端 LUN



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 存储处理器的 IP 地址
- 只读用户名和密码
- SSH 端口 22

Configuration

字段	Description
Celerra的地址	Celerra设备的IP地址或完全限定域名
用户名	用于登录到Celerra设备的名称
Password	用于登录到Celerra设备的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
SSH进程等待超时(秒)	SSH进程超时(默认值为600秒)

重试次数	清单重试尝试次数
SSH横幅等待超时(秒)	SSH横幅等待超时(默认为20秒)

EMC CLARiiON (NaviCLI)数据源

在配置此数据源之前、请确保目标设备和Insight服务器上安装了EMC Navisphere命令行界面。Navisphere命令行界面版本必须与控制器上的固件版本匹配。要收集性能数据、必须打开统计信息日志记录。

Navisphere命令行界面语法

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

术语

OnCommand Insight 从EMC CLARiiON数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
存储	存储
存储处理器	存储节点
精简池、RAID组	存储池
LUN	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 每个CLARiiON存储处理器的IP地址
- CLARiiON阵列的只读Navisphere用户名和密码
- 必须在Insight服务器/RAU上安装navicli
- 访问验证：使用上述用户名和密码运行从Insight服务器到每个阵列的NaviCLI。
- Navicli版本应与阵列上的最新FLARE代码相对应
- 为了提高性能、必须打开统计信息日志记录。

- 端口要求： 80 ， 443

Configuration

字段	Description
CLARiiON存储	CLARiiON存储的IP地址或完全限定域名
用户名	用于登录到CLARiiON存储设备的名称。
Password	用于登录到CLARiiON存储设备的密码。
指向NaviCLI.exe路径或naviseccli.exe路径的命令行界面路径	的完整路径 <code>navicli.exe</code> 或 <code>naviseccli.exe</code> 可执行文件

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
使用安全客户端(naviseccli)	选择以使用安全客户端(naviseccli)
范围	安全客户端范围。默认值为 "Global" 。
CLARiiON命令行界面端口	用于CLARiiON命令行界面的端口
清单外部进程超时(秒)	外部进程超时(默认值为1800秒)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
性能外部进程超时(秒)	外部进程超时(默认值为1800秒)

EMC Data Domain数据源

此数据源从EMC Data Domain重复数据删除存储系统收集存储和配置信息。要添加数据源、您必须使用特定的配置说明和命令、并了解数据源要求和使用建议。

术语

OnCommand Insight 从EMC Data Domain数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk

数组	存储
Port	Port
文件系统	内部卷
Mtree	mtree
配额	配额
NFS 和 CIFS 共享	文件共享



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- Data Domain 设备的 IP 地址
- Data Domain 存储的只读用户名和密码
- SSH 端口 22

Configuration

字段	Description
IP 地址	Data Domain 存储阵列的 IP 地址或完全限定域名
用户名	Data Domain 存储阵列的用户名
Password	Data Domain 存储阵列的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
SSH进程等待超时(秒)	SSH进程超时(默认值为180秒)
SSH 端口	SSH 服务端口

EMC ECC StorageScope数据源

EMC ECC StorageScope设备有三种类型的数据源：5.x、6.0和6.1。

Configuration



从OnCommand Insight 7.3.11开始、此数据收集器不再可用。

* 字段 *	* 问题描述 *
ECC服务器	ECC服务器的IP地址或完全限定域名
用户名	ECC服务器的用户名
Password	ECC服务器的密码

高级配置

* 字段 *	* 问题描述 *
ECC端口	用于ECC服务器的端口
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为30分钟)
连接到数据库的协议	用于连接到数据库的协议
查询文件系统信息	选择以检索WWN别名和文件系统的详细信息。

Dell EMC ECS数据源

此数据收集器从 EMC ECS 存储系统采集清单和性能数据。在配置方面、数据收集器需要ECS服务器的IP地址和管理级别域帐户。

术语

OnCommand Insight 从EMC ECS数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
克隆用户	存储
租户	存储池
存储分段	内部卷
Disk	Disk



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- ECS 管理控制台的 IP 地址
- ECS 系统的管理级别域帐户
- 端口 443 （ HTTPS ）。需要与 ECS 系统上的 TCP 端口 443 建立出站连接。
- 对于性能，使用只读用户名和密码访问 ssh/scp 。
- 为提高性能，需要端口 22 。

Configuration

字段	Description
ECS 主机	ECS系统的IP地址或完全限定域名
ECS 主机端口	用于与 ECS 主机通信的端口
ECS 供应商 ID	ECS 的供应商 ID
Password	用于 ECS 的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔。默认值为 360 分钟。

EMC Isilon数据源

Isilon SSH数据源从EMC Isilon横向扩展NAS存储收集清单和性能。

术语

OnCommand Insight 从EMC Isilon数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
驱动器	Disk
集群	存储
Node	存储节点
文件系统	内部卷



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- Isilon 存储的管理员权限
- 已使用验证访问 telnet 连接到端口22

Configuration

字段	Description
IP 地址	Isilon 集群的 IP 地址或完全限定域名
用户名	Isilon集群的用户名
Password	Isilon集群的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
SSH进程等待超时	SSH进程超时(默认值为60秒)
SSH 端口	SSH 服务端口

正在运行CLI命令

从OnCommand Insight 7.3.11和服务包 9开始、EMC Isilon数据源包含一项增强功能、可使Insight运行更多命令行界面命令。如果您在数据源中使用的是非root用户、则可能已配置一个"sudoers"文件、以使该用户帐户能够通过SSH运行特定的命令行界面命令。

为了让Insight了解EMC的"访问区域"功能、Insight现在还将运行以下新的命令行界面命令：

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

Insight会分析这些命令的输出并运行更多现有命令实例、以获取非默认访问区域中的qtree、配额和NAS共享/导出等对象的逻辑配置。现在、Insight会通过此增强功能为非默认访问区域报告这些对象。由于Insight通过运行现有命令(使用不同的选项)来获取数据、因此无需对sudoers文件进行更改、这些命令才能正常运行；只有在上述新命令推出后、才需要进行更改。

在升级到此Insight版本之前、请更新sudoers文件以允许您的Insight服务帐户运行这些命令。否则、Isilon数据源将失败。

"文件系统"统计信息

从OnCommand Insight 7.3.12开始、EMC Isilon数据收集器引入了EMC Isilon节点对象的"文件系统"统计信息。OnCommand Insight 报告的现有节点统计信息基于"磁盘"、即、对于存储节点的IOPS和吞吐量、此节点中的磁盘在聚合中执行了哪些操作？但是、对于读取缓存在内存中且/或正在使用数据压缩的工作负载、文件系统工作负载可能远远高于实际命中磁盘的工作负载-因此、压缩5：1的数据集可能具有5倍于存储节点读取吞吐量的"文件系统读取吞吐量"值、后者用于测量磁盘的读取、当节点解压缩数据以满足客户端的读取请求时、磁盘将扩展5倍。

Dell EMC PowerStore数据源

Dell EMC PowerStore数据收集器从Dell EMC PowerStore存储收集清单信息。在配置方面，数据收集器需要存储处理器的 IP 地址以及只读用户名和密码。

术语

OnCommand Insight 从EMC Data Domain数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
host	host
host_volume_mapping	host_volume_mapping
硬件（驱动器位于 "ext_details" 对象下）： drives	Disk
设备	StoragePool
集群	存储阵列
Node	StorageNode
FC_port	Port
volume	Volume
内部卷	file_system
文件系统	内部卷
Mtree	qtree
配额	配额
NFS 和 CIFS 共享	文件共享



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 存储处理器的 IP 地址或完全限定域名
- 只读用户名和密码

说明了父级序列号

传统上、Insight可以报告存储阵列序列号或单个存储节点序列号。但是、某些存储阵列架构并不完全符合此要求。一个PowerStore集群可以由1-4个设备组成、每个设备都有2个节点。如果设备本身具有序列号、则该序列号既不是集群的序列号、也不是节点的序列号。

如果各个节点位于仅属于较大集群一部分的中间设备/机箱中、则存储节点对象上的"父序列号"属性会针对Dell/EMC PowerStore阵列正确填充。

Configuration

字段	Description
PowerStore 网关	PowerStore 存储的 IP 地址或完全限定域名
用户名	PowerStore 的用户名
Password	PowerStore 使用的密码

高级配置

字段	Description
HTTPS 端口	默认值为 443
清单轮询间隔（分钟）	两次清单轮询的间隔。默认值为 60 分钟。

OnCommand Insight的PowerStore性能收集利用了PowerStore的5分钟粒度源数据。因此、Insight每五分钟轮询一次该数据、而这是无法配置的。

EMC RecoverPoint数据源

EMC RecoverPoint数据源从EMC RecoverPoint存储收集清单信息。在配置方面、数据源需要存储处理器的IP地址以及_read-only_用户名和密码。

EMC RecoverPoint数据源收集RecoverPoint在其他存储阵列之间协调的卷到卷复制关系。OnCommand Insight会显示每个RecoverPoint集群的存储阵列、并收集该集群上节点和存储端口的清单数据。不会收集任何存储池或卷数据。

要求

- 存储处理器的 IP 地址或完全限定域名
- 只读用户名和密码
- 通过端口 443 进行 REST API 访问
- 通过PuTTY进行SSH访问

Configuration

字段	Description
RecoverPoint 的地址	RecoverPoint 集群的 IP 地址或完全限定域名
用户名	RecoverPoint 集群的用户名
Password	RecoverPoint集群的密码

高级配置

字段	Description
TCP 端口	用于连接到 Recoverpoint 集群的 TCP 端口
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
排除的集群	要在轮询时排除的集群ID或名称的逗号分隔列表

具有SMI-S性能数据源的EMC Solutions Enabler

OnCommand Insight 使用Solutions Enabler发现Symmetrix存储阵列 `symcli` 命令与环境中的现有Solutions Enabler服务器结合使用。现有Solutions Enabler服务器可通过访问Gatekeeper卷连接到Symmetrix存储阵列。要访问此设备、需要管理员权限。

术语

OnCommand Insight 从EMC Solutions Enabler数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
磁盘组	磁盘组
存储阵列	存储

总监	存储节点
设备池，存储资源池（SRP）	存储池
设备、TDev	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

在配置此数据源之前、您应确保OnCommand Insight 服务器与现有Solutions Enabler服务器上的端口2707具有TCP连接。OnCommand Insight 会发现此服务器上"local"的所有Symmetrix阵列、如该服务器的"symcfg list"输出所示。

- 必须安装带有SMI-S提供程序的EMC Solutions Enabler (CLI)应用程序、并且此版本必须与Solutions Enabler服务器上运行的版本匹配或早于此版本。
- 已正确配置 {installdir}\EMC\SYMAPI\config\netcnfg 文件为必填项。此文件定义 Solutions Enabler 服务器的服务名称以及访问方法（SECURE / NOSECURE / ANY）。
- 如果在存储节点级别需要读 / 写延迟，SMI-S Provider 必须与正在运行的 Unisphere for VMAX 应用程序实例进行通信。
- Solutions Enabler （SE）服务器上的管理员权限
- SE 软件的只读用户名和密码
- Solutions Enabler Server 6.5X 要求：
 - 安装了SMI-S V1.2的SMI-S Provider 3.3.1
 - 安装完成后、运行 \Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd
- 适用于VMAX的Unisphere应用程序必须正在运行并收集由SMI-S Provider安装管理的Symmetrix VMAX存储阵列的统计信息
- 访问验证：验证SMI-S提供程序是否正在运行：telnet <se_server> 5988

Configuration



如果未启用SMI-S用户身份验证、则会忽略OnCommand Insight 数据源中的默认值。

在Symmetrix阵列上启用symauth可能会阻止OnCommand Insight 发现它们。OnCommand Insight 采集以系统用户身份在与解决方案启用程序服务器通信的OnCommand Insight /远程采集单元服务器上运行。如果hostname\system没有symauth权限、则OnCommand Insight 将无法发现阵列。

EMC Solutions Enabler Symmetrix CLI数据源支持精简配置和Symmetrix远程数据工具(SRDF)的设备配置。

提供了光纤通道和交换机性能软件包的定义。

字段	Description
服务名称	在netcnfg文件中指定的服务名称

CLI 的完整路径	Symmetrix CLI的完整路径
-----------	--------------------

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
选择 " 排除 " 或 " 包括 " 以指定列表	指定在收集数据时是包含还是排除以下阵列列表
清单排除设备	要包含或排除的设备 ID 的逗号分隔列表
连接缓存	<p>选择连接缓存方法：</p> <ul style="list-style-type: none"> 本地表示OnCommand Insight 采集服务正在Solutions Enabler服务器上运行、该服务器可通过光纤通道连接到您要发现的Symmetrix阵列、并可访问Gatekeeper卷。在某些远程采集单元（RAU）配置中可能会出现这种情况。 remote_cached为默认值、大多数情况下应使用。这将使用 NETCNFG 文件设置通过 IP 连接到 Solutions Enabler 服务器，该服务器必须通过光纤通道连接到您要发现的 Symmetrix 阵列，并有权访问 Gatekeeper 卷。 如果remote_cached选项使CLI命令失败、请使用remote选项。请注意，这会减慢采集过程的速度（在极端情况下可能会减慢到数小时甚至数天）。NETCNFG 文件设置仍用于通过 IP 连接到 Solutions Enabler 服务器，该服务器通过光纤通道连接到正在发现的 Symmetrix 阵列。 <div>  <p>此设置不会更改与"symcfg list"输出中列为REMOTE的阵列相关的OnCommand Insight 行为。OnCommand Insight 仅收集此命令显示为local的设备上的数据。</p> </div>
CLI超时(秒)	CLI进程超时(默认值为7200秒)
SMI-S主机IP	SMI-S提供程序主机的IP地址
SMI-S端口	SMI-S Provider主机使用的端口
协议	用于连接到 SMI-S 提供程序的协议
SMI-S命名空间	SMI-S提供程序配置要使用的互操作性命名空间

SMI-S 用户名	SMI-S Provider 主机的用户名
SMI-S 密码	SMI-S Provider 主机的用户名
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 1000 秒）
性能筛选器类型	指定在收集性能数据时是包含还是排除以下阵列列表
性能筛选器设备列表	要包含或排除的设备 ID 的逗号分隔列表
RPO轮询间隔(秒)	RPO轮询之间的时间间隔(默认值为300秒)

EMC VNX数据源

在配置方面、EMC VNX (SSH)数据源需要控制站的IP地址以及_read-ononly_用户名和密码。

Configuration

字段	Description
VNX IP	VNX 控制站的 IP 地址或完全限定域名
VNX用户名	VNX 控制站的用户名
VNX密码	VNX 控制站的密码

要求

- Control Station的IP地址
- 只读用户名和密码。
- 访问验证：通过PuTTY验证SSH访问。

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
VNX SSH进程等待超时(秒)	VNX SSH进程超时(默认值为600秒)
Celerra命令重试尝试次数	Celerra命令重试的次数
CLARiiON清单外部进程超时(秒)	CLARiiON清单外部进程超时(默认值为1800秒)

性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
CLARiiON性能外部进程超时(秒)	CLARiiON性能外部进程超时(默认值为1800秒)

EMC VNXe数据源

EMC VNXe数据源为EMC VNXe和Unity统一存储阵列提供清单支持。

此数据源基于CLI、需要在VNXe数据源所在的采集单元上安装Unisphere for VNXe CLI (uemcli.exe)。uemcli.exe使用HTTPS作为传输协议、因此采集单元必须能够启动与VNXe/Unity阵列的HTTPS连接。您必须至少具有一个只读用户以供数据源使用。

术语

OnCommand Insight 从EMC VNXe数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
存储阵列	存储
处理器	存储节点
存储池	存储池
常规 iSCSI 块信息， VMware VMFS	Volume
共享文件夹	内部卷
CIFS共享、NFS共享、VMware NFS数据存储库中的共享	共享
复制远程系统	同步
iSCSI 节点	iSCSI 目标节点
iSCSI 启动程序	iSCSI 目标启动程序



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

以下是配置和使用此数据源的要求：

- VNXe 数据收集器基于 CLI；您必须将适用于 VNXe CLI 的 Unisphere（uemcli.exe）安装到 VNXe 数据收集器所在的采集单元上。
- uemcli.exe 使用 HTTPS 作为传输协议，因此采集单元需要能够启动与 VNXe 的 HTTPS 连接。
- 您必须至少具有一个只读用户以供数据源使用。
- 管理解决方案启用程序服务器的 IP 地址。
- 端口 443 上的 HTTPS 为必填项
- EMC VNXe数据收集器为清单提供NAS和iSCSI支持；将发现光纤通道卷、但Insight不会报告FC映射、屏蔽或存储端口。

Configuration

字段	Description
VNXe 存储	VNXe 设备的 IP 地址或完全限定域名
用户名	VNXe 设备的用户名
Password	VNXe 设备的密码
uemcli可执行文件的完整路径	的完整路径 uemcli.exe 可执行文件

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
VNXe命令行界面端口	用于 VNXe 命令行界面的端口
清单外部进程超时(秒)	外部进程超时(默认值为1800秒)

EMC VPLEX数据源

在配置方面、此数据源需要VPLEX服务器的IP地址和管理级别域帐户。

术语

OnCommand Insight 从EMC VPLEX数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
集群	存储

引擎	存储节点
设备、系统扩展	后端存储池
虚拟卷	Volume
前端端口，后端端口	Port
分布式设备	存储同步
存储视图	卷映射，卷掩码
存储卷	后端 LUN
ITL	后端路径



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- VPLEX服务器的IP地址
- VPLEX 服务器的管理级别域帐户
- 端口 443 （ HTTPS ）。需要通过出站连接到 VPLEX 管理工作站上的 TCP 端口 443 。
- 对于性能，使用只读用户名和密码访问 ssh/scp 。
- 为提高性能，需要端口 22 。
- 验证访问：使用进行验证 telnet 连接到端口443。对于默认端口以外的端口、可使用任何浏览器

Configuration

字段	Description
VPLEX 管理控制台的 IP 地址	VPLEX 管理控制台的 IP 地址或完全限定域名
用户名	VPLEX 命令行界面的用户名
Password	用于 VPLEX 命令行界面的密码
VPLEX管理控制台的性能远程IP地址	VPLEX 管理控制台的性能远程 IP 地址
性能远程用户名	VPLEX 管理控制台的性能远程用户名
性能远程密码	VPLEX 管理控制台的性能远程密码

字段	Description
通信端口	用于VPLEX命令行界面的端口
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
连接超时(秒)	连接超时(默认为60秒)
重试次数	清单重试尝试次数
性能轮询间隔（秒）	性能轮询之间的时间间隔(默认值为600秒)
性能SSH进程等待超时(秒)	SSH进程超时(默认值为600秒)
SSH横幅等待超时(秒)	SSH横幅等待超时(默认为20秒)
重试次数	性能重试尝试次数

EMC XtremIO数据源

要配置EMC XtremIO (HTTP)数据源、您必须具有XtremIO管理服务器(XMS)主机地址和具有管理员权限的帐户。

术语

OnCommand Insight 从EMC XtremIO数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
磁盘（SSD）	Disk
集群	存储
控制器	存储节点
Volume	Volume
LUN 映射	卷映射
启动程序、目标	卷掩码



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 每个XtremIO管理服务器的IP地址
- 具有管理员权限的帐户
- 访问端口 443 （ HTTPS ）

Configuration

字段	Description
XMS 主机	XtremIO 管理服务器的 IP 地址或完全限定域名
用户名	XtremIO 管理服务器的用户名
Password	XtremIO 管理服务器的密码

高级配置

字段	Description
TCP 端口	用于连接到XTremIO管理服务器的TCP端口(默认值为443)
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为60分钟)
连接超时(秒)	连接超时(默认为60秒)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

Fujitsu Eternus数据源

Fujitsu Eternus数据源需要存储的IP地址。不能以逗号分隔。

术语

OnCommand Insight 从Fujitsu Eternus数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
存储	存储

精简池、灵活层池、 RAID 组	存储池
标准卷、快照数据卷(SDV)、 快照数据池卷(SDPV)、 精简配置卷(TPV)	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- Eternus 存储的 IP 地址，不能以逗号分隔
- SSH 管理级别的用户名和密码
- 端口 22
- 确保已禁用页面滚动。(clienv-show-more-sl滚动 禁用)

Configuration

字段	Description
Eternus 存储的 IP 地址	Eternus 存储的 IP 地址
用户名	Eternus 存储的用户名
Password	用于ternus的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
SSH进程等待超时(秒)	SSH进程超时(默认值为600秒)

Hitachi Content Platform (HCP)数据源

此数据收集器使用 HCP 管理 API 支持 Hitachi 内容平台（HCP）。

术语

OnCommand Insight 从HCP数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
HCP 集群	存储
租户	存储池
命名空间	内部卷
Node	Node



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

清单要求

- HCP 服务器的 IP 地址
- HCP 软件的只读用户名和密码以及对等权限

Configuration

* 字段 *	* 问题描述 *
HCP 主机	HCP 主机的 IP 地址或完全限定域名
HCP 端口	默认值为 9090
HCP 用户 ID	HCP 主机的用户名
HCP 密码	用于 HCP 主机的密码
HCP 身份验证类型	选择 HCP_local 或 active_directory

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为60分钟)
性能轮询间隔（秒）	性能轮询之间的时间间隔(默认值为900秒)

HDS HiCommand Device Manager 数据源

HDS HiCommand 和 HiCommand Lite 精简版数据源支持 HiCommand Device Manager 服务器。OnCommand Insight 使用标准 HiCommand API 与 HiCommand 设备管理器服务器进行通信。

OnCommand Insight 从HDS HiCommand和HiCommand Lite精简版数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
PDEV	Disk
日志池	磁盘组
存储阵列	存储
端口控制器	存储节点
阵列组， DP 池	存储池
逻辑单元， LDEV	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

清单要求

- HiCommand Device Manager 服务器的 IP 地址
- HiCommand Device Manager 软件的只读用户名和密码以及对等权限
- 端口要求： 2001 （ http ） 或 2443 （ https ）
- 验证访问：
 - 使用对等用户名和密码登录到HiCommand Device Manager软件。
 - 验证对HiCommand Device Manager API的访问： `telnet <HiCommand Device_Manager_server_ip> 2001`

性能要求

- HDS USP ， USP V 和 VSP 性能
 - Performance Monitor 必须获得许可。
 - 必须启用监控交换机。
 - 导出工具 (Export.exe)必须复制到OnCommand Insight 服务器。
 - 导出工具版本必须与目标阵列的微代码版本匹配。
- HDS AMS性能
 - Performance Monitor需要获得许可。
 - OnCommand Insight 服务器上需要安装存储导航器模块化2 (SNM2)命令行界面实用程序。
 - 您必须使用以下命令注册所有需要由OnCommand Insight 获取性能的AMS、WMS、SMS存储阵列：

- 。您必须确保已注册的所有阵列均在此命令的输出中列出： `auunitref.exe`。

Configuration

* 字段 *	* 问题描述 *
HiCommand 服务器	HiCommand Device Manager 服务器的 IP 地址或完全限定域名
用户名	HiCommand Device Manager 服务器的用户名。
Password	HiCommand Device Manager 服务器使用的密码。
设备— VSP G1000 (R800) , VSP (R700) , HUS VM (HM700) 和 USP 存储	<p>VSP G1000 (R800) , VSP (R700) , HUS VM (HM700) 和 USP 存储的设备列表。每个存储都需要：</p> <ul style="list-style-type: none"> • Array's IP: 存储的IP地址 • User Name: 存储的用户名 • Password: 存储的密码 • Folder Containing Export Utility JAR Files: 包含导出实用程序的文件夹 .jar 文件
SNM2Devices — WMS/SMS/AMS 存储	<p>WMS/SMS/AMS 存储的设备列表。每个存储都需要：</p> <ul style="list-style-type: none"> • Array's IP: 存储的IP地址 • 存储导航器CLI路径: SNM2 CLI路径 • Account Authentication Valid: 选择可选择有效的帐户身份验证 • User Name: 存储的用户名 • Password: 存储的密码
选择性能调整管理器	选择性能调整管理器并覆盖其他性能选项
调整管理器主机	调整管理器的 IP 地址或完全限定域名
调整管理器端口	用于调整管理器的端口
调整管理器用户名	调整管理器的用户名
调整管理器密码	调整管理器的密码



在HDS USP、USP V和VSP中、任何磁盘都可以属于多个阵列组。

字段	Description
HiCommand 服务器端口	HiCommand Device Manager 所使用的端口
已启用 HTTPS	选择以启用 HTTPS
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
选择 " 排除 " 或 " 包括 " 以指定列表	指定在收集数据时是包含还是排除以下阵列列表
排除或包括设备	要包含或排除的设备 ID 或阵列名称的逗号分隔列表
查询 Host Manager	选择以查询主机管理器
HTTP超时(秒)	HTTP连接超时(默认为60秒)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
导出超时（以秒为单位）	导出实用程序超时(默认值为300秒)

Hitachi Ops Center 数据收集器

此数据收集器使用 Hitachi Ops Center 的集成应用程序套件来访问多个存储设备的清单和性能数据。要发现清单和容量，您的运营中心安装必须同时包含 " 通用服务 " 和 " 管理员 " 组件。要收集性能，您还必须部署 " 分析器 "。

术语

OnCommand Insight从此数据收集器采集以下清单信息。对于所采集的每种资产类型，均显示了此资产最常用的术语。查看此数据收集器或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	OnCommand Insight 术语
存储系统	存储
Volume	Volume
奇偶校验组	存储池（RAID），磁盘组
Disk	Disk
存储池	存储池（精简，快照）
外部奇偶校验组	存储池（后端），磁盘组
Port	存储节点→控制器节点→端口
主机组	卷映射和屏蔽

供应商 / 型号术语	OnCommand Insight 术语
卷对	存储同步

注意：这些只是常见的术语映射，可能并不代表此数据收集器的所有情形。

清单要求

要收集清单数据，您必须满足以下条件：

- 托管"通用服务"组件的操作中心服务器的IP地址或主机名
- 托管Operations Center组件的所有服务器上存在的root/sysadmin用户帐户和密码。在Operations Center 10.8+之前、HDS未实施REST API支持以供LDAP/SSO用户使用

性能要求

要收集性能数据，必须满足以下要求：

- 必须安装HDS Ops Center"分析器"模块
- 存储阵列必须为运营中心的"分析器"模块馈送数据

Configuration

字段	Description
Hitachi Ops Center IP 地址	托管 " 通用服务 " 组件的操作中心服务器的 IP 地址或完全限定域名
用户名	Operations Center 服务器的用户名。
Password	用于 Operations Center 服务器的密码。

高级配置

字段	Description
连接类型	HTTPS （端口 443 ）为默认值
覆盖 TCP 端口	指定要使用的端口（如果不是默认端口）
清单轮询间隔（分钟）	两次清单轮询的间隔。默认值为 40. 。
选择 " 排除 " 或 " 包括 " 以指定列表	指定在收集数据时是包含还是排除以下阵列列表。
筛选设备列表	要包含或排除的设备序列号的逗号分隔列表
性能轮询间隔（秒）	性能轮询之间的时间间隔。默认值为 300. 。

HDS存储

适用于HDS存储资产登录页面上可能存在的对象或引用的术语。

HDS存储术语

以下术语适用于您在 HDS 存储资产登录页面上可能找到的对象或引用。其中许多术语也适用于其他数据收集器。

- name—通过GetStorageArray XML API调用直接来自HDS HiCommand设备管理器的"name"属性
- 型号—通过GetStorageArray XML API调用直接来自HDS HiCommand Device Manager的"arrayType"属性
- 供应商—HDS
- 系列—通过GetStorageArray XML API调用直接来自HDS HiCommand Device Manager的"arrayFamily"属性
- ip—这是阵列的管理IP地址、而不是阵列上所有IP地址的完整列表
- 原始容量—BASE2值、表示此系统中所有磁盘的总容量之和、而不管磁盘角色如何。

HDS存储池

适用于HDS存储池资产登录页面上可能存在的对象或引用的术语。

HDS存储池术语

以下术语适用于您在 HDS 存储池资产登录页面上可能找到的对象或引用。其中许多术语也适用于其他数据收集器。

- type：此处的值将为以下值之一：
 - Reserved—如果此池专用于数据卷、即日志、快照以外的其他用途
 - 精简配置—如果这是一个HDP池
 - RAID组—您可能无法看到这些内容、原因如下：

OCI采取强有力的立场、避免在任何成本下重复计算容量。在 HDS 上，通常需要使用磁盘构建 RAID 组，在这些 RAID 组上创建池卷，并从这些池卷构建池（通常为 HDP，但可能具有特殊用途）。如果OCI按原样报告底层RAID组以及池、则其原始容量之和将远远超过磁盘之和。

相反、OCI的HDS HiCommand数据收集器会根据池卷的容量任意缩减RAID组的大小。这可能会导致OCI根本不报告RAID组。此外、任何生成的RAID组都会以某种方式进行标记、使其在OCI WebUI中不可见、但它们确实会流入OCI数据仓库(DWH)。这些决策的目的是避免大多数用户不关心的事情出现UI混乱情况—如果您的HDS阵列中的RAID组可用空间为50 MB、您可能无法使用该可用空间来获得有意义的结果。

- 节点—不适用，因为 HDS 池不会绑定到任何一个特定节点
- 冗余—池的 RAID 级别。一个由多种 RAID 类型组成的 HDP 池可能具有多个值
- 容量 % —池中数据使用量的已用百分比，以及池的已用 GB 和总逻辑 GB 大小
- 过量使用容量—一个派生值、表示"由于逻辑卷之和超过池的逻辑容量之和、此池的逻辑容量由此百分比超额使用"
- Snapshot —显示此池上为快照使用预留的容量

HDS存储节点

适用于HDS存储节点资产登录页面上可能存在的对象或引用的术语。

HDS存储节点术语

以下术语适用于您在 HDS 存储节点资产登录页面上可能找到的对象或引用。其中许多术语也适用于其他数据收集器。

- name—单片阵列上的前端控制器(FED)或通道适配器的名称、或者模块化阵列上的控制器的名称。一个给定的 HDS 阵列将具有 2 个或更多存储节点
- Volumes—卷表将显示映射到此存储节点拥有的任何端口的任何卷

Hitachi Ops Center 数据收集器

此数据收集器使用 Hitachi Ops Center 的集成应用程序套件来访问多个存储设备的清单和性能数据。要发现清单和容量，您的运营中心安装必须同时包含 " 通用服务 " 和 " 管理员 " 组件。要收集性能，您还必须部署 " 分析器 "。

术语

OnCommand Insight从此数据收集器采集以下清单信息。对于所采集的每种资产类型，均显示了此资产最常用的术语。查看此数据收集器或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	OnCommand Insight 术语
存储系统	存储
Volume	Volume
奇偶校验组	存储池（ RAID ），磁盘组
Disk	Disk
存储池	存储池（精简，快照）
外部奇偶校验组	存储池（后端），磁盘组
Port	存储节点→控制器节点→端口
主机组	卷映射和屏蔽
卷对	存储同步

注意：这些只是常见的术语映射，可能并不代表此数据收集器的所有情形。

清单要求

要收集清单数据，您必须满足以下条件：

- 托管"通用服务"组件的操作中心服务器的IP地址或主机名
- 托管Operations Center组件的所有服务器上存在的root/sysadmin用户帐户和密码。在Operations Center 10.8+之前、HDS未实施REST API支持以供LDAP/SSO用户使用

性能要求

要收集性能数据，必须满足以下要求：

- 必须安装HDS Ops Center"分析器"模块

- 存储阵列必须为运营中心的"分析器"模块馈送数据

Configuration

字段	Description
Hitachi Ops Center IP 地址	托管 " 通用服务 " 组件的操作中心服务器的 IP 地址或完全限定域名
用户名	Operations Center 服务器的用户名。
Password	用于 Operations Center 服务器的密码。

高级配置

字段	Description
连接类型	HTTPS （端口 443 ）为默认值
覆盖 TCP 端口	指定要使用的端口（如果不是默认端口）
清单轮询间隔（分钟）	两次清单轮询的间隔。默认值为 40. 。
选择 " 排除 " 或 " 包括 " 以指定列表	指定在收集数据时是包含还是排除以下阵列列表。
筛选设备列表	要包含或排除的设备序列号的逗号分隔列表
性能轮询间隔（秒）	性能轮询之间的时间间隔。默认值为 300. 。

HDS NAS (HNAS)数据源

HDS NAS (HNAS)数据源是一个清单和配置数据源、用于支持发现HDS NAS集群。Insight支持发现NFS和CIFS共享、文件系统(Insight内部卷)和跨区(Insight存储池)。

此数据源基于SSH、因此要托管它的采集单元需要能够在HNAS本身或集群所连接的系统管理单元(Systems Management Unit、SMU)上启动与TCP 22的SSH会话。

术语

OnCommand Insight 从HNAS数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
层	磁盘组
集群	存储
Node	存储节点
范围	存储池
文件系统	内部卷



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

以下是配置和使用此数据源的要求：

- 设备 IP 地址
- 端口 22 ， SSH 协议
- username and password —权限级别： supervisor
- 注意：此数据收集器基于SSH、因此托管此数据收集器的AU必须能够在HNAS本身或集群所连接的系统管理单元(SMU)上启动与TCP 22的SSH会话。



此数据收集器基于SSH、因此托管此数据收集器的AU必须能够在HNAS本身或集群所连接的系统管理单元(SMU)上启动与TCP 22的SSH会话。

Configuration

字段	Description
HNAS 主机	HNAS 管理主机的 IP 地址或完全限定域名
用户名	HNAS CLI 的用户名
Password	HNAS CLI 使用的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为30分钟)
SSH横幅等待超时(秒)	SSH横幅等待超时(默认值为15秒)
SSH命令超时(秒)	SSH命令超时(默认为30秒)

HP CommandView AE数据源

HP CommandView高级版(AE)和CommandView AE CLI/SMI (AE精简版)数据源支持CommandView (也称为HiCommand) Device Manager服务器的清单和性能。

术语

OnCommand Insight 从HP CommandView AE和AE精简版数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
PDEV	Disk
日志池	磁盘组
存储阵列	存储
端口控制器	存储节点
阵列组， DP 池	存储池
逻辑单元， LDEV	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

清单要求

- HiCommand Device Manager 服务器的 IP 地址
- CommandView AE软件的只读用户名和密码以及对等权限
- 设备管理器的CommandView AE精简版仅许可使用CLI
- 端口要求： 2001

性能要求

- HDS USP ， USP V 和 VSP 性能
 - Performance Monitor 必须获得许可。
 - 必须启用监控交换机。
 - 导出工具 (Export.exe)必须复制到OnCommand Insight 服务器。
 - 导出工具版本必须与目标阵列的微代码版本匹配。
- HDS AMS性能
 - Performance Monitor需要获得许可。
 - OnCommand Insight 服务器上需要安装存储导航器模块化2 (SNM2)命令行界面实用程序。
 - 您必须使用以下命令注册所有需要由OnCommand Insight 获取性能的AMS、WMS、SMS存储阵列：
 - 您必须确保已注册的所有阵列均在此命令的输出中列出： `auunitref.exe`。

Configuration

* 字段 *	* 问题描述 *
HiCommand 服务器	HiCommand Device Manager 服务器的 IP 地址或完全限定域名

用户名	HiCommand Device Manager 服务器的用户名。
Password	HiCommand Device Manager 服务器使用的密码。
设备—USP、USP V、VSP/R600存储	<p>VSP G1000（R800），VSP（R700），HUS VM（HM700）和 USP 存储的设备列表。每个存储都需要：</p> <ul style="list-style-type: none"> • Array's IP：存储的IP地址 • User Name：存储的用户名 • Password：存储的密码 • Folder Containing Export Utility JAR Files：包含导出实用程序的文件夹 .jar 文件
SNM2Devices — WMS/SMS/AMS 存储	<p>WMS/SMS/AMS 存储的设备列表。每个存储都需要：</p> <ul style="list-style-type: none"> • Array's IP：存储的IP地址 • 存储导航器CLI路径：SNM2 CLI路径 • Account Authentication Valid：选择可选择有效的帐户身份验证 • User Name：存储的用户名 • Password：存储的密码
选择性能调整管理器	选择性能调整管理器并覆盖其他性能选项
调整管理器主机	调整管理器的 IP 地址或完全限定域名
调整管理器端口	用于调整管理器的端口
调整管理器用户名	调整管理器的用户名
调整管理器密码	调整管理器的密码



在HDS USP、USP V和VSP中、任何磁盘都可以属于多个阵列组。

高级配置

字段	Description
HiCommand 服务器端口	HiCommand Device Manager 所使用的端口
已启用 HTTPS	选择以启用 HTTPS

清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
选择 " 排除 " 或 " 包括 " 以指定列表	指定在收集数据时是包含还是排除以下阵列列表
排除或包括设备	要包含或排除的设备 ID 或阵列名称的逗号分隔列表
查询 Host Manager	选择以查询主机管理器
HTTP超时(秒)	HTTP连接超时(默认为60秒)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
导出超时（以秒为单位）	导出实用程序超时(默认值为300秒)

HP EVA存储数据源

在配置方面、EVA存储(SSSU)数据源需要Command View (CV)服务器的IP地址以及CV软件的_read-oned_用户名和密码。用户必须在CV软件中进行定义。

术语

OnCommand Insight 从HP EVA数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
磁盘组	磁盘组(未建模)
存储单元	存储
虚拟磁盘	存储池
虚拟磁盘	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

清单要求

- CV服务器的IP地址
- CV软件的只读用户名和密码。用户必须在CV软件中进行定义。
- OnCommand Insight Server/Rau上安装的第三方软件： `sssu.exe`。 `sssu.exe` 版本应与CV版本相对应。

- 访问验证：运行 `sssu.exe` 使用用户名和密码的命令。

性能要求

OnCommand Insight 服务器上必须安装HP StorageWorks Command View EVA软件套件。或者、您也可以
在EVA服务器上安装远程采集单元(RAU)：

1. 在OnCommand Insight 服务器上安装HP StorageWorks Command View EVA软件套件、或者在Command View EVA服务器上安装远程采集单元。
2. 找到 `evaperf.exe` 命令：例如：`c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. 使用Command View服务器的IP执行以下步骤：
 - a. 运行此命令、其中860为默认端口 `Evaperf.exe server <Command View Server IP\> 860 <username\>`
 - b. 在密码提示符处输入Command View服务器密码。

此操作应返回命令行提示符、而不返回任何其他内容。

4. 运行以验证设置 `evaperf.exe ls`。

您应看到一个由Command View服务器管理的阵列或控制器列表。每行显示EVA阵列上的一个控制器。

Configuration

* 字段 *	* 问题描述 *
CommandView服务器	EVA Storage Manager的IP地址或完全限定域名
用户名	Command View管理器的用户名。此名称必须在Command View中定义。
Password	Command View管理器使用的密码。
性能用户名	为提高性能、命令视图管理器的用户名。此名称必须在Command View中定义。
性能密码	为提高性能、命令视图管理器使用的密码。

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
命令行界面主页	CLI主目录的完整路径名、其中 <code>sssu.exe</code> 已找到

清单排除设备	要包含的设备名称的逗号分隔列表
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
性能命令行界面主页	对于阵列性能、请输入sssu.exe所在的命令行界面主目录的完整路径名。要验证访问、请运行 sssu.exe
命令超时(秒)	evaperf 命令等待超时(默认值为600秒)
性能排除设备	收集性能数据时要排除的设备名称的逗号分隔列表

HPE Nimble数据源

HPE Nimble 数据收集器支持 HPE Nimble 存储阵列的清单和性能数据。

术语

OnCommand Insight 从HPE Nimble数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
数组	存储
Disk	Disk
池	存储池
Volume	Volume
启动程序	存储主机别名
控制器	存储节点
光纤通道接口	控制器



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 阵列必须已安装和配置，并且可通过其完全限定域名（ FQDN ）或阵列管理 IP 地址从客户端访问。
- 该阵列必须运行 NimbleOS 2.3.x 或更高版本。
- 您必须具有该阵列的有效用户名和密码。

- 阵列上的端口 5392 必须处于打开状态。

Configuration

* 字段 *	* 问题描述 *
阵列管理 IP 地址	完全限定域名（ FQDN ）或阵列管理 IP 地址。
用户名	Nimble 阵列的用户名
Password	Nimble 阵列的密码

高级配置

* 字段 *	* 问题描述 *
Port	Nimble REST API 使用的端口。默认值为 5392. 。
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为60分钟)

注意：默认性能轮询间隔为 300 秒，无法更改。这是 Nimble 唯一支持的间隔。

Huawei OceanStor数据源

OnCommand Insight 使用Huawei OceanStor (REST/HTTPS)数据源发现Huawei OceanStor存储的清单。

术语

OnCommand Insight 从华为OceanStor采集以下清单和性能信息。对于OnCommand Insight 收购的每种资产类型、均显示了此资产最常用的术语。查看此数据收集器或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	OnCommand Insight 术语
存储池	存储池
文件系统	内部卷
控制器	存储节点
FC 端口（已映射）	卷映射
主机 FC 启动程序（已映射）	卷掩码
NFS/CIFS 共享	共享

共享	iSCSI 目标节点
iSCSI 链路启动程序	iSCSI 启动程序节点
Disk	Disk
LUN	Volume

要求

配置和使用此数据收集器的要求如下：

- 设备IP
- 用于访问 OceanStor 设备管理器的凭据
- 端口 8088 必须可用

Configuration

字段	Description
OceanStor 主机 IP 地址	OceanStor Device Manager 的 IP 地址或完全限定域名
用户名	用于登录到 OceanStor Device Manager 的名称
Password	用于登录到 OceanStor Device Manager 的密码

高级配置

字段	Description
TCP 端口	用于连接到OceanStor Device Manager的TCP端口(默认值为8088)
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为60分钟)
连接超时（秒）	连接超时(默认为60秒)

IBM Cleversafe数据源

此数据源收集IBM Cleversafe的清单和性能数据。

要求

以下是配置此数据源的要求：

- 管理器IP地址或主机名
- 用户名和密码相同
- 端口 9440

Configuration

字段	Description
Cleversafe Manager主机名或IP地址	Cleversafe设备的主机IP地址
用户名	用于登录到Cleversafe的名称
Password	用于登录到Cleversafe的密码

高级配置

字段	Description
清单轮询间隔（分钟）	默认值为 60 分钟
HTTP连接超时)	默认值为60秒

IBM DS数据源

IBM DS (CLI)数据源仅支持DS6xxx和DS8xxx设备。NetApp E系列数据源支持DS3xxx、DS4xxx和DS5xxx设备。有关支持的型号和固件版本、请参见Insight数据源支持列表。

术语

OnCommand Insight 从IBM DS数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
磁盘驱动器模块	Disk
存储映像	存储
块区池	存储池
固定块卷	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 每个 DS 阵列的 IP 地址
- 存储显示名称是可选的、仅供外观使用
- 每个 DS 阵列上的只读用户名和密码
- Insight服务器上安装的第三方软件：IBM dscli
- 访问验证：运行 dscli 使用用户名和密码的命令
- 端口要求： 80 ， 443 和 1750

Configuration

字段	Description
DS存储	DS存储主机的IP地址或完全限定域名
用户名	DS命令行界面使用的名称
Password	DS命令行界面使用的密码
可执行文件dscli.exe路径	的完整路径 dscli.exe实用程序。

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
存储显示名称	IBM DS 存储阵列的名称
清单排除设备	要从清单收集中排除的设备序列号的逗号分隔列表
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
性能筛选器类型	Include： 仅从列表中的设备收集数据。Exclude： 不会从这些设备收集任何数据
性能筛选器设备列表	要从性能收集中包括或排除的设备 ID 的逗号分隔列表

IBM PowerVM数据源

IBM PowerVM (SSH)数据源收集有关在由硬件管理控制台(HMC)管理的IBM POWER硬件实例上运行的虚拟分区的信息。对于配置、此数据源需要用户名才能通过SSH登录到HMC、并需要对HMC配置具有查看级别权限。

OnCommand Insight 从 IBM PowerVM 数据源采集以下清单信息。对于 Insight 获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight 术语
hdisk	虚拟磁盘
受管系统	主机
LPAR ， VIO 服务器	虚拟机
卷组	数据存储
物理卷	LUN



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 硬件管理控制台（HMC）的 IP 地址
- 通过SSH访问HMC的用户名和密码
- 端口要求 SSH-22
- 查看所有管理系统和逻辑分区安全域的权限

用户还必须对 HMC 配置拥有查看权限，并能够为 HMC 控制台安全分组收集 VPD 信息。在逻辑分区安全分组下，还必须允许用户访问虚拟 IO 服务器命令。最好从操作员角色开始，然后删除所有角色。HMC 上的只读用户无权在 AIX 主机上运行代理命令。

- IBM 最佳实践是，让两个或更多 HMCS 监控设备。请注意，这可能是发生原因 OnCommand Insight 报告重复的设备，因此强烈建议将冗余设备添加到此数据收集器的高级配置中的 " 排除设备 " 列表中。

Configuration

* 字段 *	* 问题描述 *
硬件管理控制台(HMC)地址	PowerVM 硬件管理控制台的 IP 地址或完全限定域名
HMC 用户	硬件管理控制台的用户名
Password	硬件管理控制台使用的密码

高级配置

* 字段 *	* 问题描述 *
--------	----------

清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
SSH 端口	用于通过 SSH 连接到 PowerVM 的端口
SSH进程等待超时(秒)	SSH进程超时(默认值为600秒)
重试次数	清单重试尝试次数
排除设备	要排除的设备 ID 或显示名称的逗号分隔列表

IBM SVC数据源

IBM SVC数据源使用SSH收集清单和性能数据、支持运行SVC操作系统的各种设备。支持的设备列表包括 SVC ， v7000 ， V5000 和 V3700 等型号。有关支持的型号和固件版本、请参见Insight数据源支持列表。

术语

OnCommand Insight 从IBM SVC数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
驱动器	Disk
集群	存储
Node	存储节点
Mdisk 组	存储池
vDisk	Volume
Mdisk	后端 LUN




这些只是常见的术语映射、可能并不代表此数据源的所有情形。

清单要求

- 每个 SVC 集群的 IP 地址
- 端口 22 可用
- 您可以通过Insight生成的公共和专用密钥对、也可以重复使用SVC上已在使用的密钥对


如果要重复使用现有密钥对、则必须将其从Putty格式转换为OpenSSH格式。

- 公共密钥安装在SVC集群上
- 需要在数据源中标识私钥
- 访问验证：打开 `ssh` 使用私钥与SVC集群进行会话

 无需安装第三方软件。

性能要求

- SVC 控制台，任何 SVC 集群都必须使用此控制台， SVC 发现基础包也需要此控制台。
- 只有将性能数据文件从集群节点复制到配置节点时才需要管理访问级别。

 由于SVC基础发现包不需要此访问级别、因此SVC基础用户可能无法成功工作。

- 需要端口22
- 必须为此用户生成私有和公共SSH密钥、并存储私钥、以便可从采集单元访问。如果SVC基础用户具有适当的权限、则相同的用户和密钥将正常工作。同一SSH密钥可用于清单和性能数据。
- 通过SSH连接到SVC集群并运行以下命令来启用数据收集：`svctask startstats -interval 1`

 或者、也可以使用SVC管理用户界面启用数据收集。

说明了父级序列号

传统上、Insight可以报告存储阵列序列号或单个存储节点序列号。但是、某些存储阵列架构并不完全符合此要求。一个SVC集群可以由1-4个设备组成、每个设备都有2个节点。如果设备本身具有序列号、则该序列号既不是集群的序列号、也不是节点的序列号。

如果各个节点位于仅属于较大集群一部分的中间设备/机箱中、则存储节点对象上的"父序列号"属性会针对IBM SVC阵列正确填充。

Configuration

* 字段 *	* 问题描述 *
集群IP	SVC存储的完全限定域名的IP地址
选择 " 密码 " 或 "OpenSSH 密钥文件 " 以指定凭据类型	用于通过SSH连接到设备的凭据类型
清单用户名	SVC 命令行界面的用户名
清单密码	SVC 命令行界面的密码
清单专用密钥的完整路径	清单专用密钥文件的完整路径
性能用户名	用于收集性能的SVC命令行界面的用户名

性能密码	用于收集性能的SVC命令行界面的密码
性能专用密钥的完整路径	性能私钥文件的完整路径

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
排除设备	要从清单收集中排除的设备ID的逗号分隔列表
SSH进程等待超时(秒)	SSH进程超时(默认为200秒)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
性能排除设备	要从性能收集中排除的设备ID的逗号分隔列表
性能SSH进程等待超时(秒)	SSH进程超时(默认为200秒)
清理转储的统计信息文件	选择此选项可清除转储的统计信息文件

IBM Tivoli监控数据源

此数据源仅用于文件系统利用率。它可以直接与Tivoli监控数据库(也称为Tivoli监控数据仓库)进行通信。支持Oracle和DB2数据库。

Oracle错误消息



从OnCommand Insight 7.3.11开始、此数据收集器不再可用。

如果指定的SID导致在尝试连接时显示包含"ORA-12154"的错误消息、请仔细检查Oracle DB网络服务配置。如果访问配置指定了完全限定的主机名(例如"names.default_domain")、请尝试在SID字段中插入完全限定的服务名称。一个简单的示例是与SID的连接 `testdb` 出现故障、并且您的Oracle配置指定了的域 `company.com`。可以使用以下字符串来尝试连接、而不是使用基础SID： `testdb.company.com`。

Configuration

字段	Description
Tivoli监控数据库IP	Tivoli监控服务器的IP地址或完全限定域名
用户名	Tivoli监控服务器的用户名

Password	Tivoli监控服务器的密码
----------	----------------

高级配置

字段	Description
Tivoli监控数据库端口	用于Tivoli监控数据库的端口
Oracle SID或DB2数据库名称	Oracle侦听器服务ID或DB2数据库名称
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为60分钟)
要使用的数据库驱动程序	选择要使用的数据库驱动程序
用于连接到数据库的协议	用于连接到数据库的协议
数据库架构	输入Database Schema

IBM TotalStorage DS4000数据源

此数据源收集清单和性能信息。有两种可能的配置(固件6.x和7.x+)、它们的值相同。API收集卷数据统计信息。

Configuration

* 字段 *	* 问题描述 *
阵列SANtricity 控制器IP的逗号分隔列表	控制器的IP地址或完全限定域名、以逗号分隔

要求

- 每个 DS5 或 FAStT 阵列的 IP 地址
- 访问验证：对每个阵列上两个控制器的IP地址执行ping操作。

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为30分钟)
性能轮询间隔(最长3600秒)	性能轮询之间的时间间隔（默认值为 300 秒）

IBM XIV数据源

IBM XIV (CLI)数据源清单可使用XIV命令行界面执行。XIV性能可通过对XIV阵列进行SMI-S调用来实现、XIV阵列在端口5989上运行SMI-S提供程序。

术语

OnCommand Insight 从IBM XIV数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
存储系统	存储
存储池	存储池
Volume	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 端口要求： TCP 端口 7778
- XIV管理接口的IP地址
- 只读用户名和密码
- XIV命令行界面必须安装在Insight服务器或RAU上
- 访问验证：使用用户名和密码从Insight服务器登录到XIV用户界面。

Configuration

* 字段 *	* 问题描述 *
IP 地址	XIV存储的IP地址或完全限定域名
用户名	XIV 存储的用户名
Password	XIV 存储的密码
XIV命令行界面目录的完整路径	XIV命令行界面目录的完整路径

高级配置

* 字段 *	* 问题描述 *
--------	----------

清单轮询间隔（分钟）	两次清单轮询的间隔（默认为 40 分钟）
CLI进程等待超时(毫秒)	CLI进程超时(默认值为7200000毫秒)
SMI-S主机IP	SMI-S提供程序主机的IP地址
SMI-S端口	SMI-S Provider主机使用的端口
SMI-S 协议	用于连接到 SMI-S 提供程序的协议
SMI-S命名空间	SMI-S命名空间
Username	SMI-S Provider 主机的用户名
Password	SMI-S Provider 主机的密码
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）
SMI-S连接重试次数	SMI-S连接重试尝试次数

Infinidat InfiniBox数据源

Infinidat InfiniBox (HTTP)数据源用于从Infinidat InfiniBox存储收集信息。您必须有权访问InfiniBox管理节点。

术语

OnCommand Insight 从InfiniBox数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
驱动器	Disk
Infiniband	存储
Node	存储节点
池	存储池
Volume	Volume
FC 端口	Port

文件系统	内部卷
文件系统	文件共享
文件系统导出	共享



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

Configuration

字段	Description
InfiniBox 主机	InfiniBox 管理节点的 IP 地址或完全限定域名
用户名	InfiniBox 管理节点的用户名
Password	InfiniBox 管理节点的密码

高级配置

字段	Description
TCP 端口	用于连接到InfiniBox服务器的TCP端口(默认值为443)
清单轮询间隔 (分钟)	两次清单轮询的间隔(默认值为60分钟)
连接超时	连接超时(默认为60秒)

Microsoft Azure计算数据源

OnCommand Insights使用Azure计算数据收集器从Azure计算实例采集清单和性能数据。

要求

要配置此数据收集器，您需要以下信息：

- 端口要求： 443 HTTPS
- Azure 管理 REST IP （ management.azure.com ）
- Azure服务主体应用程序(客户端) ID (用户帐户)
- Azure服务主体身份验证密钥(用户密码)

您需要为Insight发现设置Azure帐户。正确配置帐户并在Azure中注册应用程序后、您将拥有在Insight中发现Azure实例所需的凭据。以下链接介绍了如何为发现设置帐户：<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

Configuration

根据下表在数据源字段中输入数据：

字段	Description
Azure 服务主体应用程序（客户端） ID （需要读取器角色）	登录到 Azure 的 ID 。需要读取器角色访问。
Azure 租户 ID	Microsoft 租户 ID
Azure 服务主体身份验证密钥	登录身份验证密钥
我了解 Microsoft 为 API 请求向我收费	选中此复选框可验证您是否了解 Microsoft 会为 Insight 轮询发出的 API 请求向您收费。

高级配置

根据下表在数据源字段中输入数据：

字段	Description
清单轮询间隔（分钟）	默认值为 60 。
选择 " 排除 " 或 " 包括 " 以应用于按标记筛选 VM	指定在收集数据时是包含还是排除虚拟机的按标记。如果选择"include"、则标记密钥字段不能为空。
标记要筛选 VM 的密钥和值	单击 * + Filter Tag * ，通过筛选与 VM 上的密钥和标记值匹配的密钥和值来选择要包含 / 排除的 VM （以及相关磁盘）。标记密钥为必填项，标记值为可选项。如果标记值为空，则只要虚拟机与标记密钥匹配，就会对其进行筛选。
性能轮询间隔(秒)	

Azure NetApp Files 数据源

此数据源用于获取Azure NetApp Files (ANF)的清单和性能数据。

要求

以下是配置此数据源的要求：

- 端口要求： 443 HTTPS
- Azure 管理 REST IP （ management.azure.com ）
- Azure服务主体应用程序(客户端) ID (用户帐户)
- Azure服务主体身份验证密钥(用户密码)

- 您需要为 Cloud Insights 发现设置 Azure 帐户。

正确配置帐户并在 Azure 中注册应用程序后，您将拥有在 Cloud Insights 中发现 Azure 实例所需的凭据。以下链接介绍如何设置帐户以进行发现：

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

Configuration

字段	Description
Azure服务主体应用程序(客户端) ID	登录到 Azure 的 ID
Azure 租户 ID	Azure 租户 ID
Azure 服务主体身份验证密钥	登录身份验证密钥
我了解 Microsoft 为 API 请求向我收费	选中此复选框可验证您是否了解 Microsoft 会为 Insight 轮询发出的 API 请求向您收费。

高级配置

字段	Description
清单轮询间隔（分钟）	默认值为 60 分钟

Microsoft Hyper-V数据源

在配置方面、Microsoft Hyper-V数据源需要物理主机(虚拟机管理程序)的IP地址或可解析的DNS名称。此数据源使用PowerShell (以前使用的WMI)。

术语

OnCommand Insight 从Hyper-V数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
虚拟硬盘	虚拟磁盘
主机	主机
虚拟机	虚拟机
集群共享卷（CSV），分区卷	数据存储

Internet SCSI 设备，多路径 SCSI LUN	LUN
光纤通道端口	Port



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- Hyper-V 需要打开端口 5985 ， 以便进行数据收集和远程访问 / 管理。
- 集群组节点的 IP 地址
- 虚拟机管理程序上的本地管理员用户和密码
- 管理级用户帐户
- 端口要求：对于Windows 2003及更早版本、端口135和动态TCP端口分配了1024-65535；对于Windows 2008、分配了49152-65535。
- DNS解析必须成功、即使数据收集器仅指向IP地址也是如此。
- 每个Hyper-V虚拟机管理程序必须为每个主机上的每个VM启用“资源计量”。这样，每个虚拟机管理程序就可以在每个子系统上为 Cloud Insights 提供更多数据。如果未设置此值，则为每个子系统获取的性能指标会更少。有关资源计量的详细信息，请参见 Microsoft 文档：

["Hyper-V 资源计量概述"](#)

["启用 VMResourceMetering"](#)

Configuration

* 字段 *	* 问题描述 *
物理主机 IP 地址	物理主机（虚拟机管理程序）的 IP 地址或完全限定域名
用户名	虚拟机管理程序的管理员用户名
Password	虚拟机管理程序的密码
NT 域	集群中节点使用的 DNS 名称

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
连接超时(毫秒)	连接超时(默认值为60000毫秒)

NetApp集群模式Data ONTAP 数据源

此数据源应用于使用集群模式Data ONTAP 的存储系统、并且需要一个用于只读API调用的管理员帐户。

术语

OnCommand Insight 从集群模式Data ONTAP 数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
RAID 组	磁盘组
集群	存储
Node	存储节点
聚合	存储池
LUN	Volume
Volume	内部卷



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 用于只读API调用的管理员帐户
- 目标IP是集群管理LIF
- 用户名(将ontapi应用程序的只读角色名称添加到默认SVM)和密码、用于登录到NetApp集群
- 端口要求： 80 或 443
- 许可证要求：发现所需的FCP许可证和映射/屏蔽卷

Configuration

* 字段 *	* 问题描述 *
NetApp 管理 IP	NetApp 集群的 IP 地址或完全限定域名
用户名	NetApp集群的用户名
Password	NetApp集群的密码

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

集群模式Data ONTAP 存储

适用于您在NetApp集群模式Data ONTAP 存储资产登录页面上可能找到的对象或参考的术语。

集群模式Data ONTAP 存储术语

以下术语适用于您在NetApp集群模式Data ONTAP 存储资产登录页面上可能找到的对象或参考。其中许多术语也适用于其他数据收集器。

- model—此集群中唯一的离散节点型号名称的逗号分隔列表。如果集群中的所有节点的型号类型相同，则只会显示一个型号名称。
- vendor—与配置新数据源时看到的供应商名称相同。
- serial number—阵列序列号。在NetApp集群模式Data ONTAP 等集群架构存储系统上、此序列号可能不如各个"存储节点`S`"序列号有用。
- ip—通常是数据源中配置的IP或主机名。
- 微代码版本—固件。
- 原始容量—系统中所有物理磁盘的基本2总和、而不管其角色如何。
- 延迟—表示主机在读取和写入工作负载方面所遇到的情况。理想情况下、OCI会直接获取此值、但这种情况通常不会发生。OCI通常会执行IOPs加权计算、而不是阵列提供这种计算、该计算是从各个内部卷'统计信息中得出的。
- 吞吐量—从内部卷聚合。
- 管理—此信息可能包含设备管理界面的超链接。由Insight数据源在清单报告中以编程方式创建。

集群模式Data ONTAP 存储池

适用于您在NetApp集群模式Data ONTAP 存储池资产登录页面上可能找到的对象或引用的术语。

集群模式Data ONTAP 存储池术语

以下术语适用于您在NetApp集群模式Data ONTAPstorage pool资产登录页面上可能找到的对象或引用。其中许多术语也适用于其他数据收集器。

- storage—此池所在的存储阵列。必填。
- type—从枚举的可能性列表中获取的描述性值。最常见的是`aggregate`或`RAID Group`。
- node—如果此存储阵列的架构使池属于特定存储节点、则其名称将在此处显示为指向其自己登录页面的超链接。

- 使用Flash Pool -是/否值-此基于SATA/SAS的池是否使用SSD进行缓存加速？
- 冗余—RAID级别或保护方案。RAID-DP 为双奇偶校验，raid_TP 为三重奇偶校验。
- 容量-此处的值为逻辑已用容量、可用容量和逻辑总容量以及这些容量中使用的百分比。
- 过量使用的容量—如果使用效率技术分配的卷或内部卷总容量大于存储池的逻辑容量、则此处的百分比值将大于0%。
- Snapshot—已用快照容量和总快照容量、前提是存储池架构将部分容量专用于专为快照划分的分区区域。MetroCluster 配置中的ONTAP 很可能会显示这一点、而其他ONTAP 配置则不会显示这一点。
- Utilization—一个百分比值、显示为该存储池贡献容量的任何磁盘的最高磁盘繁忙百分比。磁盘利用率不一定与阵列性能有很强的关联—如果没有主机驱动的工作负载、则由于磁盘重建、重复数据删除活动等、利用率可能会很高。此外、许多阵列的复制实施可能会提高磁盘利用率、而不会显示为内部卷或卷工作负载。
- IOPS -为该存储池贡献容量的所有磁盘的IOPS之和。
- throughput—为该存储池提供容量的所有磁盘的总吞吐量。

集群模式Data ONTAP 存储节点

适用于您在NetApp集群模式Data ONTAPs存储节点资产登录页面上可能找到的对象或参考的术语。

集群模式Data ONTAP 存储节点术语

以下术语适用于您在NetApp集群模式Data ONTAP 存储池资产登录页面上可能找到的对象或参考。其中许多术语也适用于其他数据收集器。

- storage—此节点所属的存储阵列。必填。
- HA配对节点—在某个节点将故障转移到一个和另一个节点的平台、通常会显示在此处。
- state—节点的运行状况。仅当阵列运行状况良好，足以供数据源进行资源清点时才可用。
- model—节点的型号名称。
- version—设备的版本名称。
- 序列号—节点序列号。
- memory—如果可用、则使用2个基本内存。
- 利用率—在ONTAP 上、这是一个来自专有算法的控制器压力指数。每次性能轮询都会报告一个介于 0 到 100% 之间的数字，该数字在 WAFL 磁盘争用或平均 CPU 利用率中较高。如果您观察到持续值> 50%、则表示规模不足—可能是控制器/节点不够大或旋转磁盘不足、无法承受写入工作负载。
- IOPS—直接从节点对象上的ONTAP ZAPI调用派生。
- 延迟—直接从节点对象上的ONTAP ZAPI调用派生。
- 吞吐量—直接从节点对象上的ONTAP ZAPI调用派生。
- 处理器—CPU计数。

NetApp集群模式Data ONTAP for Unified Manager数据源

此数据源从Unified Manager (UM) 6.0+数据库收集ONTAP 8.1.x数据。使用此数据源、Insight会发现UM中配置和填充的所有集群。为了提高效率、Insight不会在集群本身上

调用ZAPI。此数据源不支持性能。

Configuration



从OnCommand Insight 7.3.11开始、此数据收集器不再可用。

* 字段 *	* 问题描述 *
Unified Manager IP	Unified Manager的IP地址或完全限定域名
用户名	Unified Manager的用户名
Password	Unified Manager的密码
Port	用于与Unified Manager通信的端口(默认值为3306)

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔(最小)间隔	两次清单轮询的间隔(默认值为15分钟)
排除集群	要排除的集群IP的逗号分隔列表

在7-模式下运行的NetApp Data ONTAP 数据源

对于使用在7-模式下运行的Data ONTAP 软件的存储系统、您应使用ONTAPI数据源、该数据源使用命令行界面来获取容量编号。

术语

OnCommand Insight 从NetApp Data ONTAP 7-模式数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Disk	Disk
RAID 组	磁盘组
存储器	存储
存储器	存储节点
聚合	存储池

LUN	Volume
Volume	内部卷



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- FAS 存储控制器和配对节点的IP地址
- 端口 443
- 控制器和配对系统的用户名和密码
- 控制器和配对控制器的自定义管理员级别用户名和密码，对于 7- 模式具有以下角色功能：
 - "api-*"：使用此命令可以使 OnCommand Insight 执行所有 NetApp 存储 API 命令。
 - "login-http-admin"：使用此命令可以允许 OnCommand Insight 通过 HTTP 连接到 NetApp 存储。
 - "security-api-vfiler"：使用此命令可以使 OnCommand Insight 执行 NetApp 存储 API 命令来检索 vFiler 单元信息。
 - "cli-options"：使用此选项可读取存储系统选项。
 - "CLI-LUN"：访问这些命令以管理 LUN 。显示给定 LUN 或 LUN 类的状态（LUN 路径，大小，联机 / 脱机状态和共享状态）。
 - cli-df：使用此选项可显示可用磁盘空间。
 - cli-ifconfig：使用此命令可显示接口和 IP 地址。

Configuration

* 字段 *	* 问题描述 *
文件系统的地址	NetApp Filer的IP地址或完全限定域名
用户名	NetApp Filer的用户名
Password	NetApp Filer的密码
集群中HA配对节点文件管理器的地址	HA配对节点存储器的IP地址或完全限定域名
集群中HA配对文件管理器的用户名	NetApp HA Partner Filer的用户名
集群中 HA 配对文件存储器的密码	NetApp HA Partner Filer的密码

高级配置

* 字段 *	* 问题描述 *
--------	----------

清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
连接类型	选择连接类型
连接端口	用于 NetApp API 的端口
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

存储系统连接

除了使用此数据源的默认管理用户之外，您还可以直接在NetApp存储系统上为用户配置管理权限，以便此数据源可以从NetApp存储系统获取数据。

要连接到 NetApp 存储系统，需要在获取存储系统所在的主 pfiler 时指定的用户满足以下条件：

- 用户必须位于 vfiler0 （根存储器 /pfiler ）上。

存储系统是在采集主 pfiler 时采集的。

- 以下命令定义了用户角色功能：
 - "api-*"：使用此命令可以使 OnCommand Insight 执行所有 NetApp 存储 API 命令。要使用 ZAPI ，需要使用此命令。
 - "login-http-admin"：使用此命令可以允许 OnCommand Insight 通过 HTTP 连接到 NetApp 存储。要使用 ZAPI ，需要使用此命令。
 - "security-api-vfiler"：使用此命令可以使 OnCommand Insight 执行 NetApp 存储 API 命令来检索 vFiler 单元信息。
 - cli-options：用于 "options" 命令，用于配对 IP 和已启用许可证。
 - "cli-lun"：访问这些命令以管理LUN。显示给定 LUN 或 LUN 类的状态（ LUN 路径，大小，联机 / 脱机状态和共享状态）。
 - cli-df：用于 "df -s "， "df -r"， "df -a -r" 命令，用于显示可用空间。
 - cli-ifconfig：用于 "ifconfig -a " 命令，用于获取存储器 IP 地址。
 - cli-rdfile：用于 "rdfile /etc/netgroup" 命令，用于获取网络组。
 - cli-date：表示 date 命令，用于获取 Snapshot 副本的完整日期。
 - cli-snap：用于 "snap list" 命令，用于获取 Snapshot 副本。

如果未提供 cli-date 或 cli-snap 权限，则可以完成采集，但不会报告 Snapshot 副本。

要成功获取 7- 模式数据源并在存储系统上不生成警告，您应使用以下命令字符串之一定义用户角色。此处列出的第二个字符串是第一个字符串的简化版本：

```
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系列数据源

NetApp E系列数据源可收集清单和性能信息。有两种可能的配置（固件 6.x 和固件 7.x+），它们的值相同。

术语

OnCommand Insight 从NetApp E系列数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
驱动器	Disk
卷组	磁盘组
存储阵列	存储
控制器	存储节点
卷组	存储池
Volume	Volume



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 阵列上每个控制器的 IP 地址
- 端口要求 2463

Configuration

* 字段 *	* 问题描述 *
阵列 SANtricity 控制器 IP 的逗号分隔列表	阵列控制器的 IP 地址和 / 或完全限定域名

高级配置

* 字段 *	* 问题描述 *
--------	----------

清单轮询间隔（分钟）	两次清单轮询的间隔(默认为30分钟)
性能轮询间隔(最长3600秒)	性能轮询之间的时间间隔（默认值为 300 秒）

E系列存储

适用于您在NetApp E系列存储资产登录页面上可能找到的对象或参考的术语。

E系列存储术语

以下术语适用于您在NetApp E系列存储资产登录页面上可能找到的对象或参考。其中许多术语也适用于其他数据收集器。

- model—设备的型号名称。
- vendor—与配置新数据源时看到的供应商名称相同。
- serial number—阵列序列号。在NetApp集群模式Data ONTAP 等集群架构存储系统上、此序列号可能不如各个"存储节点`S`"序列号有用。
- ip—通常是数据源中配置的IP或主机名。
- 微代码版本—固件。
- 原始容量—系统中所有物理磁盘的基本2总和、而不管其角色如何。
- 延迟—表示主机在读取和写入工作负载方面所遇到的情况。Insight会计算从存储中的卷派生的IOPS加权平均值。
- throughput—阵列面向主机的总吞吐量。Insight会对卷的`吞吐量求和以得出此值。
- 管理—此信息可能包含设备管理界面的超链接。由Insight数据源在清单报告中以编程方式创建。

E系列存储池

适用于您在NetApp E系列存储池资产登录页面上可能找到的对象或参考的术语。

E系列存储池术语

以下术语适用于您在NetApp E系列存储池资产登录页面上可能找到的对象或参考。其中许多术语也适用于其他数据收集器。

- storage—此池所在的存储阵列。必填。
- type—从枚举的可能性列表中获取的描述性值。最常见的是"精简配置"或"RAID组"。
- node—如果此存储阵列的架构使池属于特定存储节点、则其名称将在此处显示为指向其自己登录页面的超链接。
- 使用Flash Pool -是/否值。
- 冗余—RAID级别或保护方案。E系列会报告DDP池的"RAID 7"。
- 容量-此处的值为逻辑已用容量、可用容量和逻辑总容量以及这些容量中使用的百分比。这些值都包括E系列"Preservation"容量、因此数字和百分比均高于E系列自己的用户界面显示的值。
- 过量使用的容量—如果使用效率技术分配的总卷容量大于存储池的逻辑容量、则此处的百分比值将大于

0%。

- Snapshot—已用快照容量和总快照容量、前提是存储池架构将部分容量专用于专为快照划分的分区区域。
- Utilization—一个百分比值、显示为该存储池贡献容量的任何磁盘的最高磁盘繁忙百分比。磁盘利用率不一定与阵列性能有很强的关联—如果没有主机驱动的工作负载、则由于磁盘重建、重复数据删除活动等、利用率可能会很高。此外、许多阵列的复制实施可能会提高磁盘利用率、而不会显示为卷工作负载。
- IOPS -为该存储池贡献容量的所有磁盘的IOPS之和。
- throughput—为该存储池提供容量的所有磁盘的总吞吐量。

E系列存储节点

适用于您在NetApp E系列存储节点资产登录页面上可能找到的对象或参考的术语。

E系列存储节点术语

以下术语适用于您在NetApp E系列存储池资产登录页面上可能找到的对象或参考。其中许多术语也适用于其他数据收集器。

- storage—此节点所属的存储阵列。必填。
- HA配对节点—在某个节点将故障转移到一个和另一个节点的平台、通常会显示在此处。
- state—节点的运行状况。仅当阵列运行状况良好，足以供数据源进行资源清点时才可用。
- model—节点的型号名称。
- version—设备的版本名称。
- 序列号—节点序列号。
- memory—如果可用、则使用2个基本内存。
- Utilization—当前不能为NetApp E系列提供利用率。
- IOPS -通过将专用于此节点的卷的所有IOPS相加计算得出。
- Latency—表示此控制器上的典型主机延迟或响应时间的数字。Insights会根据专用于此节点的卷计算IOPS加权平均值。
- 吞吐量-表示此控制器上主机驱动的吞吐量的数字。计算方法是将专用于此节点的卷的所有吞吐量相加。
- 处理器—CPU计数。

NetApp主机和VM文件系统数据源

您可以使用NetApp主机和VM文件系统数据源检索所有Microsoft Windows主机和VM (虚拟机)文件系统以及所有受支持的Linux VM (仅虚拟映射的VM)的文件系统详细信息和存储资源映射 位于Insight服务器中、并使用已配置的计算资源组(Compute Resource Group、CRG)进行标注。

一般要求

- 此功能必须单独购买。

您可以联系Insight代表以获得帮助。

- 您应查看Insight支持列表以验证您的主机或虚拟机操作系统是否受支持。

要验证是否已创建从文件系统到存储资源的链接、请检查相关存储或虚拟化供应商类型和版本是否报告所需的卷或虚拟磁盘标识数据。

Microsoft Windows要求

- 此数据源使用Window Management Instrumentation (WMI)数据结构来检索数据。

此服务必须正常运行且可远程访问。特别是、端口135必须可访问、如果位于防火墙后面、则必须打开。

- Windows域用户必须具有访问WMI结构的相应权限。
- 需要管理员权限。
- 为Windows 2003及更早版本分配了1024-65535的动态TCP端口
- 端口49152—65535、适用于Windows 2008



通常、在尝试在Insight、AU和此数据源之间使用防火墙时、您应咨询Microsoft团队、确定他们认为需要的端口。

Linux要求

- 此数据源使用安全Shell (SSH)连接在Linux VM上执行命令。

SSH服务必须正常运行且可远程访问。特别是、端口22必须可访问、如果位于防火墙后面、则必须打开。

- SSH用户必须具有sudo权限才能在Linux VM上执行只读命令。

您必须使用相同的密码登录到SSH并对任何sudo密码质询进行问题解答。

使用建议

- 您应使用相同的计算资源组标注为一组具有通用操作系统凭据的主机和虚拟机添加标注。

每个组都有一个此数据源的实例、用于从这些主机和虚拟机发现文件系统详细信息。

- 如果此数据源的某个实例的成功率较低(例如、OnCommand Insight 仅发现组中1000个主机和虚拟机中50个的文件系统详细信息)、 您应将成功发现的主机和虚拟机移动到单独的计算资源组中。

Configuration

字段	Description
用户名	操作系统用户、具有为Windows操作系统用户检索文件系统数据的适当权限、必须包括域前缀。
Password	操作系统用户的密码

计算资源组	用于标记数据源的主机和虚拟机的标注值将发现文件系统。空值表示数据源将发现当前未标注任何计算资源组的所有主机和虚拟机的文件系统。
-------	---

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为360分钟)

NetApp SolidFire 数据源

NetApp SolidFire 数据源支持iSCSI和光纤通道SolidFire 配置、用于清单和性能收集。

SolidFire 数据源利用SolidFire REST API。数据源所在的采集单元需要能够启动与SolidFire 集群管理IP地址上的TCP端口443的HTTPS连接。数据源需要能够在SolidFire 集群上进行REST API查询的凭据。

术语

OnCommand Insight 从NetApp SolidFire 数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
驱动器	Disk
集群	存储
Node	存储节点
Volume	Volume
光纤通道端口	Port
卷访问组， LUN 分配	卷映射
iSCSI 会话	卷掩码



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

以下是配置此数据源的要求：

- 管理虚拟 IP 地址

- 端口 443

Configuration

字段	Description
管理虚拟 IP 地址 (MVIP)	SolidFire 集群的管理虚拟 IP 地址
用户名	用于登录到 SolidFire 集群的名称
Password	用于登录到 SolidFire 集群的密码

高级配置

字段	Description
清单轮询间隔 (分钟)	两次清单轮询的间隔(默认值为60分钟)
TCP 端口	用于连接到SolidFire 服务器的TCP端口(默认值为443)
连接超时 (秒)	连接超时(默认为60秒)
性能轮询间隔 (秒)	性能轮询之间的时间间隔 (默认值为 300 秒)

故障排除

当SolidFire 报告错误时、它将显示在OnCommand Insight 中、如下所示：

```
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：

- method 是一种 HTTP 方法，例如 get 或 put 。
- parameterString> 是 REST 调用中包含的参数的逗号分隔列表。
- message> 是设备作为错误消息返回的内容。

NetApp StorageGRID 数据源

此数据源收集StorageGRID 的清单和性能数据。

要求

以下是配置此数据源的要求：

- StorageGRID 主机 IP 地址

- 分配了 Metric 查询和租户访问角色的用户的用户名和密码
- 端口 443

Configuration

字段	Description
StorageGRID 主机IP地址(MVIP)	StorageGRID 的主机IP地址
用户名	用于登录到StorageGRID 的名称
Password	用于登录到StorageGRID 的密码

高级配置

字段	Description
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为60分钟)
性能轮询间隔（秒）	性能轮询之间的时间间隔(默认值为900秒)

OpenStack数据源

OpenStack (REST API/KVM)数据源收集有关OpenStack硬件实例的信息。此数据源可收集所有OpenStack实例的清单数据、也可收集虚拟机性能数据。

要求

以下是配置OpenStack数据源的要求。

- OpenStack 控制器的 IP 地址
- 建议使用OpenStack管理员角色凭据以及对Linux KVM虚拟机管理程序的sudo访问权限。



如果您不使用管理员帐户或管理员等效权限、则仍可从数据源获取数据。您需要修改策略配置文件(例如etc/nva/policy.json)、以允许具有非管理员角色的用户调用API:

- "OS_compute_API: os-availability—zone: detail": ""
- "OS_compute_API: 操作系统虚拟机管理程序": ""
- os_compute_api: 服务器: 详细信息: get_all_tenants: ""
- 要收集性能、必须安装和配置OpenStack Ceilometer模块。可通过编辑来配置Ceilometer nova.conf 为每个虚拟机管理程序创建文件、然后在每个虚拟机管理程序上重新启动Nova Compute服务。对于不同版本的OpenStack，选项名称会发生变化：
 - Icehouse
 - 6 月

- 千克
- 自由
- Mitaka
- Newton
- Ocata
- 对于CPU统计信息、需要在计算节点上的/etc/nva/nva.conf中打开"compute_monitors=ComputeDriverCPUMonitor"。
- 端口要求
 - 对于 http 为 5000 ，对于 https 为 13000 ，对于 Keystone 服务为 13000
 - 22 表示 KVM SSH
 - 8774 用于 Nova 计算服务
 - 8776 用于 Cinder 块服务
 - 8777 ，适用于 Ceilometer 性能服务
 - 9292.用于Glance映像服务



端口绑定到特定服务、该服务可以在较大环境中的控制器或其他主机上运行。

Configuration

* 字段 *	* 问题描述 *
OpenStack 控制器 IP 地址	OpenStack 控制器的 IP 地址或完全限定域名
OpenStack 管理员	OpenStack 管理员的用户名
OpenStack 密码	OpenStack 管理员使用的密码
OpenStack 管理员租户	OpenStack 管理员租户
KVM sudo 用户	KVM sudo 用户名
选择 " 密码 " 或 "OpenSSH 密钥文件 " 以指定凭据类型	用于通过SSH连接到设备的凭据类型
清单专用密钥的完整路径	清单专用密钥的完整路径
KVM sudo 密码	KVM sudo 密码

高级配置

* 字段 *	* 问题描述 *
--------	----------

通过 SSH 启用虚拟机管理程序清单发现	选中此复选框可通过 SSH 启用虚拟机管理程序清单发现
OpenStack 管理 URL 端口	OpenStack 管理 URL 端口
使用 HTTPS	选中以使用安全 HTTP
HTTP 连接超时（秒）	HTTP连接超时(默认为300秒)
SSH 端口	用于 SSH 的端口
SSH进程等待超时(秒)	SSH进程超时(默认为30秒)
SSH 进程重试	清单重试尝试次数
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)

Oracle ZFS数据源

Oracle ZFS数据源支持清单和性能收集。

术语

OnCommand Insight 从此数据源获取以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
磁盘(SDD)	Disk
集群	存储
控制器	存储节点
LUN	Volume
LUN 映射	卷映射
启动程序、目标	卷掩码
共享	内部卷



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

以下是配置此数据源的要求：

- ZFS Controller-1 和 ZFS Controller-2 的主机名
- 管理员用户名和凭据
- 端口要求： 215 HTTP/HTTPS

Configuration

ZFS Controller-1 主机名	存储控制器 1 的主机名
ZFS Controller-2 主机名	存储控制器 2 的主机名
用户名	存储系统管理员用户帐户的用户名
Password	管理员用户帐户的密码

高级配置

字段	Description
TCP 端口	用于连接到ZFS的TCP端口(默认值为215)
连接类型	HTTP或HTTPS
清单轮询间隔	清单轮询间隔(默认为60分钟)
连接超时	默认值为60秒
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

故障排除

如果此数据收集器出现问题，请尝试执行以下操作：

问题：	请尝试以下操作：
" 登录凭据无效 "	验证 ZFS 用户帐户和密码
"配置错误"、并显示错误消息"reST Service is disabled"	验证是否已在此设备上启用 REST 服务。

"配置错误"、并显示错误消息"User unauthorized for command"	<p>可能是由于某些角色(例如、"advanced_Analytics ")不适用于已配置的用户<userName>。可能的解决方案：</p> <ul style="list-style-type: none"> 更正具有只读角色的用户\$ {user} 的分析(统计信息)范围：-在配置→用户屏幕中、将鼠标置于该角色上方并双击以允许编辑 从范围下拉菜单中选择"分析"。此时将显示可能属性的列表。 单击最上面的复选框、它将选择所有三个属性。-单击右侧的添加按钮。 单击弹出窗口右上角的应用按钮。此时将关闭弹出窗口。
---	---

Pure Storage FlashArray数据源

Pure Storage FlashArray (HTTP)数据源用于从Pure Storage Flash Array收集信息。Insight支持清单和性能收集。

术语

OnCommand Insight 从Pure Storage FlashArray数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
驱动器（SSD）	Disk
数组	存储
控制器	存储节点
Volume	Volume
Port	Port
LUN映射(主机、主机组、目标端口)	卷映射，卷掩码



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 存储系统 IP 地址
- Pure 存储系统管理员帐户的用户名和密码。
- 端口要求： HTTP/HTTPS 80/443

Configuration

* 字段 *	* 问题描述 *
FlashArray主机	FlashArray管理服务器的IP地址或完全限定域名
用户名	FlashArray管理服务器的用户名
Password	FlashArray管理服务器的密码

高级配置

* 字段 *	* 问题描述 *
连接类型	管理服务器
TCP 端口	用于连接到FlashArray服务器的TCP端口(默认值为443)
连接超时 (秒)	连接超时(默认为60秒)
清单轮询间隔 (分钟)	两次清单轮询的间隔(默认值为60分钟)
性能轮询间隔 (秒)	性能轮询之间的时间间隔(默认值为300秒)

QLogic FC交换机数据源

在配置方面、QLogic FC交换机(SNMP)数据源需要FC交换机设备的网络地址(指定为IP地址)以及用于访问此设备的SNMP_read-onium_社区字符串。

Configuration

* 字段 *	* 问题描述 *
SANSurfer交换机	SANSurfer交换机的IP地址或完全限定域名
SNMP 版本	SNMP 版本
SNMP社区	SNMP 社区字符串
用户名	SANSurfer交换机的用户名
Password	SANSurfer交换机的密码

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔(默认值为15分钟)
SNMP 身份验证协议	SNMP 身份验证协议（仅限 SNMPv3）
SNMP 重试	SNMP 重试尝试次数
SNMP 超时（毫秒）	SNMP 超时（默认为 5000 毫秒）
启用陷阱	选择以启用陷阱
陷阱之间的最短时间（秒）	陷阱触发的两次采集尝试之间的最短时间（默认值为 10 秒）
网络结构名称	数据源要报告的网络结构名称。留空以将网络结构名称报告为 WWN。
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

Red Hat (RHEV)数据源

Red Hat Enterprise Virtualization (REST)数据源通过HTTPS收集有关RHEV实例的信息。

要求

- 通过 REST API 通过端口 443 访问 RHEV-Server 的 IP 地址
- 只读用户名和密码
- RHEV3.0 及更高版本

Configuration

字段	Description
RHEV 服务器 IP 地址	RHEN服务器的IP地址或完全限定域名
用户名	RHEV-Server的用户名
Password	用于RHEV-Server的密码

高级配置

字段	Description
----	-------------

HTTPS 通信端口	用于与 RHEV-HTTPS 通信的端口
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
连接超时(秒)	连接超时(默认为60秒)

Violin Flash Memory阵列数据源

Violin 6000系列闪存阵列(HTTP)数据源可从Violin 6000系列闪存阵列收集网络信息以供分析和验证。

术语



从OnCommand Insight 7.3.11开始、此数据收集器不再可用。

OnCommand Insight 从Violin 6000系列闪存阵列数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
Violin智能内存模块(VIMM)	Disk
容器	存储
内存网关	存储节点
LUN	Volume
启动程序、启动程序组、目标	卷映射，卷掩码



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- 您需要存储的只读用户名和密码。
- 使用存储IP地址验证Web浏览器的访问。

Configuration

字段	Description
Violin内存阵列主网关的IP地址或FQDN	Violin内存阵列主网关的IP地址或完全限定域名
用户名	Violin内存阵列主网关的用户名

Password	Violin内存阵列主网关的密码
----------	------------------

高级配置

字段	Description
通信端口	用于与Violin阵列通信的端口
已启用HTTPS	选择以使用HTTPS
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
连接超时(秒)	连接超时(默认为60秒)
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

VMware vSphere数据源

VMware vSphere (Web服务)数据源收集ESX主机信息、并要求对虚拟中心内的所有对象具有_read-only_特权。

术语

OnCommand Insight 从VMware vSphere数据源采集以下清单信息。对于Insight获取的每种资产类型、均显示了此资产最常用的术语。查看此数据源或对其进行故障排除时，请记住以下术语：

供应商 / 型号术语	Insight术语
虚拟磁盘	Disk
主机	主机
虚拟机	虚拟机
数据存储	数据存储
LUN	LUN
光纤通道端口	Port



这些只是常见的术语映射、可能并不代表此数据源的所有情形。

要求

- Virtual Center 服务器的 IP 地址
- Virtual Center 中的只读用户名和密码
- 对虚拟中心内的所有对象具有只读权限。
- 在Virtual Center服务器上访问SDK
- 端口要求： HTTP-80 https-443
- 通过使用您的用户名和密码登录到Virtual Center Client并输入验证是否已启用SDK来验证访问 telnet <vc_ip\> 443。

Configuration

* 字段 *
* 问题描述 *
虚拟中心地址
虚拟中心或vSphere服务器的网络地址、指定为IP _(nnn.nnn.nnn.nnn_格式)地址或可通过DNS解析的主机名。
用户名
VMware服务器的用户名。
Password
VMware服务器的密码。

高级配置

* 字段 *	* 问题描述 *
清单轮询间隔（分钟）	两次清单轮询的间隔(默认为20分钟)
连接超时(毫秒)	连接超时(默认值为60000毫秒)
按筛选 VM	选择如何筛选VM
选择 " 排除 " 或 " 包括 " 以指定列表	指定在收集数据时是包含还是排除以下虚拟机列表
要筛选的VM列表(如果值中使用了逗号、则以逗号分隔或以分号分隔)	要在轮询中包括或排除的VM的逗号分隔或分号分隔列表
vCenter请求的重试次数	vCenter请求重试尝试次数

通信端口	用于VMware服务器的端口
性能轮询间隔（秒）	性能轮询之间的时间间隔（默认值为 300 秒）

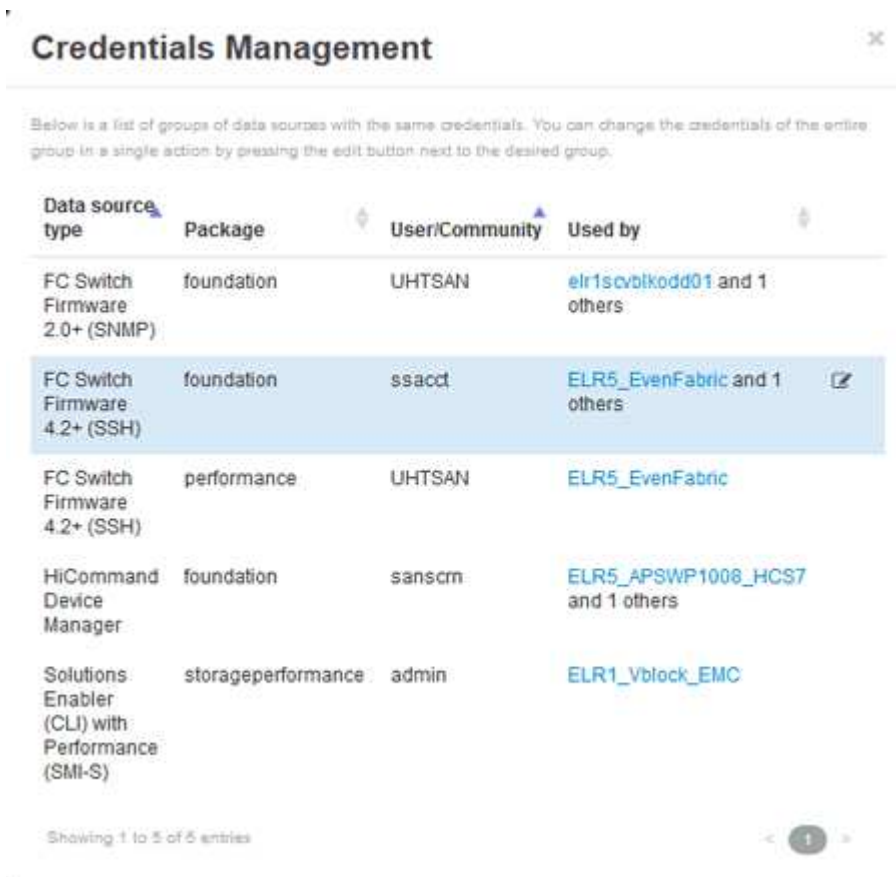
更改数据源凭据

如果同一类型的多个数据源共享用户名和密码、则可以同时更改组中所有设备的密码。

步骤

1. 在Insight工具栏上、单击*管理*。
此时将打开*数据源*列表。
2. 单击*操作*按钮并选择*更改凭据*选项。
3. 在凭据管理对话框中、从列表选择一个数据源组。

编辑图标(一张纸上的笔)将在右侧变为活动状态。



4. 单击 * 编辑 *。
5. 输入新密码并进行确认。

导致数据收集问题的更改

如果您在OnCommand Insight 中遇到数据收集问题、则环境中的更改可能是发生原因。作为一般维护规则、您还应在Insight中适应环境中的任何更改。

您可以使用此检查清单确定可能导致问题的网络更改：

- 您是否更改过任何密码？是否在Insight中更改了这些密码？
- 是否已从网络中删除设备？您还必须从OnCommand Insight 中删除此设备、以防止重新发现和重新引入此设备。
- 您是否升级了基础架构软件(例如HP CommandView EVA或EMC Solutions Enabler)？

确保采集单元上安装了相应版本的客户端工具。如果数据源故障持续存在、您需要联系技术支持以请求帮助、可能还需要获取数据源修补程序。

- 您的所有OnCommand Insight 采集单元是否都使用相同的OnCommand Insight 版本？如果远程采集单元和本地采集单元运行的OnCommand Insight 版本不同、请在所有单元上安装相同的版本以更正数据收集问题。

如果需要在所有采集单元上安装新版本的OnCommand Insight 、请转到支持站点并下载正确的版本。

- 您是否更改了任何域名或添加了新域？您必须更新设备解析(以前称为自动解析)方法。

详细检查一个数据源

如果您发现某个数据源出现故障或速度变慢、则可能需要检查该数据源的详细信息摘要、以确定问题的发生原因。需要引起注意的情况的数据源用红色实心圆圈标记。

步骤

1. 在Insight工具栏上、单击*管理*。

此时将打开*数据源*列表。列出的任何可能存在问题的数据源都用红色实心圆圈标记。最严重的问题位于列表顶部。

2. 选择引起问题的数据源。
3. 单击数据源名称链接。
4. 在数据源摘要页面上、检查以下任一部分中的信息：

- 事件时间表

列出与数据源列表中显示的当前状态相关的事件。此摘要中的事件按设备显示。错误以红色显示。您可以将鼠标指针放在时间线项目上以显示追加信息。

- 此数据源报告的设备

列出了设备的类型及其IP地址、以及指向每个设备更多详细信息的链接。

- 此数据源报告的更改(过去**3**周)

列出已添加或删除或更改配置的任何设备。

5. 检查数据源信息后、您可能需要使用页面顶部的按钮执行以下操作之一：

- *编辑*数据源的问题描述 以更正此问题。
- *再次轮询*强制轮询以确定问题是持续存在还是间歇性问题。
- *推迟*数据源轮询3天、7天或30天、以便您有时间研究问题并停止警告消息。
- *在数据源上安装修补程序*以更正此问题。
- 为技术支持准备*错误报告*。
- *从Insight监控环境中删除*数据源。

调查故障数据源

如果数据源出现"清单失败！"或"性能失败！"消息且影响较大或中等、则需要使用数据源摘要页面及其链接信息来研究此问题。

步骤

1. 单击数据源的链接*名称*以打开"摘要"页面。
2. 在摘要页面上、选中*注释*区域、以阅读可能也在调查此故障的其他工程师留下的任何注释。
3. 记下所有性能消息。
4. 如果有应用于此数据源的修补程序、请单击链接以检查*修补程序页面*以查看是否导致了此问题。
5. 将鼠标指针移动到*事件时间线*图的各个部分上以显示追加信息。
6. 选择显示在事件时间线下方的设备错误消息、然后单击消息右侧显示的*错误详细信息*图标。

错误详细信息包括错误消息的文本，最可能的原因，正在使用的信息以及可尝试更正问题的建议。

7. 在此数据源报告的设备区域中、您可以筛选列表以仅显示感兴趣的设备、并且可以单击某个设备的链接*名称*以显示该设备的_asset page_。
8. 要返回到先前显示的页面、请使用以下方法之一：
 - 单击浏览器后退箭头。
 - 右键单击后退箭头以显示页面列表、然后选择所需页面。
9. 要显示有关其他资源的详细信息、请单击其他链接名称。
10. 返回数据源摘要页面后、请查看页面底部的*更改*区域、以查看最近的更改是否导致了此问题。

控制数据源轮询

对数据源进行更改后、您可能希望它立即轮询以检查所做的更改、或者在处理问题时、您可能希望将数据源上的数据收集推迟一、三或五天。

步骤

1. 单击*管理*并导航到数据源列表视图

2. 选择要控制轮询的数据源。
3. 单击数据源名称链接。
4. 在数据源摘要页面上、检查信息并单击以下两个轮询选项之一：
 - *再次轮询*以强制数据源立即收集数据。
 - *推迟*并选择轮询延迟的时间长度、从3天、7天或30天开始。

完成后

如果您推迟了对数据源的数据收集、并希望重新启动收集、请单击摘要页面上的*恢复*。

编辑数据源信息

您可以快速编辑数据源设置信息。

步骤

1. 单击*管理*并导航到数据源列表视图
2. 找到要编辑的数据源。
3. 使用以下方法之一开始更改：
 - 单击选定数据源右侧的*编辑数据源*。
 - 单击选定数据源的链接名称、然后单击*编辑*。任一方法都会打开编辑数据源对话框。
4. 进行所需更改并单击*保存*。

编辑多个数据源的信息

您可以同时编辑同一供应商和型号的多个数据源的大部分信息。例如、如果这些数据源共享用户名和密码、则可以在一个位置更改密码、从而更新所有选定数据源的密码。

关于此任务

无法为选定数据源编辑的选项将显示为灰色或不会显示在编辑数据源对话框中。此外、如果某个选项显示的值为*混合*、则表示该选项的值在选定数据源之间有所不同。例如、如果两个选定数据源的*超时(秒)选项为*混合*、则一个数据源的超时值可能为60、而另一个数据源的值可能为90；因此、如果将此值更改为120并将更改保存到数据源、则两个数据源的超时设置均为120。

步骤

1. 单击*管理*并导航到数据源列表视图
2. 选择要修改的数据源。选定数据源必须属于同一供应商、型号和采集单元。
3. 单击*操作*按钮并选择*编辑*选项。
4. 在编辑对话框中、根据需要更改任何*设置*。
5. 单击*配置*链接以更改数据源的任何基本选项。
6. 单击*高级配置*链接可更改数据源的任何高级选项。

7. 单击 * 保存 *。

将数据源标记映射到标注

将数据源配置为轮询标记数据时、Insight会自动为与标记同名的现有Insight标注设置标注值。

如果在数据源中启用标记之前存在Insight标注、则数据源标记数据会自动添加到Insight标注中。

启用标记后创建标注时、对数据源的初始轮询不会自动更新标注。替换或填充Insight标注所需的时间有所延迟。为了避免延迟、您可以通过延迟并恢复数据源来强制标记进行标注更新。

删除数据源

如果您已从环境中删除数据源、则还必须从OnCommand Insight 监控环境中删除该数据源。

步骤

1. 在Insight工具栏上、单击*管理*。
此时将打开数据源列表。
2. 选择要删除的数据源。
3. 单击链接的数据源名称。
4. 在摘要页面上检查选定数据源的信息、以确保该数据源是您要删除的数据源。
5. 单击 * 删除 *。
6. 单击*确定*确认操作。

什么是数据源修补程序

数据源修补程序可修复现有修补程序中的问题、并使您能够轻松添加新的数据源类型(供应商和型号)。对于网络中的每种数据源类型、您可以上传数据源修补程序。您还可以安装、测试和管理修补过程。但是、对于一种数据源类型、一次只能有一个修补程序处于活动状态。

对于每个修补程序、您可以执行以下任务：

- 检查接收修补程序的每个数据源的前后比较。
- 编写注释以解释决策或总结研究结果。
- 更改对修补程序响应不佳的数据源。
- 批准要提交到Insight服务器的修补程序。
- 回滚未按预期运行的修补程序。
- 将故障修补程序替换为其他修补程序。

应用数据源修补程序

数据源修补程序会定期提供、您可以通过这些修补程序修复现有数据源的问题、为新供应商添加数据源或为供应商添加新型号。

开始之前

您必须已获取 .zip 包含最新数据源的文件 .patch 来自技术支持的文件。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*修补程序*。
3. 从"Actions"按钮中、选择*应用修补程序*。
4. 在*应用数据源修补程序*对话框中、单击*浏览*以查找 .patch 文件
5. 检查*修补程序名称*、问题描述 *和*受影响的数据源类型。
6. 如果选定的修补程序正确无误、请单击*应用修补程序*。

如果您要应用修补程序来修复数据源的问题、则同一类型的所有数据源都将使用该修补程序进行更新、您必须批准该修补程序。如果修补程序不影响任何已配置的数据源、则会自动获得批准。

完成后

如果您要应用修补程序来为新供应商或新型号添加数据源、则必须在应用修补程序后添加数据源。

在一种类型的数据源上安装修补程序

上传数据源修补程序后、您可以将其安装在同一类型的所有数据源上。

开始之前

您必须已上传要在一种类型的数据源上安装的修补程序文件。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*修补程序*。
3. 从"Actions"按钮中、选择*应用修补程序*。
4. 在*应用数据源修补程序*对话框中、单击*浏览*以查找上传的修补程序文件。
5. 检查*修补程序名称*、问题描述 *和*受影响的数据源类型。
6. 如果选定的修补程序正确无误、请单击*应用修补程序*。

同一类型的所有数据源都会使用此修补程序进行更新。

管理修补程序

您可以查看应用于网络的所有数据源修补程序的当前状态。如果要对修补程序执行操作、可以单击当前正在查看的修补程序表中的链接名称。

开始之前

您必须已上传并安装至少一个修补程序。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*修补程序*。

如果未安装任何修补程序、则当前正在查看的修补程序表为空。

3. 在*当前正在审核的修补程序*中、检查当前正在应用的数据源修补程序的状态。
4. 要检查与特定修补程序关联的详细信息、请单击此修补程序的链接名称。
5. 对于选定的修补程序、您可以单击以下任一选项对该修补程序执行下一个操作：
 - *批准修补程序*将修补程序提交到数据源。
 - *回滚*将删除此修补程序。
 - 使用*替换修补程序*、您可以为这些数据源选择其他修补程序。

提交数据源修补程序

您可以使用修补程序摘要中的信息来确定修补程序是否按预期运行、然后将修补程序提交到您的网络。

开始之前

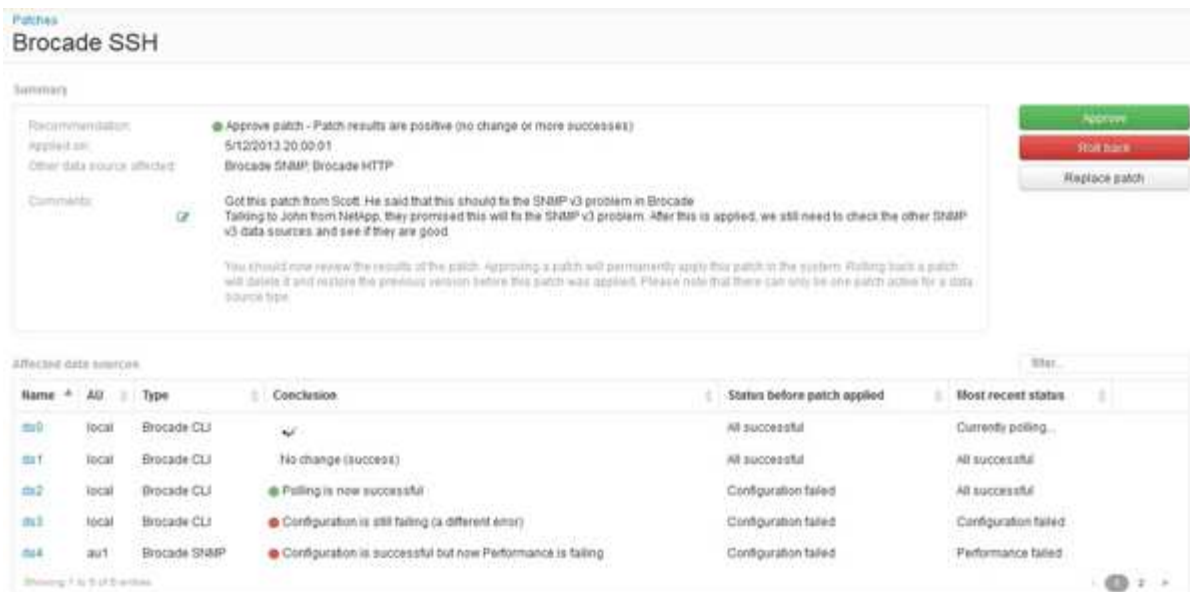
您已安装修补程序、需要确定修补程序是否成功且应获得批准。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*修补程序*。

如果未安装任何修补程序、则当前正在审核的修补程序为空。

3. 在*当前正在审核的修补程序*中、检查当前正在应用的数据源修补程序的状态。
4. 要检查与特定修补程序关联的详细信息、请单击此修补程序的链接名称。
5. 在本示例所示的修补程序摘要信息中、检查*建议*和*注释*以评估修补程序的进度。



6. 检查*受影响的数据源*表、查看修补程序前后每个受影响数据源的状态。

如果您担心要修补的某个数据源出现问题、请单击"受影响的数据源"表中的链接名称。

7. 如果您认为应将修补程序应用于此类数据源、请单击*批准*。

数据源将发生更改、修补程序将从当前正在审核的修补程序中删除。

回滚数据源修补程序

如果数据源修补程序未按预期方式运行、您可以将其回滚。回滚修补程序将删除该修补程序、并还原应用此修补程序之前的先前版本。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*修补程序*。
3. 在*当前正在审核的修补程序*中、单击看起来不成功的修补程序的链接名称。
4. 在数据源的"Patches"页面上、检查以下信息：
 - *摘要*介绍了应用修补程序的时间、受影响的数据源以及您或您的团队其他成员对修补程序的注释。
 - *受影响的数据源*列出了要修补的所有数据源、并对修补前后的状态进行了比较。
5. 要显示未成功处理修补程序的数据源的详细信息、请单击链接的*名称*。
 - a. 检查摘要信息。
 - b. 检查*事件时间线*以查看可能影响此数据源的任何配置或性能数据。
6. 如果您认为修补程序不会成功、请单击浏览器后退箭头返回到修补程序摘要页面。
7. 单击*回滚*以删除该修补程序。

如果您知道其他修补程序更有可能成功、请单击*替换修补程序*并上传新的修补程序。

设备解析

您需要发现要使用OnCommand Insight 监控的所有设备。要准确跟踪环境中的性能和清单、需要进行发现。通常、环境中的大多数设备都是通过自动设备解析来发现的。



如果您正在执行升级、并且要升级的系统中存在非活动的自动解析规则、则这些规则将在升级期间被删除。要保留非活动的自动解析规则、请在执行升级之前激活规则(选中复选框)。

安装和配置数据源后、系统将确定环境中的设备、包括交换机、存储阵列以及虚拟机管理程序和VM的虚拟基础架构。但是，这通常并不能识别您环境中的 100% 设备。

配置数据源类型的设备后、最佳实践是利用设备解析规则来帮助确定环境中其余未知设备。设备解析有助于将未知设备解析为以下设备类型：

- 物理主机
- 存储阵列
- 磁带
- 交换机

在设备解析后仍保留为“unknown”的设备被视为通用设备、您也可以在查询和信息板中显示这些设备。

然后，创建的规则将自动识别添加到环境中的具有类似属性的新设备。在某些情况下、设备解析还允许在Insight中绕过未发现设备的设备解析规则进行手动标识。

设备标识不完整可能会导致以下问题：

- 路径不完整
- 未标识的多路径连接
- 无法对应用程序进行分组
- 拓扑视图不准确
- 数据仓库和报告中的数据不准确

设备解析功能(管理>*设备解析*)包括以下选项卡、每个选项卡在设备解析规划和查看结果中都起着作用：

- “FC identify”包含未通过自动设备解析解决的光纤通道设备的WWN和端口信息列表。此选项卡还会标识已标识的设备的百分比。
- “IP identify”包含访问未通过自动设备解析进行标识的CIFS共享和NFS共享的设备列表。此选项卡还会标识已标识的设备的百分比。
- “自动解析规则”包含执行光纤通道设备解析时运行的规则列表。这些规则是您为解析未标识的光纤通道设备而创建的。
- “首选项”提供了一些配置选项、您可以使用这些选项为您的环境自定义设备解析。

开始之前

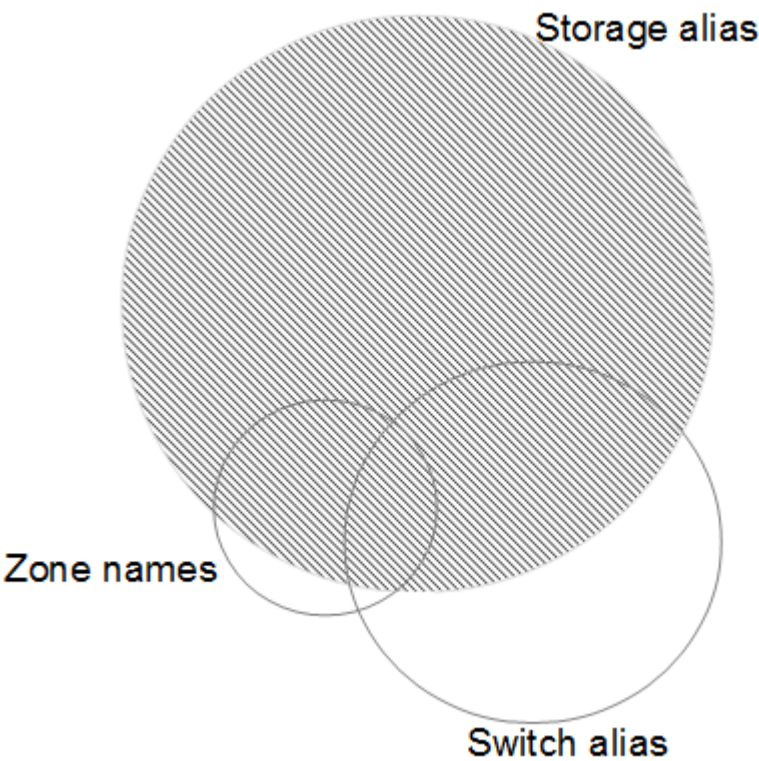
在定义用于标识设备的规则之前，您需要了解环境的配置方式。您对环境了解越多，识

别设备就越容易。

您需要问题解答回答类似于以下内容的问题，以帮助您创建准确的规则：

- 您的环境是否具有分区或主机的命名标准，其中有多少百分比是准确的？
- 您的环境是否使用交换机别名或存储别名？它们是否与主机名匹配？
- 您的环境是否使用SRM工具？您是否可以使用它来标识主机名？SRM提供哪些覆盖范围？
- 您的环境中的命名方案更改频率如何？
- 是否有任何收购或合并引入了不同的命名方案？

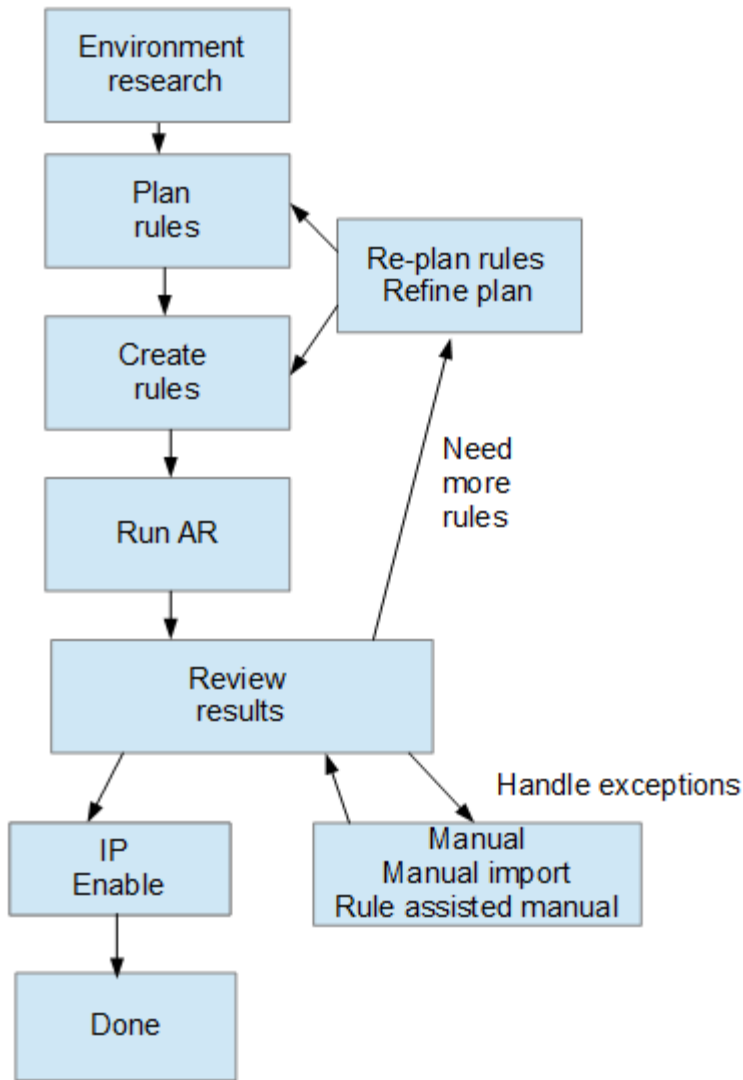
分析环境后，您应该能够确定可靠性可能会遇到哪些命名标准。您收集的信息可能会以图形方式显示在类似于下图的图中：



在此示例中，存储别名可以可靠地表示设备数量最大的情况。应首先编写用于标识使用存储别名的主机的规则，然后编写使用交换机别名的规则，最后创建的规则应使用分区别名。由于分区别名和交换机别名的使用重叠，某些存储别名规则可能会标识其他设备，从而减少了分区别名和交换机别名所需的规则。

在环境中定义设备的步骤

通常、您可以使用类似于以下内容的工作流来标识环境中的设备。标识是一个迭代过程，可能需要执行多个规划和细化规则步骤。



如果您的环境中存在未标识的设备(也称为“unknown”或通用设备)、并且随后配置了一个数据源、用于在轮询时标识这些设备、则这些设备将不再显示或计为通用设备。

为您的环境规划设备解析规则

使用规则标识环境中的设备通常是一个迭代过程、需要对环境进行全面分析、并创建多个规则来标识尽可能多的设备。最佳情形是设定一个目标、以确定您环境中100%的设备。

最有效的规则顺序是、首先放置限制性最强的规则、从而导致大多数条目不匹配模式、而过程会采用限制性较低的规则。这样、Insight就可以对每个条目应用更多模式、从而增加模式匹配和主机识别的可能性。

创建规则时、目标应是创建尽可能多的未标识设备的规则。例如、与创建30个覆盖百分比比较低的规则相比、创建覆盖模式类似于以下内容的规则的效率要高得多：

规则	覆盖百分比
规则 1.	60%

规则 2.	25%
规则 3.	8%
规则4.	4%
第5条	1%

创建设备解析规则

您可以创建设备解析规则来标识OnCommand Insight 当前未自动标识的主机、存储和磁带。您创建的规则用于标识当前环境中的设备，并在将类似设备添加到环境中时标识这些设备。

关于此任务

创建规则时，首先要确定规则所针对的信息源，用于提取信息的方法以及是否对规则结果应用 DNS 查找。

用于标识设备的源
<ul style="list-style-type: none"> • 主机的SRM别名 • 包含嵌入式主机或磁带名称的存储别名 • 包含嵌入式主机或磁带名称的交换机别名 • 包含嵌入式主机名的分区名称
用于从源提取设备名称的方法
<ul style="list-style-type: none"> • 原样(从SRM提取名称) • 分隔符 • 正则表达式
DNS 查找
指定是否使用DNS验证主机名。

您可以在自动解析规则选项卡中创建规则。以下步骤介绍了规则创建过程。

步骤

1. 单击*管理*>*设备解析*
2. 在*自动解析规则*选项卡中、单击*+添加*

此时将显示"New Rule"屏幕。



"新建规则"屏幕包含一个*? *图标、用于提供有关创建正则表达式的帮助和示例。

3. 在 * 类型 * 列表中，选择要标识的设备。

您可以选择主机或磁带。

4. 在 * 源 * 列表中，选择要用于标识主机的源。

根据您选择的源、Insight会显示以下响应：

- Zones列出了需要由Insight标识的分区和WWN。
- SRM列出了需要由Insight标识的未标识别名
- 存储别名列出了需要由Insight标识的存储别名和WWN
- 交换机别名列出了需要由Insight标识的交换机别名

5. 在 * 方法 * 列表中，选择要用于标识主机的方法。

源	方法
SRM	"as is`、""Delimiters"、"正则表达式"
存储别名	"delimiters`"或" 正则表达式"
交换机别名	"delimiters`"或" 正则表达式"
分区	"delimiters`"或" 正则表达式"

- 使用`Delimiters`的规则要求使用分隔符和主机名的最小长度。

主机名的最小长度是Insight应用于标识主机的字符数。Insight仅对长度超过此长度的主机名执行DNS查找。

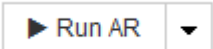
对于使用分隔符的规则，输入字符串由分隔符标记，并通过对相邻令牌进行多种组合来创建主机名候选对象列表。然后，该列表将按从大到小的顺序进行排序。例如、对于vpsnq03_hba3_emc3_12ep0、此列表将导致以下结果：

- vpsnq03_hba3_emc3_12ep0
- vpsnq03_hba3_emc3
- hba3 emc3_12ep0
- vpsnq03_hba3
- emc3_12ep0
- hba3_emc3.
- vpsnq03
- 12ep0

- emc3.
- hba3.

◦ 使用“正则表达式”的规则需要选择正则表达式、格式和区分大小写。

6.

单击  要运行所有规则、或者单击按钮中的向下箭头以运行您创建的规则(以及自上次完全运行AR以来创建的任何其他规则)。

结果

规则运行的结果将显示在FC Identify选项卡中。

启动自动设备解析更新

设备解析更新会提交自上次运行完全自动设备解析以来添加的手动更改。运行更新只能用于提交和运行对设备解析配置所做的新手动条目。不执行完整的设备解析运行。

步骤

1. 登录到Insight Web UI。
2. 单击*管理*>*设备解析*
3. 在*设备解析*屏幕中、单击*运行AR*按钮中的向下箭头。
4. 单击 * 更新 * 开始更新。

规则辅助手动标识

如果您希望运行特定规则或规则列表(无论是否一次性重新排序)来解析未知主机、存储和磁带设备或这些设备的组、则可以使用此功能。

开始之前

您有许多设备尚未标识，您也有多个规则可以成功标识其他设备。

关于此任务



如果源仅包含主机或设备名称的一部分，请使用正则表达式规则并对其进行格式化以添加缺少的文本。

步骤

1. 登录到OnCommand Insight Web UI。
2. 单击*管理*>*设备解析*
3. 单击* FC Identify"*选项卡。

系统将显示已标识和未标识的设备。

4. 选择多个未标识的设备。

5. 单击*标识*>*设置主机解析*或*>设置磁带解析*

系统将显示 "Identify" 屏幕，其中包含成功标识设备的所有规则的列表。

6. 将规则的顺序更改为满足您需求的顺序。

规则的顺序会在 "Identify" 屏幕中更改，但不会全局更改。

7. 选择满足您需求的方法。

OnCommand Insight 按照方法的显示顺序执行主机解析过程、从顶部的顺序开始。

遇到应用的规则时，规则名称将显示在规则列中，并标识为手动。

光纤通道设备解析

"FC Identify"屏幕将显示其主机尚未通过自动设备解析进行标识的光纤通道设备的WWN和WWPN。此屏幕还会显示通过手动设备解析解决的所有设备。

已通过手动解析解决的设备的状态为"OK"、并标识用于标识设备的规则。缺少的设备的状态为"Unidentified"。此页面列出了用于标识设备的总覆盖范围。

+ Add

Total coverage
30% (3/10)

FC Identify (10)

Identify Unidentify

filter...

↑

⌵

<input type="checkbox"/>	WWN	Port WWN	IP	Name	Type	Status	Rule
<input type="checkbox"/>	30:E0:00:00:00:00:00:00	10:B0:00:00:00:00:28:20	1.1.1.1	ResolvedHost1	Host	OK	Hosts by zone
<input type="checkbox"/>	30:E0:00:00:00:00:00:02	10:B0:00:00:00:00:28:22	2.2.2.2	ResolvedHost2	Host	OK	Rule deleted
<input type="checkbox"/>	30:E0:00:00:00:00:00:03	10:B0:00:00:00:00:28:23			Unknown	Unidentified	
<input type="checkbox"/>	30:E0:00:00:00:00:00:04	10:B0:00:00:00:00:28:24			Unknown	Unidentified	
<input type="checkbox"/>	30:E0:00:00:00:00:00:05	10:B0:00:00:00:00:28:25			Unknown	Unidentified	

Showing 1 to 5 of 10 entries

< 1 2 >

您可以通过在FC Identify屏幕左侧选择多个设备来执行批量操作。可以通过将鼠标悬停在某个设备上并选择列表最右侧的"Identify"或"Unidentify"按钮对单个设备执行操作。

"总覆盖范围"链接将显示您的配置的"已识别设备数/可用设备数"列表：

- SRM 别名
- 存储别名
- 交换机别名
- 分区
- 用户定义

手动添加光纤通道设备

您可以使用设备解析FC标识选项卡中提供的手动添加功能将光纤通道设备手动添加到OnCommand Insight。此过程可用于预先识别预计将来会发现的设备。

开始之前

要成功向系统添加设备标识，您需要知道 WWN 或 IP 地址以及设备名称。

关于此任务

您可以手动添加主机、存储、磁带或未知光纤通道设备。

步骤

- 1. 登录到Insight Web UI
- 2. 单击*管理*>*设备解析*
- 3. 单击* FC Identify"*选项卡。
- 4. 单击添加按钮。

此时将显示添加设备对话框

- 5. 输入 WWN 或 IP 地址，设备名称，然后选择设备类型。

结果

您输入的设备将添加到FC Identify选项卡的设备列表中。"规则"标识为"手动"。

从CSV文件导入光纤通道设备标识

您可以使用CSV文件中的设备列表手动将光纤通道设备标识导入到OnCommand Insight 设备解析功能中。

开始之前

您必须具有格式正确的CSV文件、才能将设备标识直接导入到设备解析功能中。光纤通道设备的CSV文件需要以下信息：

WWN
IP
Name
Type



作为最佳实践、建议先将FC标识信息导出到CSV文件、在该文件中进行所需的更改、然后再将该文件导回FC标识。这样可以确保所需列的存在顺序正确。

要导入FC标识信息、请执行以下操作：

步骤

1. 登录到Insight Web UI。
2. 单击*管理*>*设备解析*
3. 选择* FC Identify"*选项卡。
4. 单击*标识*>*从文件标识* .
 - a. 导航到包含要导入的CSV文件的文件夹、然后选择所需文件。

您输入的设备将添加到FC Identify选项卡的设备列表中。“规则”标识为“M手动”。

将光纤通道设备标识导出到**CSV**文件

您可以通过OnCommand Insight 设备解析功能将现有光纤通道设备标识导出到CSV文件。您可能希望导出设备标识、以便对其进行修改、然后将其导回Insight、在此可以使用它来标识与导出标识最初匹配的设备类似的设备。


关于此任务

如果设备具有类似的属性、可以在CSV文件中轻松编辑这些属性、然后将其导回系统、则可能会出现这种情况。

将光纤通道设备标识导出到CSV文件时、该文件将按所示顺序包含以下信息：

WWN
IP
Name
Type

步骤

1. 登录到Insight Web UI。
2. 单击*管理*>*设备解析*
3. 选择* FC Identify"*选项卡。
4. 选择要导出其标识的一个或多个光纤通道设备。
5. 单击导出  图标。
6. 选择是要打开CSV文件还是保存该文件。

IP 设备解析

"IP Identify" 屏幕将显示通过自动设备解析或手动设备解析标识的任何 iSCSI 和 CIFS 或 NFS 共享。此外，还会显示未标识的设备。此屏幕包括设备的 IP 地址，名称，状态，iSCSI 节点和共享名称。此外，还会显示已成功标识的设备的百分比。

+Add

Total coverage
20% (2/10)

IP identify (10)

Identify

Unidentify

filter...

↑

☰

<input type="checkbox"/>	Address	IP	Name	Status	iSCSI node	Share name
<input type="checkbox"/>	1.1.1.1	1.1.1.1	LA3-CNS-SQL-06A	OK		/vol/ServerLogs_STG/
<input type="checkbox"/>	0.0.0.0/0					/vol/ServerLogs_STG/
<input type="checkbox"/>	10.56.100.18				iqn.1991-05.com.microsoft:la3-cns-sql-06b.cns.comcastnets.com	
<input type="checkbox"/>	10.56.100.19				iqn.1991-05.com.microsoft:jec20643597717.tfayd.com	/vol/wc_sc_libraries_prod/libraries_qtree/
<input type="checkbox"/>	100.54.18.100	100.54.18.100	ushapl000961b	OK		

Showing 1 to 5 of 10 entries

< 1 2 >

手动添加 IP 设备

您可以使用"IP Identify"屏幕中提供的手动添加功能将IP设备手动添加到OnCommand Insight。

步骤

- 1. 登录到Insight Web UI。
- 2. 单击*管理*>*设备解析*
- 3. 单击* IP Identif*选项卡。
- 4. 单击添加按钮。

此时将显示添加设备对话框

- 5. 输入地址， IP 地址和唯一设备名称。

结果

您输入的设备将添加到"IP Identify"选项卡的设备列表中。

从CSV文件导入IP设备标识

您可以使用CSV文件中的设备标识列表将IP设备标识手动导入到设备解析功能中。

开始之前

要导入设备标识、您必须具有格式正确的CSV文件。IP设备的CSV文件需要以下信息：

Address
IP
Name

作为最佳实践、建议先将IP标识信息导出到CSV文件、在该文件中进行所需的更改、然后再将该文件导回IP标识。这样可以确保所需列的存在顺序正确。

要导入IP Identify信息、请执行以下操作：

步骤

- 1. 登录到Insight Web UI。
- 2. 单击*管理*>*设备解析*
- 3. 选择* IP Identify"*选项卡。
- 4. 单击*标识*>*从文件标识* .
 - a. 导航到包含要导入的CSV文件的文件夹、然后选择所需文件。

您输入的设备将添加到"IP Identify"选项卡的设备列表中。

将IP设备标识导出到CSV文件


您可以使用设备解析功能从Insight导出现有IP设备标识。您可能希望导出设备标识、以便对其进行修改、然后将其导回Insight、以便可以使用它来标识与导出标识中的设备类似的设备。

关于此任务

将IP设备标识导出到CSV文件时、该文件将按所示顺序包含以下信息：

Address
IP
Name

步骤

- 1. 登录到Insight Web UI。
- 2. 单击*管理*>*设备解析*
- 3. 选择* IP Identify"*选项卡。
- 4. 选择要导出其标识的 IP 设备。
- 5. 单击导出  图标。
- 6. 选择是要打开CSV文件还是保存该文件。

设置首选项选项卡中的选项

通过设备解析首选项选项卡，您可以创建自动解析计划，指定要在标识中包含或排除的存储和磁带供应商，以及设置 DNS 查找选项。

自动解析计划

自动解析计划可以指定何时运行自动设备解析：

选项	Description
每	使用此选项可以按天，小时或分钟的间隔运行自动设备解析。
每天	使用此选项可在特定时间每天运行自动设备解析。
手动	使用此选项只能手动运行自动设备解析。
环境发生变化时	使用此选项可在环境发生变化时运行自动设备解析。

如果手动指定、则会禁用夜间自动设备解析。


DNS 处理选项

您可以通过 DNS 处理选项选择以下功能：

- 启用 DNS 查找结果处理后，您可以添加 DNS 名称列表以附加到已解析的设备。
- 您可以选择"Auto resolution of IPs: ""、以便使用DNS查找为访问NFS共享的iSCSI启动程序和主机启用自动主机解析。如果未指定此参数，则仅执行基于 FC 的解析。
- 您可以选择在主机名中使用下划线，并在结果中使用 "connected to" 别名，而不是标准端口别名。

包括或排除特定存储和磁带供应商

您可以包括或排除特定的存储和磁带供应商以进行自动解析。例如，如果您知道某个特定主机将成为旧主机并应从新环境中排除，则可能需要排除特定供应商。您还可以重新添加先前已排除但不再希望排除的供应商。



磁带的设备解析规则仅适用于WWN、其中此WWN的供应商在供应商首选项中设置为*仅包含为磁带*。

正则表达式示例

如果您选择正则表达式方法作为源命名策略、则可以使用正则表达式示例作为在OnCommand Insight 自动解析方法中使用的表达式的参考。

设置正则表达式的格式

在为OnCommand Insight 自动解析创建正则表达式时、您可以通过在名为的字段中输入值来配置输出格式 FORMAT。

默认设置为 \1、表示与正则表达式匹配的分区名称将替换为正则表达式创建的第一个变量的内容。在正则表达式中，变量值由括号语句创建。如果出现多个括号语句，则变量将从左到右以数字形式引用。这些变量可以按任意顺序以输出格式使用。通过将常量文本添加到、也可以在输出中插入常量文本 FORMAT 字段。

例如，根据此分区命名约定，您可能具有以下分区名称：

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

- S123_Miami_hostname1_filer_fc1
- S14_Tampa_hostname2_switch_FC4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_solaris FC1

您可能希望输出采用以下格式：

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

为此，您需要捕获变量中的主机名，数据中心和设备类型字段，并在输出中使用它们。以下正则表达式将执行此操作：

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

由于有三组圆括号、因此可以使用变量 \1， \2 和 \3 将填充。

然后，您可以使用以下格式以首选格式接收输出：

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

您的输出如下所示：

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

变量之间的连字符提供了一个在格式化输出中插入的常量文本示例。

显示分区名称的示例 1

在此示例中，您可以使用正则表达式从分区名称中提取主机名。如果您具有类似于以下分区名称的内容，则可以创建正则表达式：

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

可用于捕获主机名的正则表达式为：

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

结果将匹配以 S 开头的分区，后跟任意数字组合，下划线，字母数字主机名（myComputer1Name），下划线或连字符，大写字母 HBA 和单个数字（0-9）。主机名单独存储在 *。\\1* 变量中。

正则表达式可以分为以下几个部分：

- "s" 表示分区名称并开始表达式。这仅与分区名称开头的 "S" 匹配。
- 方括号中的字符 [0-9] 表示 "S" 后面的数字必须介于 0 到 9 之间（包括 0 到 9）。
- 符号 + 表示前面括号中的信息必须存在 1 次或更多次。
- （下划线）表示 S 后面的数字必须紧跟在分区名称中只有下划线字符。在此示例中，分区命名约定使用下划线将分区名称与主机名分隔开。
- 在所需下划线之后，圆括号表示中包含的模式将存储在 \\1 变量中。
- 括号内的字符 [a-zA-Z0-9] 表示要匹配的字符全部为字母（无论大小写如何）和数字。
- 方括号后面的 *（星号）表示括号内的字符出现 0 次或更多次。
- 带括号的字符（下划线和短划线）表示字母数字模式后面必须有以下划线或短划线。
- 正则表达式中的字母 HBA 表示分区名称必须包含此字符序列。
- 最后一组带括号的字符 [0-9] 与 0 到 9 之间的一个数字（包括 0 到 9）匹配。

示例 2.

在此示例中，跳到第一个下划线 ""，然后将 E 以及此后的所有内容匹配到第二个 ""，然后跳过之后的所有内容。

分区： Z_E2FHDBS01_E1NETAPP

主机名： E2FHDBS01

注册时间： .?(E.?).*?

示例 3

正则表达式（下方）最后一部分的圆括号（）用于标识主机名的部分。如果希望 VSAN3 成为主机名，则应为：_([a-zA-Z0-9])。*

分区： A_VSAN3_SR48KENT_A_CX2578_SPA0

主机名： SR48KENT

注册时间： _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

示例 4 显示了一个更复杂的命名模式

如果您具有类似于以下分区名称的内容，则可以创建正则表达式：

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

可用于捕获这些数据的正则表达式如下：

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

。 \1 变量只能包含 myComputerName123 使用此表达式求值后。

正则表达式可以分为以下几个部分：

- 圆括号表示中包含的模式将存储在 \1 变量中。
- 括号内的字符 [a-zA-Z0-9" 表示任何字母（无论大小写）或数字都匹配。
- 方括号后面的 *（星号）表示括号内的字符出现 0 次或更多次。
- 正则表达式中的 _（下划线）字符表示分区名称必须与前面的方括号匹配的字母数字字符串后面紧跟一个下划线。
- 。 （句点）匹配任意字符（通配符）。
- （星号）表示前一句点通配符可能出现 0 次或更多次。

换言之，组合 .* 表示任意字符，任意次数。

示例 5：显示无模式的分区名称

如果您具有类似于以下分区名称的内容，则可以创建正则表达式：

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

可用于捕获这些数据的正则表达式如下：

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

1 变量将包含 myComputerName（在第一个分区名称示例中）或 myComputerName123（在第二个分区名称示例中）。因此，此正则表达式将与第一个下划线之前的所有内容匹配。

正则表达式可以分为以下几个部分：

- 圆括号表示中包含的模式将存储在 \1 变量中。
- *（句点星号）可匹配任意字符，任意次数。

- 方括号后面的 *（星号）表示括号内的字符出现 0 次或更多次。
- 。字符使匹配成为非聚合。这会强制其在第一个下划线处停止匹配，而不是在最后一个下划线处停止匹配。
- 字符 `_*` 与找到的第一个下划线及其后面的所有字符匹配。

示例 6：显示具有模式的计算机名称

如果您具有类似于以下分区名称的内容，则可以创建正则表达式：

- `storage1_Switch1_myComputerName123A_A1_FC1`
- `Storage2_Switch2_myComputerName123B_A2_FC2`
- `Storage3_Switch3_myComputerName123T_A3_FC3`

可用于捕获这些数据的正则表达式如下：

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

由于分区命名约定包含更多模式，因此我们可以使用上述表达式，该表达式将匹配以 A，B 或 T 结尾的主机名（示例中为 `myComputerName`）的所有实例，并将该主机名置于 \1 变量中。

正则表达式可以分为以下几个部分：

- *（句点星号）可匹配任意字符，任意次数。
- 。字符使匹配成为非聚合。这会强制其在第一个下划线处停止匹配，而不是在最后一个下划线处停止匹配。
- 下划线字符与分区名称中的第一个下划线匹配。
- 因此、第一个 `. *? _` 组合与第一个分区名称示例中的字符 `_storage1_` 匹配。
- 第二个 `. *? _` 组合的行为与第一个类似、但与第一个分区名称示例中的 `_Switch1_` 匹配。
- 圆括号表示中包含的模式将存储在 \1 变量中。
- 括号内的字符 `[a-zA-Z0-9]` 表示任何字母（无论大小写）或数字都匹配。
- 方括号后面的 *（星号）表示括号内的字符出现 0 次或更多次。
- 正则表达式（`ABT`）中的括号字符与分区名称中的一个字符匹配，该字符必须为 A，B 或 T
- 圆括号后面的 `_`（下划线）表示必须在下划线后面加上一个字符匹配项。
- *（句点星号）可匹配任意字符，任意次数。

因此，此操作的结果将使 \1 变量发生原因为包含以下任意字母数字字符串：

- 前面有一定数量的字母数字字符和两个下划线
- 后面是下划线（然后是任意数量的字母数字字符）
- 在第三个下划线之前，最后一个字符为 A，B 或 T。

示例 7

分区：`myComputerName123_HBA1_Symm1_FA1`

主机名: myComputerName123

注册时间: ([a-zA-Z0-9]+)_.*

示例 8

此示例将查找第一个 _ 之前的所有内容。

分区: MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

主机名: MyComputerName

注册时间: (.?)_.

示例9

此示例将查找第一个 _ 到第二个 _ 之后的所有内容。

分区: Z_MyComputerName_StorageName

主机名: MyComputerName

注册时间: .?(.?).*?

示例 10

此示例从分区示例中提取 MyComputerName123 。

分区: Storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

主机名: MyComputerName123

注册时间: .??.?([a-zA-Z0-9]+) [ABT]_.

示例 11

分区: Storage1_Switch1_MyComputerName123A_A1_FC1

主机名: MyComputerName123A

注册时间: .??.?([a-zA-z0-9]+).*?

示例 12

{caret} (周长或记号)*内方括号*将否定表达式、例如、 { {caret} FF}表示大写或小写F以外的任何内容、而 {

{caret} a-z表示小写a到z以外的所有内容、在上述情况下、除_以外的任何内容。format 语句将 "-" 添加到输出主机名中。

分区: mhs_apps44_d_A_10a0_0429

主机名: mhs-apps44-d

注册时间: ([^_])_([AB]).*+OnCommand Insight 中的格式:

([^_])_().*+OnCommand Insight 中的格式:

示例 13

在此示例中, 存储别名以 "\" 分隔, 表达式需要使用 "\\" 来定义字符串中实际正在使用 "\", 而这些字符串不属于表达式本身。

存储别名: \Hosts\E2DOC01C1\E2DOC01N1

主机名: E2DOC01N1

注册时间: \\.\.?\\.\.?\\ (.*)

示例 14

此示例从分区示例中提取了 "PD-RV-W-AD-2" 。

分区: PD_D-PD-RV-W-AD-2_01

主机名: PD-RV-W-AD-2

注册时间: [^_]-(-\d+).+

示例 15

在这种情况下, 格式设置会将 "US-BV-" 添加到主机名中。

分区: SRV_USBVM11_F1

主机名: US-BV-M11

注册时间: SRV_USBV([A-Za-z0-9]+)_F[12]

格式: US-BV-\1

维护Insight

无论您是Insight的新用户、要设置新系统、还是您的系统已运行一段时间、您都必须采取措施来保持Insight和您的网络平稳运行。维护的主要概念是、通常需要在Insight中适应网络的变化。

以下是最常见的维护任务：

- 维护Insight备份
- 更新已过期的Insight许可证
- 协调数据源修补程序
- 更新所有采集单元上的Insight版本
- 从Insight中删除已删除的数据源

管理Insight

OnCommand Insight 可监控您的环境、使您能够在报告危机之前研究潜在问题。资产信息板提供汇总饼图、IOPS热图以及利用率最高的10个存储池的交互式图表。

步骤

1. 打开Insight*资产信息板*、将光标移动到饼图上以检查这三个图表中的资产分布：
 - Capacity by Vendor显示每个供应商的存储总原始容量。
 - Capacity by Tier显示每个存储层的总可用容量。
 - 交换机端口饼图显示了端口的制造商、并显示了已用端口的百分比。
2. 查看*有关您的环境的事实*、查看有关您环境的已用容量、容量效率、已用FC资源以及虚拟基础架构统计信息的信息。
3. 将光标置于*已利用的前10个池*图表中的存储池条上、可查看存储池的已用容量和未用容量。
4. 单击*存储IOP*热图中以大文本格式显示的任何资产名称(表示资产存在问题)、以显示一个页面、其中汇总了该资产的当前状态。
5. 在*资产信息板*的右下角、单击*虚拟机IOPS*热图中以大文本格式显示的任何资产名称(表示资产存在问题)、以显示一个汇总资产当前状态的页面。
6. 在Insight工具栏上、单击*管理*。
7. 记下显示红色实心圆的任何区域。

在OnCommand InsightWeb UI中、潜在问题会用红色实心圆圈标记。

8. 单击*数据源*以检查所有受监控数据源的列表。

检查包含带有红色实心圆的消息且*影响*列为"高"或"中"的*状态*列的任何数据源。这些信息位于表的顶部。这些数据源的问题会影响您的大部分网络、您需要解决这些问题。

9. 单击*采集单元*以记下运行Insight的每个IP地址的状态、并根据需要重新启动采集单元
10. 单击*运行状况*可查看Insight服务器的高级实例监控。

监控OnCommand Insight 系统运行状况

您应通过查看运行状况页面定期检查Insight系统组件的当前状态、该页面会显示每个组件的状态、并在存在问题描述 时向您发出警报。

步骤

1. 登录到InsightWeb UI。
2. 单击*管理*并选择*运行状况*。

此时将显示"运行状况"页面。

3. 查看组件的当前状态摘要、尤其要注意前面带有红色圆圈的*详细信息*列中的任何注意状态、该圆圈表示需要立即引起关注的问题描述。

"运行状况"页面根据您的系统配置显示以下任意或所有Insight组件的信息：

组件	测试	详细信息	显示
采集	清单数据处理	本地采集单元的状态	如果并发轮询数据源的数量小于执行池最大值的75%(默认最大值为30)、则为"OK"。如果使用率大于75%、则为"Acquisition is busy"、建议增加轮询间隔或添加更多远程采集单元。
DWH	备份	数据仓库计划备份的状态	如果启用了DWH计划备份、则显示"OK"和上次成功的DWH备份时间。否则、将显示有关发现的任何错误的信息。
DWH	ETL	数据仓库ETL的状态	"正常"和上次成功的DWH构建时间(如果没有错误)。否则、将显示有关发现的任何错误的信息。
服务器	ASUP	ASUP的状态	<p>"ASUP Enabled"和上次成功的自动通报时间(如果可用)。如果已启用自动通报、但遇到问题、则显示"ASUP Failed"。</p> <p>如果备份目录无效、则+"备份位置无效"。</p> <p>+显示上次成功的自动通报时间以及上次失败尝试的时间(如果可用)。</p> <p>如果已禁用自动通报、则+"ASUP Disabled"。</p>

服务器	自动解析	自动设备解析的状态	<p>如果没有错误、则显示"OK"。如果标识错误阻止解决进度、则显示"Auto resolution is blocked"。</p> <p>+“低成功率”、前提是可以识别不到75%的通用设备。</p>
服务器	Elasticsearch	弹性搜索数据存储的状态	<p>如果没有错误、则显示"OK"。如果无法连接到弹性搜索服务、则显示"服务不可用's"。</p> <p>如果检测到多个节点、则+"检测到集群模式"。</p> <p>如果已用堆空间超过85%、则+"高内存利用率"。</p> <p>+“状态：红色”表示弹性搜索报告的错误。显示有关此错误的信息、并建议联系客户支持。</p>
服务器	CPU	Insight CPU使用情况	<p>如果CPU负载小于65%、则为"正常"。"sCPU负载较高。降低CPU负载。" CPU负载大于65%。</p>
服务器	磁盘空间	磁盘空间的状态	<p>可用磁盘空间、Insight正在使用的磁盘空间以及建议为Insight预留的磁盘空间。如果磁盘利用率超过80%、则为"磁盘空间不足"。</p>
服务器	EventBus	EventBus的状态	<p>如果EventBus队列为空、则为"EventBus is empty"、否则将显示EventBus队列的状态。</p>

服务器	清单数据处理	Insight服务器清单数据处理功能的状态	如果Insight服务器不繁忙、则显示“OK”。如果服务器在过去一小时中至少有75%的时间处于繁忙状态、则显示“server is busy”。建议不要添加更多数据源、并建议将环境拆分为多个服务器。
服务器	MySQL	MySQL数据库的状态	<p>如果未检测到问题、则显示“OK”。“数据库存在性能问题。如果较慢的查询数超过5%、则某些查询运行时间过长”。</p> <p>+“数据库日志文件在过去一小时内的增长超过了<size>。如果错误日志增长到20 KB以上、请检查MySQL日志文件”。</p>
服务器	性能归档	性能归档的状态	“性能归档已启用”或“性能归档未启用”。
服务器	物理内存	物理内存的状态	如果内存使用率低于85%、则为“正常”。“内存使用率很高。如果内存使用率超过85%、请减少整体内存占用空间以确保系统稳定性”。
服务器	服务包	Service Pack可用性	显示是否有可用于Insight的Service Pack。如果有可用的Service Pack、则显示相关说明。
服务器	使用情况信息	发送使用情况信息的状态	<p>显示是启用还是禁用向NetApp发送使用情况信息。如果已禁用、建议启用。显示上次尝试发送的时间或上次成功发送的时间。</p> <p>+显示有关遇到的任何问题的信息。</p>

服务器	违规	未处理违规的状态	<p>如果未处理的违规数量小于违规限制的75%、则为"OK"。如果未解决的违规数超过违规限制的75%、则`m允许的最大未解决违规数为<number>`。建议查看性能策略配置。</p> <p>如果未处理的违规数量达到违规限制、则+“Violation manager is blocked”。</p> <p>+请注意、违规管理器无法创建新的违规、因此建议查看性能策略配置。</p>
服务器	每周备份	每周备份的状态	<p>如果启用了每周备份、则会显示"正常"、否则显示"未启用每周备份"。</p>

删除非活动设备

删除处于非活动状态的设备有助于保持数据更干净、更易于导航。

关于此任务

要从Insight中删除非活动设备、请执行以下操作：

步骤

1. 创建新查询或打开现有查询。
2. 选择`_generic device_`、`host`、`storage`、`_switch_`或`tape_asset`类型。
3. 为*处于活动状态*添加一个筛选器、并将此筛选器设置为*否*。

结果表仅显示非活动资产。

4. 选择要删除的设备。
5. 单击*操作*按钮并选择*删除非活动设备*。

您的非活动设备将被删除、并且将不再显示在Insight中。

审核系统和用户活动

如果要查找意外更改、可以查看OnCommand Insight 系统及其用户活动的审核跟踪。除了

显示在Audit页面上之外、还可以选择将审核日志消息发送到系统日志。

关于此任务

Insight会为影响存储网络或其管理的任何用户活动生成审核条目、包括以下内容：

- 登录
- 授权或取消授权路径
- 正在更新授权路径
- 设置全局策略或阈值
- 添加或删除数据源
- 启动或停止数据源
- 正在更新数据源属性
- 添加，编辑或删除任务
- 删除应用程序组
- 确定或更改设备的标识
- 创建用户
- 删除用户
- 用户角色更改
- 修改用户(来宾 à 管理员)
- 用户注销(强制注销或手动注销)
- 删除采集单元
- 更新许可证
- 启用备份
- 正在禁用备份
- 启用ASUP (审核日志报告在同一页面上启用代理)
- 禁用ASUP (审核日志中报告了在同一页面上禁用代理)
- 安全性—重新设置密钥、更改系统密码。
- 删除/添加资产上的标注
- CAC用户登录/注销
- CAC用户会话超时

步骤

1. 在浏览器中打开Insight。
2. 单击*管理*并选择*审核*。

"Audit "页面将在表中显示审核条目。

3. 您可以在此表中查看以下详细信息：

◦ * 时间 *

进行更改的日期和时间

◦ * 用户 *

与审核条目关联的用户的名称

◦ * 角色 *

用户帐户的角色、即来宾、用户或管理员

◦ * IP *

与审核条目关联的IP地址

◦ * 操作 *

审核条目中的活动类型

◦ * 详细信息 *

审核条目的详细信息

如果存在影响资源的用户活动、例如数据源或应用程序、则详细信息将包含指向资源登录页面的链接。



删除数据源后、与数据源相关的用户活动详细信息不再包含指向数据源登录页面的链接。

4. 您可以通过选择特定时间段(1小时、3小时、24小时、3天和7天)来显示审核条目。 Insight在选定时间段内最多显示1000个违规。

如果单个页面上的数据太多、您可以单击表下方的页码按页浏览数据。

5. 您可以通过单击列标题中的箭头将表中列的排序顺序更改为升序(向上箭头)或降序(向下箭头)；要返回到默认排序顺序、请单击任何其他列标题。

默认情况下、此表按降序显示条目。

6. 您可以使用*筛选器*框仅显示表中所需的条目。

仅查看用户的审核条目 izzyk、键入 izzyk 在*筛选器*框中。

监控网络中的违规



当Insight因性能策略中设置的阈值而生成违规时、您可以使用违规信息板查看这些违规。信息板列出了网络中发生的所有违规、并可用于查找和解决问题。

步骤

1. 在浏览器中打开OnCommand Insight。
2. 在Insight工具栏上、单击*信息板*并选择*违规信息板*。

此时将显示违规信息板。



3. 可以通过以下方式使用*按策略划分的违规*饼图：

- 您可以将光标置于图表的任何部分上方、以显示特定策略或指标发生的违规总数的百分比。
- 您可以单击图表的一个分区以“放大”它、这样、您可以将该分区从图表的其余部分移开、从而更加仔细地强调和研究该分区。
- 您可以单击  图标以全屏模式显示饼图、然后单击  再次尝试将饼图最小化。一个饼图最多可包含五个扇区；因此、如果您有六个策略生成违规、Insight会将第五个和第六个扇区合并为“Others”扇区。Insight会为第一个分区分配最多的违规、为第二个分区分配第二多的违规、依此类推。

4. 您可以通过以下方式使用*违规历史记录*图表：


- 您可以将光标置于图表上方、以显示特定时间发生的违规总数以及每个指定指标发生的违规总数。
- 您可以单击图例标签以从图表中删除与图例关联的数据。

单击该图例可再次显示数据。

- 您可以单击  图标以全屏模式显示图表、然后单击  再次尝试将饼图最小化。

5. 您可以通过以下方式使用*违规表*：

- 您可以单击  图标以全屏模式显示此表、然后单击  再次尝试将饼图最小化。


如果窗口大小太小、则违规表仅显示三列；但是、在单击时 、将显示其他列(最多七列)。

- 您可以显示特定时间段(* 1小时*、* 3小时*、* 24小时*、* 3天*、* 7天*、和* 30 d*)、Insight显示选定时间段内最多1000个违规。
- 您可以使用*筛选器*框仅显示所需的违规。
- 您可以通过单击列标题中的箭头将表中列的排序顺序更改为升序(向上箭头)或降序(向下箭头)；要返回到默认排序顺序、请单击任何其他列标题。

默认情况下、此表按降序显示违规。

- 您可以在ID列中单击违规、以显示违规期间的资产页面。
- 您可以单击问题描述 列中的资源链接(例如、存储池和存储卷)以显示与这些资源关联的资产页面。
- 您可以单击策略列中的性能策略链接以显示编辑策略对话框。

如果您认为某个策略生成的违规太少或太多、则可能需要调整该策略的阈值。

- 如果单个页面上的数据太多、则可以单击页码按页浏览数据。
- 您可以单击  以消除违规。

采集单元状态

Acquisition Unit屏幕可显示所有采集单元的视图、包括状态和存在的任何错误。

连接到服务器的Insight采集单元的状态显示在*管理*>*采集单元*表中。此表显示了每个采集单元的以下信息：

- * 名称 *
- * IP *
- *状态*是采集单元的运行状态。
- 上次报告的时间*显示连接到采集单元的数据源上次报告的时间。
- *注释*显示用户输入的与AU相关的注释。

如果列表中的采集单元出现问题、则状态字段将显示一个红色圆圈、其中包含有关问题的简要信息。您应调查任何采集单元问题、因为它们可能会影响数据收集。

要重新启动采集单元、请将鼠标悬停在该单元上、然后单击显示的_Restart Acquisition Unit"按钮。

要添加文本注释、请将鼠标悬停在采集单元上、然后单击显示的_Add Note_按钮。仅显示最近输入的注释。

还原Insight数据库

要从经验证的备份文件还原Insight数据库、请使用Troubleshooting选项。此操作将完全替换当前的OnCommand Insight 数据。

开始之前

最佳实践：*在还原OnCommand Insight 数据库之前、请使用手动备份过程创建当前数据库的副本。检查计划还原的备份文件、确保该备份成功、其中包含要还原的文件。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*故障排除*。

Send / Collect data

Action	Description
<input type="button" value="Back up"/>	Back up the database (configuration and performance) into a ZIP file.
<input type="button" value="Bundle logs"/>	Collect all log files (including acquisition recordings) and bundle them into a ZIP file. Can be used to send data back to NetApp support when troubleshooting an issue with the software.
<input type="button" value="Send ASUP now"/>	Forces an ad-hoc ASUP report. Can be used to allow NetApp support to get the latest support data when troubleshooting an issue with the software.

Restore a database

Warning: Your current database will be discarded!

Other tasks

Couldn't find what you are looking for? Connect to the old [OnCommand Insight Portal](#).
Need to send anonymous data back? Open the [scrub utilities](#).

3. 在还原数据库部分中、从*选择备份*菜单中选择要还原的备份文件。
4. 单击 * 还原 *。
5. 出现所有数据都将被替换的警告时、单击*确定*

还原活动的状态将显示在还原页面上。

正在更新已过期的许可证

如果一个或多个Insight许可证已过期、您可以使用与最初安装许可证相同的操作步骤 快速更新许可证。

步骤

1. 在文本编辑器(如Notepad)中、打开从NetApp支持收到的新许可证文件、并将许可证密钥文本复制到Windows剪贴板。
2. 在浏览器中打开OnCommand Insight。
3. 单击工具栏上的*管理员*。
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。

此操作会将新许可证添加到任何当前处于活动状态的Insight许可证中。

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"使用情况"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。

许可证不再合规

如果您在"Insight Licenses"页面上看到"Not Compliance"消息、则Insight管理的TB数将超过您公司许可的TB数。

"不合规"消息表示贵公司支付的TB数少于Insight当前管理的TB数。不合规消息旁边会显示受管TB数与许可的TB数之间的差值。

Insight系统的运行不会受到影响、但您应联系NetApp代表以增加许可证覆盖范围并更新相应的许可证。

替换旧版Insight的许可证

如果您购买的新Insight版本与旧版本的产品不向后兼容、则必须将旧许可证替换为新许可证。

安装新许可证时、必须先选择*替换*操作、然后再保存许可证密钥文本。

应用Service Pack

我们会定期提供服务包、您可以应用这些服务包来利用OnCommand Insight 的修复和增强功能。

开始之前

- 您必须已下载服务包文件(例如、 7.2service_pack_1.patch)。
- 您必须已批准所有修补程序。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*修补程序*。
3. 从"Actions"按钮中、选择*应用修补程序*。
4. 在*应用数据源修补程序*对话框中、单击*浏览*以查找服务包文件。
5. 检查*修补程序名称*、问题描述*、*受影响的数据源类型(用于显示是否有任何数据源受到影响)以及*详细信息*(用于描述服务包包含的增强功能)。
6. 如果选定的服务包正确无误、请单击*应用修补程序*。

服务包会自动获得批准；无需采取进一步操作。

准备特殊的故障排除报告

Insight会通过您在安装软件后设置的ASUP系统自动向NetApp客户支持发送信息。但是、您可能需要创建故障排除报告、并与支持团队就特定问题创建案例。

您可以使用Insight中的工具执行手动Insight备份、捆绑日志并将这些信息发送给NetApp客户支持。

手动备份OnCommand Insight 数据库

如果为OnCommand Insight 数据库启用了每周备份、则会自动生成副本、以便在必要时用于还原数据库。如果您需要在执行还原操作之前创建备份、或者发送给NetApp技术支持以寻求帮助、则可以创建备份 .zip 文件。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*故障排除*。
3. 在发送/收集数据部分中、单击*备份*。
4. 单击*保存文件*。
5. 单击 * 确定 *。

捆绑支持日志

在解决Insight软件的问题时、您可以快速生成日志和采集记录的zip文件(使用"gz"格式)、以发送给NetApp客户支持。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*故障排除*。
3. 在发送/收集数据部分中、单击*捆绑包日志*。
4. 单击*保存文件*。
5. 单击 * 确定 *。

将信息发送给NetApp支持部门

NetApp自动化支持(ASUP)工具会将故障排除信息直接发送给NetApp客户支持团队。您可以强制发送特殊报告。

步骤

1. 在Insight工具栏上、单击*管理*。
2. 单击*设置*。
3. 单击*备份/ASUP*选项卡。
4. 在发送/收集数据区域中、单击*立即发送ASUP *、将日志、记录和备份提交给NetApp支持部门。

Send / Collect data

Action	Description
Back up	Back up the database (configuration and performance) into a ZIP file.
Bundle logs	Collect all log files (including acquisition recordings) and bundle them into a ZIP file. Can be used to send data back to NetApp support when troubleshooting an issue with the software.
Send ASUP now	Forces an ad-hoc ASUP report. Can be used to allow NetApp support to get the latest support data when troubleshooting an issue with the software.

Restore a database

[Select backup](#) ▼ No file selected [Restore](#)

Warning: Your current database will be discarded!

Other tasks

Couldn't find what you are looking for? Connect to the old [OnCommand Insight Portal](#).
Need to send anonymous data back? Open the [scrub utilities](#).

擦洗数据以传输到支持部门

拥有安全环境的客户需要与NetApp客户服务进行通信、以便在不影响其数据库信息的情况下对出现的问题进行故障排除。通过OnCommand Insight 擦洗实用程序、您可以设置一个包含关键字和模式的综合词典、以便"清理"敏感数据并将擦洗的文件发送给客户支持。

步骤

1. 在Web UI中、单击*管理*并选择*故障排除*。
2. 在页面底部的其他任务区域中、单击*擦洗实用程序*链接。

擦除部分有几个：在词典中查找、擦除数据和构建词典、自定义关键字和正则表达式。

+ .. 在"*在词典中查找"*部分中、输入一个代码以显示其替换的值、或者输入一个值以查看替代该值的代码。注意：在执行查找之前、必须*构建*词典以标识要从支持数据中擦除的值。

1. 要添加您自己的关键字以从支持数据中擦除、请在*自定义关键字*部分中单击菜单：操作[添加自定义关键字]。输入关键字并单击*保存*。此关键字将添加到词典中。
2. 展开*模式(regex)*。单击*添加*以显示用于输入新模式的对话框。
3. 要使用正则表达式来标识要擦除的词或短语、请在*正则表达式*部分中输入一个或多个模式。单击菜单：操作[添加正则表达式]、在字段中输入模式名称和正则表达式、然后单击*保存*。此信息已添加到词典中。



模式必须包含在圆括号中、才能标识正则表达式捕获组。

4. 在"*构建词典"*部分中、单击*构建*以对OnCommand Insight 数据库中标识为敏感的所有词启动词典编译。

完成后、您会看到一个提示、告知您修订后的词典可用。Database问题描述 包含一条线、用于指示词典中的关键字数量。检查词典中的关键字是否准确。如果您发现问题并希望重建词典、请单击数据库块上的*重置*以从词典中删除从OnCommand Insight 数据库收集的所有关键字。如提示所述、不会删除任何其他关键字。返回到擦洗实用程序、然后重新输入自定义关键字。

5. 创建擦除词典后、您可以使用它擦除日志、XML或其他文本文件以使数据匿名。
6. 要擦除日志、XML或其他文本文件、请在*擦除数据*部分中浏览找到该文件、然后单击*擦除文件*。

高级故障排除

要完成OnCommand Insight 配置、您必须使用高级故障排除工具。这些工具可在浏览器中运行、并可从*管理*>*故障排除*页面打开。

要在浏览器中打开高级故障排除工具、请单击页面底部的*高级故障排除*链接。

通过高级故障排除工具、您可以查看各种报告、系统信息、已安装的软件包和日志、并执行许多操作、例如重新启动服务器或采集单元、更新DWH标注以及导入标注。

有关所有可用选项、请参见高级故障排除页面。

配置忽略动态数据的小时数

您可以配置OnCommand Insight 忽略更新动态数据的小时数、例如已用容量。如果使用默认值6小时、并且未发生配置更改、则只有在默认小时数之后、才会使用动态数据更新报告。此选项可提高性能、因为此选项仅在动态数据发生更改时延迟更新。

关于此任务

如果为此选项设置了值、OnCommand Insight 将根据以下规则更新动态数据：

- 如果未发生配置更改、但容量数据发生更改、则不会更新数据。
- 只有在此选项中指定的超时之后、才会更新动态数据(配置更改除外)。
- 如果发生配置更改、则会更新配置和动态数据。

受此选项影响的动态数据包括以下内容：

- 容量违规数据
- 文件系统已分配容量和已用容量
- 虚拟机管理程序
 - 虚拟磁盘已用容量
 - 虚拟机已用容量
- 内部卷
 - 数据已分配容量
 - 已用数据容量
 - 重复数据删除节省的空间
 - 上次已知访问时间
 - 上次Snapshot时间
 - 其他已用容量

- Snapshot计数
- Snapshot已用容量
- 已用总容量
- iSCSI会话启动程序IP、目标会话ID和启动程序会话ID
- qtree配额已用容量
- 配额已用文件和已用容量
- 存储效率技术、收益/损失和潜在收益/损失
- 存储池
 - 已用数据容量
 - 重复数据删除节省的空间
 - 其他已用容量
 - Snapshot已用容量
 - 已用总容量
- Volume
 - 重复数据删除节省的空间
 - 上次已知访问时间
 - Used capacity

步骤

1. 在Insight工具栏上、单击*管理*并选择*故障排除*。
2. 在页面底部的"Other tasks"区域中、单击*高级故障排除*链接。
3. 单击*高级设置*选项卡、在采集动态属性部分中输入OnCommand Insight 应忽略采集动态属性的动态数据的小时数。
4. 单击 * 保存 *。
5. (可选)要重新启动采集单元、请单击*重新启动采集单元*链接。

重新加载本地采集单元会重新加载所有OnCommand Insight 数据源视图。此更改将在下次轮询期间应用、因此您无需重新启动采集单元。

为客户支持生成日志

如果客户支持部门要求、请生成服务器、采集或远程日志以进行故障排除。

关于此任务

如果NetApp客户支持部门要求、请使用此选项生成日志。

步骤

1. 在Insight工具栏上、单击*管理*并选择*故障排除*。

2. 在页面底部的"Other tasks"区域中、单击*高级故障排除*。
3. 在下一页的高级菜单中、单击*故障排除*链接。
4. 单击*日志*选项卡、然后选择要下载的日志文件。

此时将打开一个对话框、您可以在本地打开日志或保存日志。

显示系统信息

您可以显示有关部署OnCommand Insight 服务器的系统的Microsoft Windows IP配置信息。

步骤

1. 在Insight工具栏上、单击*管理*并选择*故障排除*。
2. 在页面底部的"Other tasks"区域中、单击*高级故障排除*链接。
3. 在高级故障排除页面上、单击*报告*选项卡。
4. 单击*系统信息*。

Windows IP配置包括主机名、DNS、IP地址、子网掩码、操作系统信息、 内存、启动设备和连接名称。

列出已安装的OnCommand Insight 组件

您可以显示已安装的OnCommand Insight 组件列表、其中包括清单、容量、维度、 和数据仓库视图。客户支持可能会要求您提供此信息、或者您可能希望了解安装的软件版本以及安装的时间。

步骤

1. 在Insight工具栏上、单击*管理*并选择*故障排除*。
2. 在页面底部的"Other tasks"区域中、单击*高级故障排除*链接。
3. 在高级故障排除页面上、单击*报告*选项卡。
4. 单击*已安装的软件包*。

计算数据库对象的数量

要确定OnCommand Insight 数据库中的对象数量、请使用计算比例功能。

步骤

1. 在Insight工具栏上、单击*管理*并选择*故障排除*。
2. 在页面底部的"Other tasks"区域中、单击*高级故障排除*链接。
3. 在高级故障排除页面上、单击*报告*选项卡。
4. 单击*计算的比例*。

重新启动OnCommand Insight 服务器

重新启动OnCommand Insight 服务器后、刷新页面并重新登录到OnCommand Insight 门户。

关于此任务



只有在NetApp客户支持提出请求时、才应使用这两个选项。重新启动之前未进行确认。

步骤

1. 在Insight工具栏上、单击*管理*并选择*故障排除*。
2. 在页面底部的"Other tasks"区域中、单击*高级故障排除*链接。
3. 在下一页的高级菜单中、单击*操作*选项卡。
4. 单击*重新启动服务器*。

使用迁移选项移动MySQL数据

您可以使用将MySQL数据目录迁移到其他目录。您可以保留当前数据目录。您可以使用Troubleshooting菜单上的migrate选项、也可以使用命令行。此操作步骤 介绍了如何使用*故障排除*>*迁移MySQL数据*选项。

关于此任务

如果保留当前数据目录、则该目录将作为备份保留并重命名。

步骤

1. 在Web UI中、单击*管理*并选择*故障排除*。
2. 单击*高级故障排除*。
3. 选择*操作*选项卡
4. 选择*迁移MySQL数据*。
5. 输入要将数据迁移到的路径。
6. 要保留现有数据目录、请选中*保留现有数据目录。*
7. 单击 * 迁移 *。

使用命令行移动MySQL数据

您可以使用将MySQL数据目录迁移到其他目录。您可以保留当前数据目录。您可以使用Troubleshooting菜单上的migrate选项、也可以使用命令行。此操作步骤 介绍了如何使用命令行。

关于此任务

如果保留当前数据目录、则该目录将作为备份保留并重命名。

您可以使用Migrate MySQL Data实用程序、也可以使用 `java -jar mysqldatamigrator.jar` 选项OnCommand Insight \bin\mysqldatamigrator 应使用以下参数的位置：

- 必需参数

- 路径

要将数据文件夹复制到的新数据路径。

- 可选参数

- `*—myCnf <my .cnf file>`

cnf文件的路径。默认值为 `<install path>\mysql\my.cnf`。只有在使用非默认MySQL时、才使用此标志。

- `—doBackup`

如果设置了此标志、则当前数据文件夹将被重命名、但不会被删除。

步骤

1. 在此处访问命令行工具： `<installation path> \bin\mysqldatamigrator\mysqldatamigrator.jar`

使用示例

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

正在强制更新标注

如果您更改了标注并希望立即在报告中使用它们、请使用强制标注选项之一。

步骤

1. 在Web UI中、单击*管理*并选择*故障排除*。
2. 在页面底部、单击*高级故障排除*链接。
3. 单击*操作*选项卡。
4. 选择以下选项之一：
 - *更新DWH标注*以强制更新数据仓库中用于报告的标注。
 - *更新DWH标注(包括Deleted)*以强制更新数据仓库中的标注(包括已删除的对象)以用于报告。

检查服务器资源的状态

此选项显示OnCommand Insight 服务器的信息、包括服务器内存、磁盘空间、操作系统以及CPU和OnCommand Insight 数据库信息、包括InnoDB数据大小和数据库所在的磁盘可用空间。

步骤

1. 在Insight工具栏上、单击*管理*并选择*故障排除*。
2. 在页面底部的其他任务区域中、单击* OnCommand Insight Portal"链接。
3. 在下一页的高级菜单中、单击*故障排除*链接。
4. 单击*服务器资源状态*。

*对于高级OnCommand Insight 用户：*管理员可以通过信息摘要末尾的按钮运行一些SQL测试来检查数据库和服务器的响应时间。如果服务器资源不足、此选项将显示警告。

查找虚影数据源

如果您已删除设备、但设备数据仍保留、则可以找到任何虚影数据源、以便将其删除。

步骤

1. 在Web UI中、单击*管理*并选择*故障排除*。
2. 在页面底部的"Other tasks"区域中、单击*高级故障排除*链接。
3. 在*报告*选项卡上、单击*虚影数据源*链接。

OnCommand Insight 会生成一个包含发起者及其设备信息的列表。

添加缺少的磁盘型号

如果由于磁盘型号未知而导致采集失败、您可以将缺少的磁盘型号添加到 `new_disk_models.txt` 文件并再次运行采集。

关于此任务

在通过OnCommand Insight 采集对存储设备进行轮询的过程中、将读取存储设备上的磁盘型号。如果供应商向其阵列中添加了Insight不知道的新磁盘型号、或者Insight查找的型号与存储设备返回的型号不匹配、则该数据源的采集将失败并显示错误。为了防止出现这些错误、必须更新Insight已知的磁盘型号信息。Insight中添加了新的磁盘型号以及更新、修补程序和维护版本。但是、您可以决定手动更新此信息、而不是等待修补程序或更新。

由于OnCommand Insight 每五分钟读取一次磁盘型号文件、因此您输入的任何新数据型号信息都会自动更新。您无需重新启动服务器即可使更改生效、但可以选择重新启动服务器和任何远程采集单元(RAU)、以便在下次更新之前使更改生效。

磁盘型号更新将添加到 `new_disk_models.txt` 文件位于

中<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war 目录。在更新之前、了解描述新磁盘型号所需的信息 `new_disk_models.txt` 文件文件中的信息不准确会产生不正确的系统数据、并可能导致采集失败。

按照以下说明手动更新Insight磁盘型号：

步骤

1. 找到适用于您的磁盘型号的正确信息。

2. 使用文本编辑器打开 `new_disk_models.txt` 文件
3. 为新数据源添加所需信息。
4. 将文件保存在中
`<SANSscreenInstallDir>\wildfly\standalone\deployments\datasources.war` 目录。
5. 备份 `new_disk_models.txt` 将文件保存到安全位置。在后续的OnCommand Insight 升级期间、此文件将被覆盖。如果升级后的文件中不存在磁盘型号信息、则需要重新输入该信息。

查找新磁盘型号所需的信息

要查找磁盘型号信息、请确定供应商和型号并运行Internet搜索。

关于此任务

查找磁盘型号信息就像运行Internet搜索一样简单。在搜索之前、请务必记下供应商名称和磁盘型号。

步骤

1. 建议在互联网上搜索供应商、型号和文档类型"PDF"、以查找供应商的数据表和/或驱动器安装指南。这些数据表通常是供应商磁盘信息的最佳来源。
2. 供应商规格并不总是根据完整的型号提供所有必要的信息。在供应商的站点上搜索型号字符串的不同部分来查找所有信息通常很有用。
3. 找到磁盘供应商名称、完整型号、磁盘大小和速度以及接口类型、以便在OnCommand Insight 中定义新的磁盘型号。您可以使用下表作为参考、在找到此信息时帮助您记下此信息：

对于此字段：	其中：	输入以下内容：
型号(也称为密钥)	Required	
供应商	Required	
磁盘速度(RPM)	Required	
大小(以GB为单位)	Required	
接口类型(选择一项)	Required	ATA、SATA、SATA2、SATA3、F C、SAS、FATA、SSD、其他
寻道时间(以毫秒为单位)	可选	
最大传输速率、以MB/秒为单位	可选	
接口传输速率、以MB/秒为单位	可选	
指向供应商/型号信息的链接	可选、但建议使用	

4. 在中输入此信息 new_disk_models.txt 文件请参见 "[new_disk_models.txt文件的内容](#)" 格式、顺序和示例。

new_disk_models.txt文件的内容

。 new_disk_models.txt 文件包含必填字段和可选字段。这些字段以逗号分隔、因此请勿在字段中使用逗号_within。

除寻道时间、传输速率和附加信息以外、所有字段均为必填字段。如果有、请在Additional _info字段中包含供应商/型号网站链接。

使用文本编辑器按此顺序为要添加的每个新磁盘型号输入以下信息、并用逗号分隔：

1. 键：使用型号(必需)
2. 供应商：名称(必需)
3. 型号：完整数字(通常与"密钥"中的值相同)(必需)
4. 磁盘的*转数*：例如10000或15000 (必需)
5. 大小：容量(GB)(必需)
6. 接口类型：ATA、SATA、FC、SAS、FATA、SSD、其他(必需)
7. 寻道时间：以毫秒为单位(可选)
8. 潜在传输速率：潜在传输速率、以MB/秒为单位磁盘本身的最大传输速率。（可选）
9. 接口传输速率：主机之间的传输速率、以MB/秒为单位(可选)。
10. 其他信息：要捕获的任何追加信息。最佳实践是、输入供应商页面的链接以查找规格、以供参考(可选)

对于留空的任何可选字段、请务必包含逗号。

示例(每行都不含空格)：

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfiles/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.toshiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

监控您的环境

Insight可帮助您防止环境中出现问题并快速排除潜在问题。

资产页面数据

资产页面可提供性能故障排除数据、并通过指向追加信息的链接提供有关基础资产(例如虚拟机或卷)及其使用的相关资产(例如存储池、存储节点和连接的交换机端口)的摘要信息。

从OnCommand Insight 7.3.1开始、所有资产页面都具有一个*主*页面和一个*附加数据*页面。主页面上是资产摘要以及图表、拓扑和其他信息的不同部分。通过*其他数据*页面、您可以为当前资产类型配置可自定义的信息板页面。

资产页面主选项卡上的行或消息旁边的红色实心圆圈表示受监控环境可能存在的问题。

资产页面的类型

资产页面汇总了资产的当前状态，并包含指向有关资产及其相关资产的追加信息的链接。

OnCommand Insight 提供了以下资产的资产页面：

- 虚拟机
- Volume
- 内部卷
- 物理主机
- 存储池
- 存储
- 数据存储库
- 虚拟机管理程序
- 应用程序
- 存储节点
- qtree
- Disk
- VMDK
- Port
- 交换机
- 网络结构
- 对象存储(例如Atmos、Centera、Amazon S3)
- 分区

映射和屏蔽信息可在分区、卷、虚拟机和主机/虚拟机管理程序资产页面上的表中查看。




摘要信息可用于对象存储资产；但是、您只能从"数据源"详细信息页面访问此信息。

在环境中搜索特定资产

您可以使用搜索工具查找有关特定资产的信息。例如、如果系统用户联系存储管理员、抱怨某个特定服务器、则管理员可以搜索服务器名称并显示一个资产页面、其中汇总了状态并提供了其他链接信息。

步骤

1. 打开OnCommand InsightWeb UI。
2. 在工具栏上、单击 。

此时将显示*搜索资产*框。

3. 输入资产的名称或名称的一部分。
4. 从搜索结果中选择所需的资源。

此时将显示该资源的资产页面。

高级搜索技术

可以使用多种搜索方法来搜索受监控环境中的数据或对象。

通配符搜索

您可以使用 * 字符执行多字符通配符搜索。例如、_applic* n_将返回应用程序。

搜索中使用的短语

短语是一组用双引号括起来的词；例如、"paw VNX LUN 5"。您可以使用双引号搜索名称或属性中包含空格的文档。

布尔运算符

使用布尔运算符、您可以组合多个术语来构成更复杂的查询。

- 或

- OR 运算符是默认的结合运算符。

如果两个术语之间没有布尔运算符，则使用 OR 运算符。

- OR 运算符链接两个术语，如果文档中存在其中任何一个术语，则会查找匹配的文档。

例如、`storage or NetApp`会搜索包含`storage`或`NetApp`的文档。

- 与大多数术语匹配的文档将获得高分。

- 和

您可以使用 AND 运算符查找一个文档中同时存在这两个搜索词的文档。例如、`aurora and NetApp`会搜索同时包含`storage`和`NetApp`的文档。

您可以使用符号&&代替单词AND。

- 不

使用 NOT 运算符时，搜索结果中将排除包含 NOT 之后的术语的所有文档。例如、`storage not NetApp`会搜索仅包含`storage`而不包含`NetApp`的文档。

您可以使用符号！而不是单词NOT。

前缀和后缀搜索

- 一旦开始键入搜索字符串、搜索引擎就会执行前缀和后缀搜索以查找最佳匹配项。
- 与前缀或后缀匹配相比、精确匹配的得分更高。分数根据搜索词与实际搜索结果之间的距离计算得出。例如、我们三个存储：“aurora”、“aurora1”和“aurora11”。搜索“aur”将返回所有三个存储。但是、“aurora”的搜索结果得分最高、因为它与前缀搜索字符串的距离最接近。
- 搜索引擎还会按相反顺序搜索术语、从而允许您执行后缀搜索。例如、当您在搜索框中键入“345”时、搜索引擎将搜索“345”。
- 搜索不区分大小写。

使用索引词进行搜索

如果搜索与更多索引词匹配，则会获得更高的分数。

搜索字符串按空格拆分为不同的搜索词。例如、搜索字符串“storage aurora NetApp”拆分为三个关键字：“storage”、“aurora”和“NetApp”。搜索将全部使用这三个词执行。与大多数术语匹配的文档得分最高。您提供的信息越多，搜索结果越好。例如、您可以按存储名称和模式搜索存储。

用户界面会显示各个类别的搜索结果，每个类别的前三个结果。如果您未找到所需的文档、可以在搜索字符串中添加更多术语以改进搜索结果。

下表列出了可添加到搜索字符串中的索引词。

类别	索引术语
存储	<ul style="list-style-type: none">• “s存储”• name• 供应商• 型号
StoragePool	<ul style="list-style-type: none">• “s存储池”• name• 存储的名称• 存储的IP地址• 存储的序列号• 存储供应商• 存储型号• 所有关联内部卷的名称• 所有关联磁盘的名称

内部卷	<ul style="list-style-type: none"> • “内部卷” • name • 存储的名称 • 存储的IP地址 • 存储的序列号 • 存储供应商 • 存储型号 • 存储池的名称 • 所有关联共享的名称 • 所有关联应用程序和业务实体的名称
Volume	<ul style="list-style-type: none"> • “卷” • name • label • 所有内部卷的名称 • 存储池的名称 • 存储的名称 • 存储的IP地址 • 存储的序列号 • 存储供应商 • 存储型号
存储节点	<ul style="list-style-type: none"> • “storagenode” • name • 存储的名称 • 存储的IP地址 • 存储的序列号 • 存储供应商 • 存储型号
主机	<ul style="list-style-type: none"> • “主机” • name • IP 地址 • 所有关联应用程序和业务实体的名称

数据存储库	<ul style="list-style-type: none"> • “d存储” • name • 虚拟中心IP • 所有卷的名称 • 所有内部卷的名称
虚拟机	<ul style="list-style-type: none"> • “虚拟机” • name • DNS名称 • IP 地址 • 主机的名称 • 主机的IP地址 • 所有数据存储库的名称 • 所有关联应用程序和业务实体的名称
交换机（常规和 NPV ）	<ul style="list-style-type: none"> • “s交换机” • IP 地址 • WWN • name • 序列号 • 型号 • 域ID • 网络结构的名称 • 网络结构的WWN
应用程序	<ul style="list-style-type: none"> • “应用程序” • name • 租户 • 业务部门 • 业务单位 • 项目

磁带	<ul style="list-style-type: none">• “磁带”• IP 地址• name• 序列号• 供应商
Port	<ul style="list-style-type: none">• “端口”• WWN• name
网络结构	<ul style="list-style-type: none">• “网络结构”• WWN• name


更改显示数据的时间范围

默认情况下、资产页面会显示最近24小时的数据；但是、您可以通过选择其他固定时间或自定义时间范围来更改显示的数据段、以查看较少或更多数据。

关于此任务

无论资产类型如何，您都可以使用每个资产页面上的选项来更改所显示数据的时间段。

步骤

1. 登录到OnCommand InsightWeb UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。
3. 在页面的左上角、单击以下任一时间图标以更改显示的数据段：
 - * 3小时*
 - 显示最近三小时的数据。
 - * 24小时*
 - 显示最近24小时的数据。
 - 三维
 - 显示最近三天的数据。
 - * 7d*

显示最近七天的数据。


- * 30天*

显示最近三十天的数据。

- 自定义

显示一个对话框、可用于选择自定义的时间范围。一次最多可显示31天的数据。

4. 如果选择*自定义*、请执行以下操作：

- 单击日期字段、然后为开始日期选择月份、日期和年份。
- 单击时间列表、然后选择开始时间。
- 对结束数据和时间重复步骤a和b。
- 单击 。

确定数据源采集状态



由于数据源是Insight的主要信息源、因此您必须确保它们保持运行状态。

可以在每个资产页面上查看直接获取的所有资产的数据源采集状态。可能会发生以下任一采集情形、其中状态显示在资产页面的右上角：

- 已成功从数据源采集

显示状态"`acquired xxxx` ``", where ``xxxx`` 指示资产数据源的最新采集时间。

- 发生采集错误。

显示状态"`acquired xxxx` ``", where ``xxxx`` 指示资产的一个或多个数据源的最新采集时间 。单击时 、此时将显示一个窗口、其中显示资产的每个数据源、数据源的状态以及上次采集数据的时间。单击某个数据源将显示该数据源的详细信息页面。

如果资产不是直接获取的、则不会显示任何状态。

资产页面部分

资产页面会显示多个部分、其中包含与资产相关的信息。您看到的部分取决于资产类型。

摘要

资产页面上的"摘要"部分显示有关特定资产的信息摘要、并显示与资产相关的问题(用红色圆圈表示)、其中包含指向追加信息 的相关资产以及分配给资产的任何性能策略的超链接。

以下示例显示了虚拟机资产页面的摘要部分中提供的一些类型的信息。旁边带有红色实心圆圈的任何项目均表示受监控环境存在潜在问题。


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

使用摘要部分

您可以查看"摘要"部分以查看有关资产的常规信息。具体而言、查看任何指标(例如内存、容量和延迟)或任何性能策略是否为值得关注的发生原因 非常有用、OnCommand Insight 会通过在该指标或性能策略旁边显示一个红色圆圈来表示此问题。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。



摘要部分中显示的信息取决于您正在查看的资产页面类型。

3. 您可以单击任何资产链接以查看其资产页面。

例如、如果您正在查看某个存储节点、则可以单击某个链接以查看与其关联的存储的资产页面、或者单击以查看HA配对节点的资产页面。

4. 您可以查看与资产关联的指标。

指标旁边的红色圆圈表示您可能需要诊断和解决潜在问题。



您可能会注意到，某些存储资产上的卷容量可能显示大于 100%。这是由于与卷容量相关的元数据属于资产报告的已用容量数据的一部分。

5. 如果适用，您可以单击性能策略链接以查看与资产关联的性能策略。

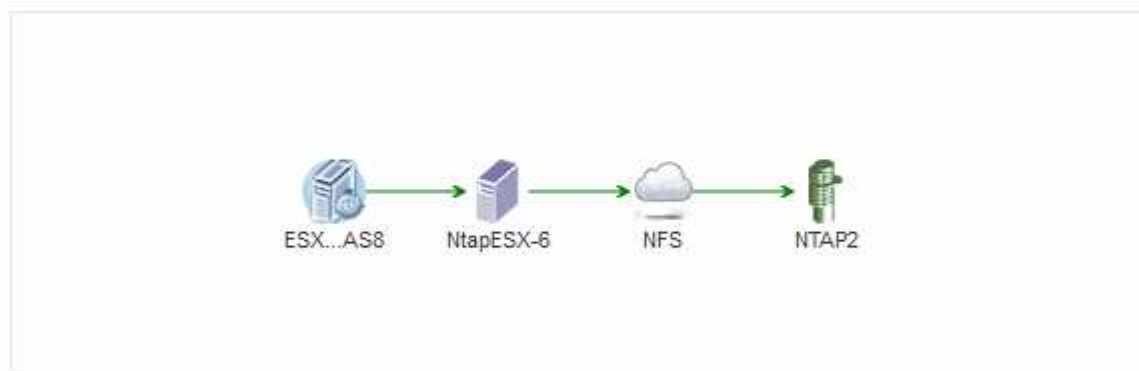
如果性能策略旁边显示红色圆圈，则表示资产已超过性能策略定义的阈值。您应检查性能策略以进一步诊断问题描述。

拓扑

如果适用于某个资产、可通过拓扑部分查看基础资产如何连接到其相关资产。

以下示例显示了虚拟机资产页面的Topology部分可能显示的内容。

Topology



如果资产的拓扑大于本节所示的范围、则会显示*单击链接以查看拓扑*超链接。

使用Topology部分

通过拓扑部分、您可以查看网络中的资产如何彼此连接、并显示有关相关资产的信息。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。您可以在资产页面的右上角找到Topology部分。

如果资产的拓扑大于本节所示的范围、请单击*单击链接以查看Topologies*超链接。

3. 要查看有关基础资产的相关资产的详细信息、请将光标置于拓扑中的相关资产上、然后单击其名称以显示其资产页面。

用户数据

资产页面的User Data部分将显示并允许您更改任何用户定义的数据、例如应用程序、业务

实体和标注。

以下示例显示了在为虚拟机资产分配应用程序、业务实体和标注时、虚拟机资产页面的"User Data"部分可能显示的内容：

User Data

Application(s):


Concur


Business Entities:

Hybridsoft Corporation.Sales.Wes...

Birthday:

01/30/2016








+ Add


使用 **User Data** 部分分配或修改应用程序

您可以将环境中运行的应用程序分配给某些资产(主机、虚拟机、卷、内部卷和虚拟机管理程序)。通过"User Data"部分、您可以更改分配给资产的应用程序、或者为资产分配应用程序或其他应用程序。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。
3. 您可以执行以下操作：
 - 要查看应用程序的资产页面、请单击应用程序的名称。
 - 要更改分配的应用程序或分配应用程序或其他应用程序、请将光标置于应用程序名称上(如果已分配应用程序)、或者将光标置于*无*之上(如果未分配任何应用程序)、单击 、键入以搜索应用程序或从列表选择一个应用程序、然后单击 。




如果您选择的应用程序与某个业务实体关联、则该业务实体将自动分配给该资产。在这种情况下、将光标置于业务实体名称上方时、将显示_derived_词。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。

 - 要删除应用程序、请单击 。

使用用户数据部分分配或修改业务实体

您可以定义业务实体、以便更精细地跟踪和报告环境数据。通过资产页面中的User Data部分、您可以更改分配给资产的业务实体或从资产中删除业务实体。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。
3. 您可以执行以下操作：
 - 要更改分配的实体或分配实体、请单击  并从列表选择一个实体。
 - 要删除业务实体、请单击 。





您不能删除从分配给资产的应用程序派生的实体。


使用 **User Data** 部分分配或修改标注

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。资产页面的 "User Data" 部分显示分配给资产的标注，还可以用于更改分配给该资产的标注。

步骤

1. 登录到OnCommand Insight Web UI。
 2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。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 。
- 此时将显示添加标注对话框。
4. 单击*标注*、然后从列表选择一个标注。
 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 *。

标注将分配给资产。您可以稍后使用查询按标注筛选资产。

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。

通过资产页面的"Expert View"部分、您可以根据所选时间段(3小时、24小时、3天、7天、或自定义时间段)以及与之相关的任何资产。

以下是卷资产页面中的"Expert View"部分的示例：



您可以选择要在性能图表中查看选定时间段的指标。

"Resources"部分显示基本资产的名称以及性能图表中表示基本资产的颜色。如果Top correlated部分不包含要在性能图表中查看的资产、则可以使用Additional Resources部分中的*搜索资产*框来查找该资产并将其添加到性能图表中。添加资源时，这些资源将显示在 Additional Resources 部分中。

如果适用，"资源"部分还会显示以下类别中与基础资产相关的任何资产：

- 相关度最高
显示与基本资产的一个或多个性能指标相关性（百分比）较高的资产。
- 主要贡献者
显示对基本资产贡献（百分比）的资产。
- 贪婪
显示了通过共享主机，网络和存储等相同资源从资产中占用系统资源的资产。
- 已降级
显示了由于此资产而耗尽系统资源的资产。

专家视图指标定义

资产页面的 "Expert View" 部分会根据为资产选择的时间段显示多个指标。每个指标都会显

示在自己的性能图表中。您可以根据要查看的数据在图表中添加或删除指标和相关资产。

衡量指标	Description
BB 信用零 Rx ， Tx	取样期间接收 / 传输缓冲区到缓冲区信用计数过渡到零的次数。此度量指标表示连接的端口由于缺少可提供的信用值而不得不停止传输的次数。
BB 信用零持续时间 Tx	采样间隔内传输 BB 信用值为零的时间（以毫秒为单位）。
缓存命中率（总计，读取，写入） %	导致缓存命中的请求百分比。对卷的命中次数与访问次数之比越高，性能越好。对于不收集缓存命中信息的存储阵列，此列为空。
缓存利用率（总计） %	导致缓存命中的缓存请求的总百分比
类 3 丢弃	光纤通道 3 类数据传输丢弃的计数。
CPU 利用率（总计） %	活动使用的 CPU 资源量，占总可用资源的百分比（对于所有虚拟 CPU）。
CRC 错误	取样期间端口检测到的具有无效循环冗余检查（CRC）的帧数
帧速率	以每秒帧数（帧数 / 秒）为单位的传输帧速率
帧大小平均值（Rx ， Tx）	流量与帧大小的比率。通过此指标，您可以确定网络结构中是否存在任何开销帧。
帧大小太长	过长的光纤通道数据传输帧的数量。
帧大小太短	太短的光纤通道数据传输帧的数量。
I/O 密度（总，读取，写入）	IOPS 数除以卷，内部卷或存储元素的已用容量（从数据源的最新清单轮询中获取）。以每 TB 每秒 I/O 操作数为单位。
IOPS（总计，读取，写入）	单位时间内通过 I/O 通道或该通道一部分的读 / 写 I/O 服务请求数（以每秒 I/O 数为单位）
IP 吞吐量（总吞吐量，读取吞吐量，写入吞吐量）	<p>Total：以 MB/ 秒为单位传输和接收 IP 数据的聚合速率。Read：IP Throughput (Receive)：接收IP数据的平均速率、以MB/秒为单位。</p> <p>Write：IP Throughput (Transmit)：以MB/秒为单位传输IP数据的平均速率。</p>


延迟（总计，读取，写入）	<p>延迟（R&W）：在固定时间内向虚拟机读取或写入数据的速率。此值以 MB/ 秒为单位。</p> <p>Latency：数据存储中虚拟机的平均响应时间。</p> <p>Top Latency：数据存储中虚拟机的最长响应时间。</p>
链路故障	取样期间端口检测到的链路故障数量。
链路重置 Rx，Tx	取样期间接收或传输链路重置的数量。此指标表示连接的端口对此端口发出的链路重置次数。
内存利用率（总计） %	主机使用的内存阈值。
部分读 / 写（总计） %	<p>读 / 写操作跨越 RAID 5，RAID 1/0 或 RAID 0 LUN 中任何磁盘模块上的条带边界的总次数通常，条带跨越并不有益，因为每个条带跨越都需要额外的 I/O 百分比。较低表示条带元素大小效率较高，并表示卷（或 NetApp LUN）对齐不正确。</p> <p>对于 CLARiiON，此值是条带跨越次数除以 IOPS 总数。</p>
端口错误	报告取样期间 / 给定时间范围内的端口错误。
信号丢失计数	信号丢失错误的数量。如果发生信号丢失错误，则表示没有电气连接，并且存在物理问题。
交换速率（总速率，速率，出速率）	在取样期间，从磁盘到活动内存的内存换入，移出或同时从磁盘到活动内存的速率。此计数器用于计数适用场景虚拟机。
同步丢失计数	同步丢失错误的数量。如果发生同步丢失错误，则硬件无法识别流量或锁定到该流量上。所有设备可能使用的数据速率不同，或者光纤或物理连接的质量可能较差。端口必须在每次出现此类错误后重新同步，这会影响系统性能。以 KB/ 秒为单位
吞吐量（总吞吐量，读取吞吐量，写入吞吐量）	在响应 I/O 服务请求的固定时间内传输，接收或同时接收数据的速率（以 MB/ 秒为单位）。
丢弃帧超时— Tx	因超时而丢弃的传输帧数。
流量速率（总计，读取，写入）	取样期间传输，接收或同时接收的流量，以每秒兆字节为单位。

流量利用率（总计，读取，写入）	取样期间接收 / 传输 / 总流量与接收 / 发送 / 总容量之比。
利用率（总计，读取，写入） %	用于传输（Tx）和接收（Rx）的可用带宽百分比。
写入待处理（总计）	待处理的写入 I/O 服务请求数。

使用专家视图部分

通过 "Expert View" 部分，您可以根据所选时间段内任意数量的适用指标查看资产的性能图表，并添加相关资产以比较和对比不同时间段内的资产和相关资产性能。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。默认情况下，性能图表显示为资产页面选择的时间段的两个指标。例如，对于存储，性能图表默认显示延迟和总 IOPS。"资源"部分显示资源名称和"其他资源"部分，您可以通过此部分搜索资产。根据资产的不同，您可能还会在"Top correlated"，"Top contributor"，"Greedy"和"Degraded"部分中看到资产。
3. 您可以单击*选择要显示的指标*、然后选择一个指标以添加指标的性能图表。

此时将为选定指标添加一个性能图表。该图表显示选定时间段的数据。您可以通过单击资产页面左上角的另一个时间段来更改时间段。

您可以再次执行此步骤、然后单击以清除指标。此时将删除此指标的性能图表。


4. 您可以将光标置于图表上方、并根据资产单击以下任一项来更改显示的度量数据：
 - 读取*或*写入
 - 默认值为"tx"或"* rx****总计"。
5. 您可以将光标拖动到图表中的数据点上，以查看指标值在选定时间段内的变化情况。
6. 在*资源*部分中、如果适用、您可以执行以下任一操作将任何相关资产添加到性能图表中：
 - 您可以在"Top correlated"、"Top contributors"、"Greedy"或"Degraded"部分中选择相关资产、以便将该资产中的数据添加到每个选定指标的性能图表中。要显示资产的关联度或贡献度必须至少为15%。

选择资产后，该资产旁边会显示一个色块，用于指示其数据点在图表中的颜色。

- 对于显示的任何资产、您可以单击资产名称以显示其资产页面、也可以单击资产与基本资产关联或贡献的百分比以查看有关资产与基本资产关系的详细信息。

例如，单击相关度最高的资产旁边的链接百分比将显示一条信息性消息，其中比较了该资产与基本资产的关联类型。

- 如果Top correlated部分不包含要在性能图表中显示以进行比较的资产、则可以使用Additional

Resources部分中的*搜索资产*框来查找其他资产。选择资产后、它将显示在Additional Resources部分中。如果不再需要查看有关资产的信息，请单击 。




相关资产




如果适用、资产页面将显示相关资产部分。例如、卷资产页面可能会显示有关存储池、已连接交换机端口和计算资源等资产的信息。每个部分都包含一个表、其中列出了该类别中的任何相关资产、指向相应资产页面的链接以及与该资产相关的多个性能统计信息。


使用相关资产部分

"相关资产"部分可用于查看与基础资产相关的任何资产。每个相关资产都会显示在一个表中、并显示该资产的相关统计信息。您可以导出资产信息、在Expert View性能图表中查看资产统计信息或显示仅显示相关资产统计信息的图表。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。
3. 要控制资产在表中的显示方式、请执行以下操作：
 - 单击任何资产的名称以显示其资产页面。
 - 使用*筛选器*框仅显示特定资产。
 - 如果表中的资产超过五个、请单击页码以按页浏览资产。
 - 单击列标题中的箭头，将表中列的排序顺序更改为升序（向上箭头）或降序（向下箭头）。
 - 将光标置于相关资产上并单击、可将相关资产添加到"Expert View"部分的任何性能图表中 。
4. 将表中显示的信息导出到 .CSV 文件：
 - a. 单击 。
 - b. 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、或者单击*保存文件*、然后单击*确定*将文件保存到"下载"文件夹。

当前选定要显示的列的所有对象属性都会导出到此文件中。仅导出显示列的属性。请注意、仅导出表的前10、000行。
5. 要在表下方的图表中显示相关资产信息、请单击  并执行以下任一操作：
 - 单击*读取*、写入*或*总计*以更改显示的指标数据。默认值为*总计*。
 - 单击  可选择其他指标。
 - 单击  更改图表类型。默认值为*折线图*。
 - 将光标移动到图表中的数据点上、查看指标值在为每个相关资产选择的时间段内的变化情况。
 - 单击图表图例中的相关资产、将其添加到图表中或从图表中删除。

- 单击相关资产表中的页码可查看图表中的其他相关资产。
- 单击  以关闭图表。

违规

您可以使用资产页面的违规部分查看因分配给资产的性能策略而在您的环境中发生的违规（如果有）。性能策略可监控您的网络阈值、并使您能够立即检测到违反阈值的情况、确定其含义、并分析问题的影响和根发生原因、以便快速有效地进行更正。

以下示例显示了虚拟机管理程序的资产页面上显示的"Violations"部分：

Violations filter...


Time	Description
06/05/2015 5:00:00 pm	Port balance index of 74 on esx1 exceeds the threshold of 50
06/12/2015 8:59:54 am	2 violations for esx2 with 'Swap out rate' > 3
06/12/2015 12:04:54 pm	esx1 violation with 'Swap out rate' > 3.00 KB/s (value of 86.85 KB/s)
06/12/2015 12:29:54 pm	esx1 violation with 'Swap in rate' > 3.00 KB/s (value of 59.90 KB/s)
06/12/2015 1:04:54 pm	7 violations for ds-30 with 'Latency - Total' > 50

Showing 1 to 5 of 32 entries < 1 2 3 4 5 >


使用Violations部分

通过 Violations 部分，您可以查看和管理因分配给资产的性能策略而在网络中发生的任何违规。

步骤

1. 登录到OnCommand Insight Web UI。
2. 通过执行以下任一操作找到资产页面：
 - 在Insight工具栏上、单击 、键入资产的名称、然后从列表中选择资产。
 - 单击*信息板*、选择*资产信息板*、找到资产名称并单击它。此时将显示资产页面。Violations部分显示违规发生的时间和超过阈值的问题描述、以及指向发生违规的资产的超链接(例如"2 violations fir ds-30 with Latency - total > 50")。
3. 您可以执行以下任一可选任务：
 - 使用*筛选器*框仅显示特定违规。
 - 如果表中存在五个以上的违规、请单击页码以按页浏览违规。
 - 单击列标题中的箭头，将表中列的排序顺序更改为升序（向上箭头）或降序（向下箭头）。
 - 单击任何问题描述中的资产名称以显示其资产页面；红色圆圈表示需要进一步调查的问题。

您可以单击性能策略以显示编辑策略对话框，以查看性能策略并在必要时对策略进行更改。

- 单击  如果您确定问题描述 不再是值得关注的发生原因、则从列表中删除违规。

可自定义的资产页面

其他数据可以显示在每个资产页面上的可自定义小工具中。自定义某个资产的页面会将此

自定义应用于此类型的所有资产的页面。

您可以通过执行以下操作来自定义资产页面小工具：

1. 向页面添加小工具
2. 为小工具创建查询或表达式以显示所需数据
3. 如果需要、请选择一个筛选器
4. 选择汇总或分组方法
5. 保存小工具
6. 对所有所需的小工具重复上述步骤
7. 保存资产页面

您还可以向自定义资产页面添加变量、以进一步细化小工具中显示的数据。除了常规变量之外、每种资产类型还可以使用一组"\$this"变量来快速识别与当前资产直接相关的资源、例如由托管当前虚拟机的同一虚拟机管理程序托管的所有虚拟机。

此自定义资产页面对于每个用户以及每个资产类型都是唯一的。例如、如果用户A为虚拟机创建了自定义资产页面、则该用户的任何虚拟机资产页面都会显示该自定义页面。

用户只能查看、编辑或删除其创建的自定义资产页面。

Insight的导出/导入功能不包括自定义资产页面。

了解"\$this"变量

通过资产的"其他数据"可自定义页面上的特殊变量、您可以轻松展示与当前资产直接相关的追加信息。

关于此任务

要在资产的可自定义登录页面上的小工具中使用"\$this"变量、请执行以下步骤。在此示例中、我们将添加一个表小工具。



"\$this"变量仅对资产的可自定义登录页面有效。它们不适用于其他Insight信息板。可用的"\$this"变量因资产类型而异。

步骤

1. 导航到您选择的资产的资产页面。在此示例中，我们选择一个虚拟机（VM）资产页面。查询或搜索虚拟机，然后单击链接以转到该虚拟机的资产页面。


此时将打开虚拟机的资产页面。

2. 单击*更改视图：*>*其他虚拟机数据*下拉列表以转到该资产的可自定义登录页面。
3. 单击*小工具*按钮、然后选择*表小工具*。

此时将打开表小工具进行编辑。默认情况下，所有存储都会显示在表中。

4. 我们希望显示所有虚拟机。单击资产选择器并将*存储*更改为*虚拟机*。

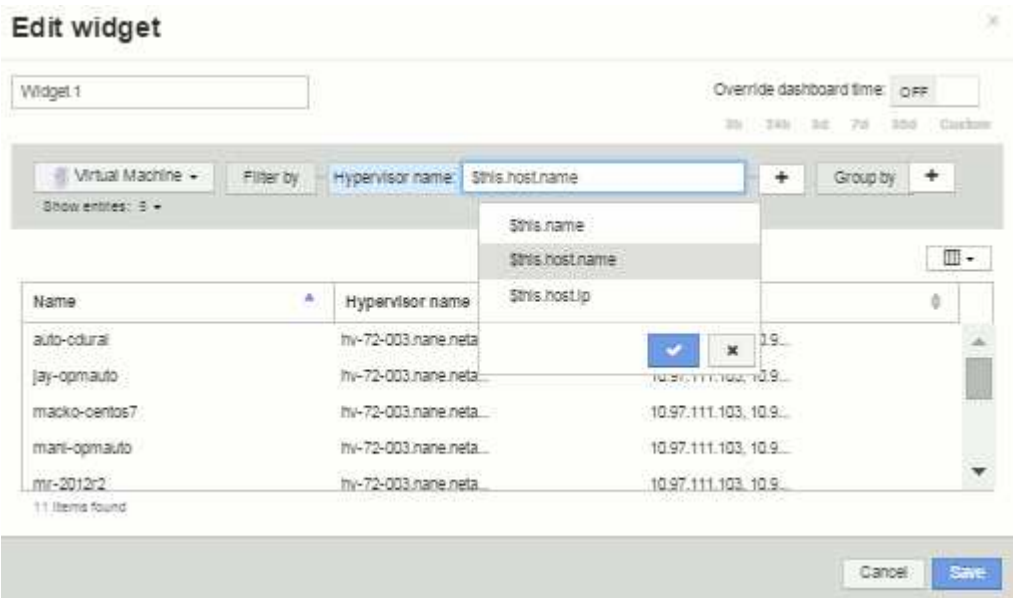
此时，表中将显示所有虚拟机。

5. 单击*列选择器*按钮  并将*虚拟机管理程序名称*字段添加到表中。

表中显示了每个虚拟机的虚拟机管理程序名称。

6. 我们只关心托管当前虚拟机的虚拟机管理程序。单击*筛选依据*字段的"++"按钮、然后选择*虚拟机管理程序名称*。

7. 单击*任何*并选择*\$this.host.name *变量。单击复选按钮以保存筛选器。



8. 此时，此表将显示由当前虚拟机的虚拟机管理程序托管的所有虚拟机。单击 * 保存 *。

结果

您为此虚拟机资产页面创建的表将显示在您显示的任何VM资产页面中。在小工具中使用*\$this.host.name *变量意味着表中仅显示当前资产的虚拟机管理程序所拥有的虚拟机。

平衡网络资源

要解决平衡问题、请使用资产页面查找问题并确定未充分利用的高容量卷。

步骤

- 1. 在浏览器中打开资产信息板。
- 2. 在虚拟机IOPS热图中、您会注意到虚拟机名称的字体非常大、通常会报告问题。
- 3. 单击虚拟机名称以显示资产页面。
- 4. 检查摘要中的错误消息。
- 5. 查看性能图表、尤其是相关资源排名靠前的资源、找到可能处于争用状态的任何卷。

6. 将卷添加到性能图表中以比较活动模式、并显示与问题相关的其他资源的更多资产页面。
7. 滚动到资产页面底部以查看与VM关联的所有资源的列表。记下以高容量运行的所有VMDK。这可能会引发争用。
8. 要解决平衡问题、请确定未充分利用的资源、以便从过度利用的资源接收负载、或者从使用率较高的资源中删除要求较低的应用程序。

检查网络性能

您可以检查存储环境的性能、确定未充分利用和过度利用的资源、并在风险转化为问题之前确定风险。

Insight可帮助您解决或防止通过收集的存储数据发现的性能和可用性问题的。

您可以使用Insight执行以下性能管理任务：

- 监控整个环境的性能
- 确定影响其他设备性能的资源

端口的重要性

Insight服务器和数据仓库(DWH)服务器可能需要多个可用的TCP端口才能可靠地运行。其中某些端口仅用于绑定到本地主机适配器(127.0.0.1)的进程、但核心服务仍需要使用这些端口才能可靠地运行。所需的端口数是网络中使用的端口数的超集。

Insight服务器端口

Insight服务器可以安装软件防火墙。需要打开的"孔"如下所述。

入站HTTPS 443-假设您的Insight WebUI运行在TCP 443上、则必须将其公开、以便允许以下任何及所有使用者：

- WebUI的Insight用户
- 希望连接到Insight服务器的远程采集单元
- 具有与此Insight服务器连接的OCI DWH服务器。
- 与Insight REST API的任何编程交互

对于希望实施Insight服务器主机级防火墙的任何人、我们的一般建议是允许对所有企业网络IP块进行HTTPS访问。

入站MySQL (TCP 3306)。此端口只需要公开到具有连接器的任何Insight DWH服务器

虽然Insight拥有数十个数据收集器、但它们都是基于轮询的—Insight将对其采集单元(AUS)进行发生原因、以便启动与各种设备的出站通信。只要基于主机的防火墙处于"状态"状态、允许通过防火墙返回流量、Insight服务器上基于主机的防火墙就不应影响数据采集。

数据仓库端口

对于Insight DWH服务器：

入站**HTTPS 443**-假设您的Insight WebUI运行在TCP 443上、则必须公开此内容以允许以下使用者：

- DWH管理门户的Insight管理用户

入站**HTTPS (TCP 9300)**—这是Cognos报告接口。如果用户要与Cognos报告界面进行交互、则必须远程公开此信息。

我们可以想象、可能不需要公开DWH的环境—报告作者可能只是与DWH服务器建立RDP连接、然后在那里创建和计划报告、同时计划通过SMTP交付或写入远程文件系统的所有报告。

入站**MySQL (TCP 3306)**。只有当您的组织与DWH数据具有任何基于MySQL的集成时、才需要公开此端口—您是否从各种DWH数据集中提取数据以输入到其他应用程序中、例如CMDB、成本分摊系统等

分析PC性能较慢的问题

如果您收到网络用户的来电、抱怨其计算机运行缓慢、则需要分析主机性能并确定受影响的资源。

开始之前

在此示例中、调用方提供了主机名。

步骤

1. 在浏览器中打开Insight。
2. 在*搜索资产*框中输入主机名、然后在搜索结果中单击主机名。

此时将打开资源的_asset page_。

3. 在主机的资产页面上、检查页面中央的性能图表。除了通常预先选择的延迟和IOPS之外、您可能还需要显示不同类型的数据。单击其他类型数据的复选框、例如吞吐量、内存、CPU或IP吞吐量、具体取决于设备类型。
4. 要在图表上显示某个点的问题描述、请将鼠标指针置于该点上方。
5. 您可能还希望将页面顶部的选择内容更改为3小时到7天、或者将所有可用数据更改为3小时。
6. 检查*前几个相关资源*列表、查看是否存在与基础资源具有相同活动模式的其他资源。

列表中的第一个资源始终为基础资源。

- a. 单击相关资源旁边的链接百分比、查看相关活动模式是针对基本资源和其他资源的IOPS还是CPU。
 - b. 单击相关资源的复选框、将其数据添加到性能图表中。
 - c. 单击相关资源的链接名称以显示其资产页面。
7. 对于VM、如本示例所示、在*相关资源排名靠前*中找到存储池、然后单击存储池名称。

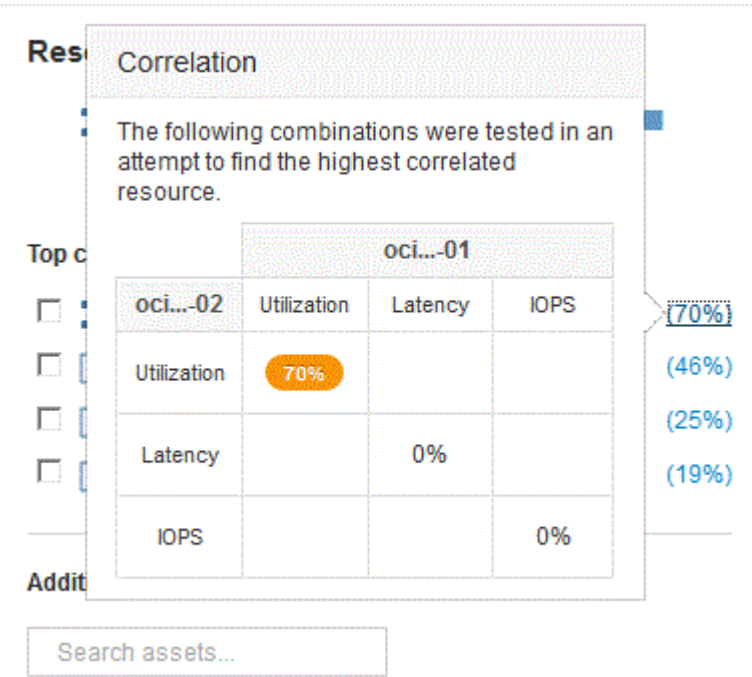
分析相关资源

在调查性能问题并打开设备的_asset page_时、应使用Top correlated resources列表细化性能图表中显示的数据。百分比较高的资源表示资源与基本资源具有类似的活动。

您正在调查性能问题并打开设备的资产页面。

步骤

1. 在*顶部相关资源*列表中、第一个资源是基础资源。列表中的相关资源按与第一个设备相关的活动百分比进行排名。单击链接的关联百分比以查看详细信息。在本示例中、70%的相关关系是利用率、因此基本资源 and 此相关资源的利用率都相同。



2. 要将相关资源添加到性能图表中、请选中要添加的资源的*顶级相关资源*列表中的复选框。默认情况下、每个资源都会提供可用的总数据、但您可以从复选框的菜单中仅选择"读取"或"仅写入"数据。

图表中的每个资源都有不同的颜色、以便您可以比较每个资源的性能测量结果。仅会为选定测量指标绘制适当类型的数据。例如、CPU数据不包括读取或写入指标、因此只有总数据可用。

3. 单击相关资源的链接名称以显示其资产页面。
4. 如果您认为在分析中应考虑的前几个相关资源中未列出某个资源、则可以使用*搜索资产*框来查找该资源。

光纤通道环境监控

使用OnCommand Insight的光纤通道资产页面、您可以监控环境中网络结构的性能和清单、并了解可能出现发生原因 问题的任何更改。

光纤通道资产页面

Insight的资产页面提供有关资源、其拓扑(设备及其连接)、性能图表以及关联资源表的摘要信息。您可以使用网络结构、交换机和端口资产页面监控光纤通道环境。在对光纤通道问题描述 进行故障排除时、每个端口资产的性能图表尤其有用、其中显示了选定最大贡献端口的流量。此外、您还可以在此图表中显示缓冲区到缓冲区信用度量指标和端口错误、Insight会为每个指标显示一个单独的性能图表。

端口指标的性能策略

您可以通过Insight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。您可以根据可用的端口指标为端口创建性能策略。如果发生违反阈值的情况、Insight会通过以下方式检测并在相关资产页面中报告该阈值：显示红色实心圆圈；显示电子邮件警报(如果已配置)；违规信息板或报告违规的任何自定义信息板。

生存时间（TTL）和缩减采样数据

从OnCommand Insight 7.3开始、数据保留或生存时间(TTL)已从7天增加到90天。由于这意味着要处理更多图表和表数据、并且可能会处理成千上万个数据点、因此、数据会在显示之前进行缩减采样。

下抽样可提供图表中数据的统计近似值、让您可以高效地查看数据、而无需显示每个数据点、同时保持所收集数据的准确视图。

为什么需要缩减采样？

Insight 7.3将数据的生存时间(TTL)增加到90天。这意味着、准备要显示在图表和图形中的数据所需的处理量会增加。为了快速高效地显示图表、数据的缩减采样方式可以保持图表的整体形状、而无需处理该图表的每个数据点。



在下抽样期间、不会丢失任何实际数据。您可以按照下面所示的步骤选择查看图表的实际数据，而不是缩减采样数据。

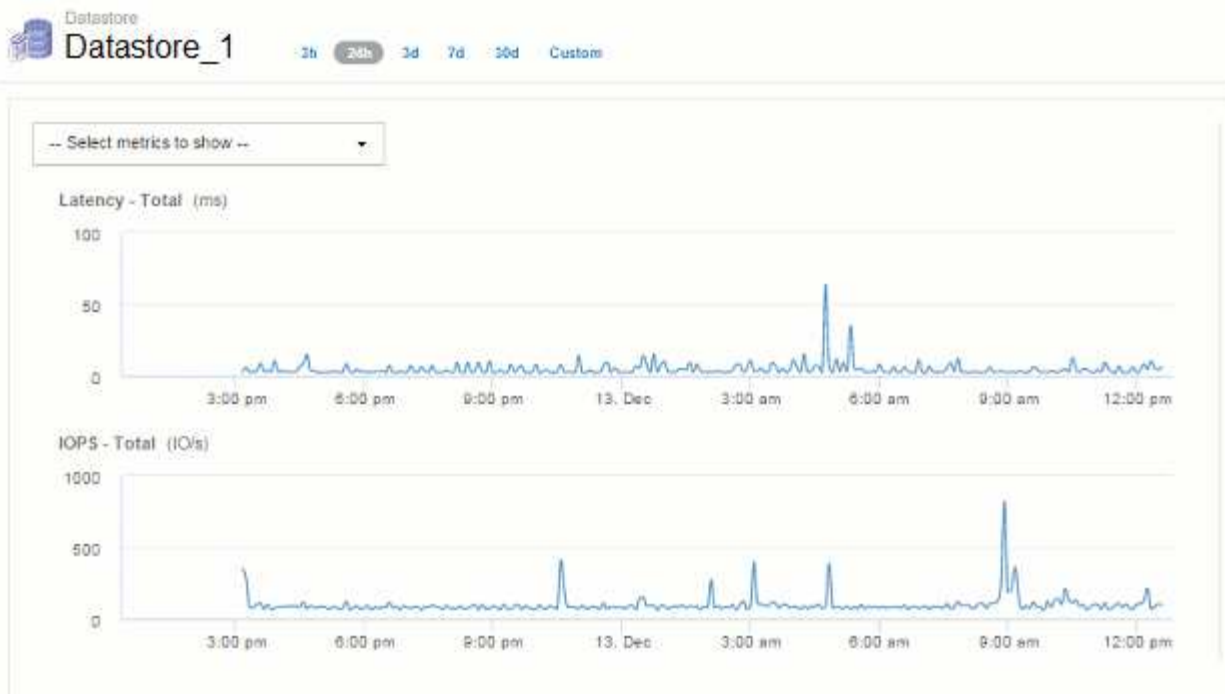
下抽样的工作原理

在以下情况下会对数据进行缩减采样：

- 如果选定时间范围包含 7 天或更短的数据，则不会进行缩减采样。图表显示实际数据。
- 如果您选择的时间范围包含 7 天以上的数据，但少于 1,000 个数据点，则不会进行缩减采样。图表显示实际数据。
- 如果选定时间范围包含 7 天以上的数据且超过 1,000 个数据点，则会对数据进行缩减采样。图表显示近似数据。

以下示例显示了缩减采样的实际操作。第一幅图显示了数据存储库资产页面上24小时内的延迟和IOPS图表、如在资产页面的时间选择器上选择"*24H"所示。您还可以通过选择*自定义*并将时间范围设置为相同的24小时时间段来查看相同的数据。

由于我们选择的时间范围小于 7 天，并且要绘制的数据点少于 1,000 个，因此显示的数据为实际数据。不会发生缩减采样。

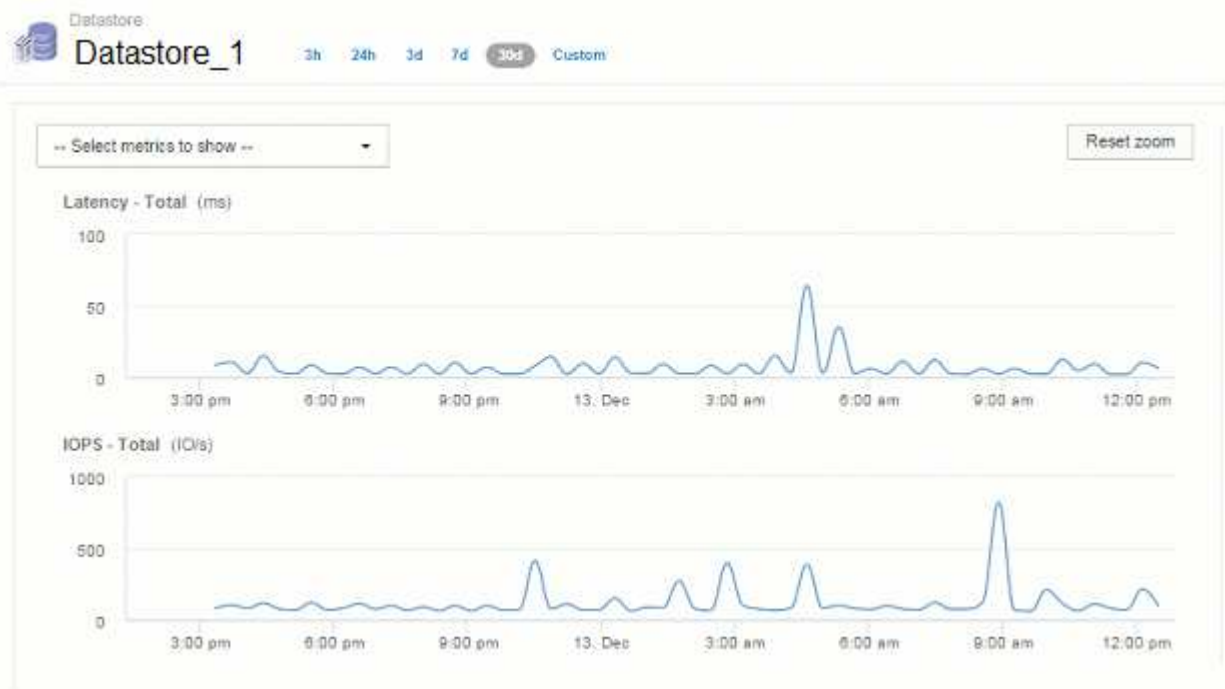


但是、如果要通过在资产页面时间选择器上选择* 30d*来查看数据、或者、如果将自定义时间范围设置为7天以上(或者如果Insight在选定时间段内收集了1、000个以上的数据样本)、则会在显示数据之前对数据进行缩减采样。放大缩减采样图表时，屏幕将继续显示近似数据。



放大缩减采样的图表时，缩放为数字缩放。此时将继续显示近似数据。

您可以在下图中看到这一点，其中时间范围首先设置为 30 天，然后放大图表以显示与上述相同的 24 小时时间段。



缩减采样的图表显示的时间段与上述 " 实际 " 图表相同，因此线条采用相同的通用形状，您可以快速在性能数据中发现有趣的峰值或谷值。



由于缩减采样的近似数据方式，在比较缩减采样与时，图表线可能会略微关闭实际数据，以便在图形中进行更好的对齐。但是，此差异很小，不会影响所显示数据的整体准确性。

缩减采样图表上的违规

查看缩减采样图表时，请注意不会显示违规。要查看违规，您可以执行以下两项操作之一：

- 通过在资产页面时间选择器中选择自定义并输入少于 7 天的时间范围来查看该时间范围的实际数据。将鼠标悬停在每个红点上。工具提示将显示发生的违规。
- 记下时间范围并在违规信息板中查找违规。

删除清单历史记录

从 7.3.2 版开始，Insight 会将清单(基础)更改历史记录保留 90 天。早期版本的 Insight 会保留安装后的所有清单更改历史记录。从旧版 Insight 升级后，旧的清单历史记录将被缩减为、然后保留 90 天。

升级到 OnCommand Insight 的当前版本后，历史记录将根据最近 90 天进行修剪。Insight 会从最早的历史记录开始、以每天一次的 30 天块的形式对历史记录进行删减、直到剩余 90 天的历史记录为止。然后，每天都会对历史记录进行修剪、以便仅保留 90 天的清单更改历史记录。

VM 的 NAS 路径

OnCommand Insight 7.3 支持虚拟机到存储共享的 NAS 路径。这些路径类似于主机到存储共享的 NAS 路径。如果允许 VM 的 IP 地址访问共享、则会创建 NAS 路径。

虚拟机的 NAS 路径显示在内部卷登录页面上。此页面包含一个子系统挂载的存储资源小工具、用于标识 VM 可以访问的内部卷。

- 当虚拟机能够访问后端共享时、将创建 NAS 路径。无法确认虚拟机是否访问共享。
- 关联计算基于延迟和 IOPS、不包括 VM 具有后端存储 NAS 路径的情况。
- 用户可以按启动程序 IP 地址查询共享、但不支持按路径查询。

现在，内部卷的计算资源表还会显示具有 NAS 路径的虚拟机。为每个 VM 提供 CPU 和内存、利用率和性能数据。

数据仓库影响

升级到 OnCommand Insight 7.3 后对数据仓库所做的更改包括以下内容：

- `dwh_inventory.nas_logical` 表将从清单数据集中删除并替换为视图。

包含 NFS 路径表的所有 Insight 7.2.x 报告都会保留下来。

- `dwh_inventory.nas_cr_logical` 表将添加到清单数据集中、其中包括以下内容：
 - 计算资源
 - 内部卷
 - 存储

- NAS共享

容量作为时间序列

在OnCommand Insight 7.3.1中、容量信息会作为时间序列数据进行报告和图表绘制。

以前、从数据源获取的容量信息仅是“时间点”(Point-In-Time、PIT)数据、这意味着它不能在图表中用作时间序列数据。现在、资产的容量值可通过以下方式用作时间序列数据：

- 在表、小工具、专家视图以及显示时间序列数据的任何位置绘制图形
- 使用现有语义应用于存在违规的性能阈值
- 在表达式中使用、并在适当的情况下与其他性能计数器结合使用

请注意、如果您从先前版本的Insight升级、则自定义信息板的查询或筛选器中使用的先前PIT容量值将替换为时间序列容量数据。与先前Insight版本中的等效数据相比、这可能会导致报告或筛选容量数据的方式发生小变化。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。