开始使用
BlueXP classification

NetApp
March 03, 2025

目录

开始使用

了解BlueXP分类

BlueXP分类(Cloud Data Sense)是一项适用于BlueXP的数据监管服务、可扫描企业内部和云数据源、以便对数据进行映射和分类、并确定私有信息。这有助于降低安全性和合规性风险，降低存储成本，并有助于您的数据迁移项目。

重要说明

从2024年5月起、BlueXP版本1.31将作为BlueXP中的核心功能免费提供。不需要分类许可证或订阅。我们还将BlueXP分类功能重点放在NetApp存储系统上、因此、某些未使用或未充分利用的功能已弃用。

"请参见已弃用功能的列表"(英文)

一直使用旧版1.3或更早版本的用户将继续使用该版本、直到其订阅到期为止。

功能

BlueXP分类使用人工智能(AI)、自然语言处理(NLL)和机器学习(ML)来了解它扫描的内容、以便提取实体并对内容进行相应的分类。这样、BlueXP分类就可以提供以下功能区域。

"详细了解BlueXP分类的用例"(英文)

保持合规性

BlueXP分类提供了多种可帮助您实现合规性的工具。您可以使用BlueXP分类来：

- 识别个人身份信息（ PiII ）。
- 根据GDPR、CCPA、PCI和HIPAA隐私法规的要求、识别广泛的敏感个人信息。
- 根据名称或电子邮件地址响应数据主体访问请求(Data Subject Access Requests、DSAar)。

增强安全性

BlueXP分类可以识别可能存在被用于犯罪目的访问风险的数据。您可以使用BlueXP分类来：

- 确定具有打开权限的所有文件和目录(共享和文件夹)、这些文件和目录会公开给您的整个组织或公有。
- 确定位于初始专用位置以外的敏感数据。
- 遵守数据保留策略。
- 使用_policies_自动检测新的安全问题、以便安全人员可以立即采取措施。

优化存储使用

BlueXP分类提供了有助于降低存储总拥有成本(TCO)的工具。您可以使用BlueXP分类来：

- 通过识别重复数据或非业务相关数据来提高存储效率。
- 识别可分层到成本较低的对象存储的非活动数据、从而节省存储成本。 "了解有关从Cloud Volumes ONTAP

系统分层的更多信息"(英文)。 "了解有关从内部ONTAP 系统分层的更多信息"(英文)。

支持的工作环境和数据源

BlueXP分类可以扫描和分析来自以下类型的工作环境和数据源的结构化和非结构化数据：

工作环境

- 适用于 ONTAP 的 Amazon FSX
- Azure NetApp Files
- Cloud Volumes ONTAP （部署在 AWS ， Azure 或 GCP 中）
- 内部 ONTAP 集群
- StorageGRID

数据源

- NetApp文件共享
- 数据库：
  - Amazon Relational Database Service （ Amazon RDS ）
  - MongoDB
  - MySQL
  - Oracle
  - PostgreSQL
  - SAP HANA
  - SQL Server （ MSSQL ）

BlueXP分类支持NFS 3.x、4.0和4.1以及CIFS 1.x、2.0、2.1和3.0。

成本

BlueXP分类现在可免费使用。不需要分类许可证或付费订阅。

基础架构成本

- 在云中安装BlueXP分类需要部署云实例、这会导致从部署该实例的云提供商处收取费用。请参阅。 为每个云提供商部署的实例类型如果您在内部系统上安装BlueXP分类、则不需要任何费用。
- BlueXP分类要求您已部署BlueXP Connector。在许多情况下、由于您在BlueXP中使用的其他存储和服务、您已经有了一个Connector。Connector 实例会从部署该实例的云提供商处收取费用。请参见 "为每个云提供商部署的实例类型"。如果在内部部署系统上安装 Connector ，则不需要任何成本。

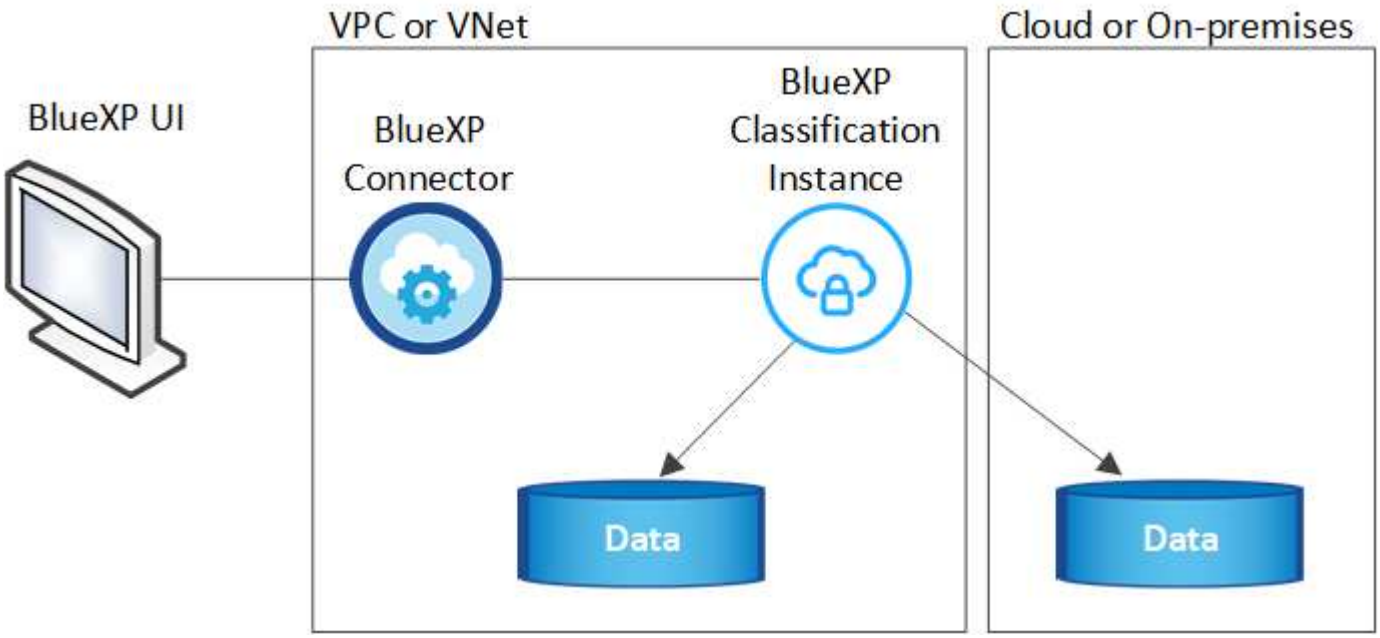
数据传输成本

数据传输成本取决于您的设置。如果BlueXP分类实例和数据源位于同一可用性区域和区域、则不会产生数据传输成本。但是、如果数据源(例如Cloud Volumes ONTAP系统)位于_不同_可用性区域或区域、则云提供商将向您收取数据传输成本。有关详细信息，请参见以下链接：

- "AWS：Amazon Elelic计算云(Amazon EC2)定价"
- "Microsoft Azure ： 带宽定价详细信息"
- "Google Cloud ： 存储传输服务定价"

BlueXP分类实例

在云中部署BlueXP 分类时、BlueXP 会将实例部署在与连接器相同的子网中。 "了解有关连接器的更多信息。"



请注意以下有关默认实例的信息：

- 在AWS中、BlueXP 分类在具有500 GiB GP2磁盘的上运行 "m6i.4xlarge实例"。操作系统映像为 Amazon Linux 2 。在AWS中部署时、如果您要扫描少量数据、则可以选择较小的实例大小。
- 在Azure中、BlueXP 分类在具有500 GiB磁盘的上运行"标准的 D16s_v3 VM"。操作系统映像为Ubuntu 22.04。
- 在GCP中、BlueXP 分类在具有500 GiB标准永久性磁盘的上运行"n2-standard-16 虚拟机"。操作系统映像为Ubuntu 22.04。
- 在默认实例不可用的区域中、BlueXP分类在备用实例上运行。"请参见备用实例类型"(英文)
- 此实例名为 *CloudCompliance* ，并与生成的哈希（ UUID ）串联在一起。例如： *CloudCompliance" — 16bb6564-38AD-4080-9a92 — 36f5fd2f71c7*
- 每个连接器仅部署一个BlueXP分类实例。

您还可以在内部的Linux主机上或首选云提供商的主机上部署BlueXP分类。无论您选择哪种安装方法，软件的工作方式都完全相同。只要该实例可以访问Internet、BlueXP分类软件的升级就会自动进行。

实例应始终保持运行状态、因为BlueXP分类会持续扫描数据。

部署在不同的实例类型

您可以在CPU更少、RAM更少的系统上部署BlueXP 分类。

系统大小	规格	限制
超大	32个CPU、128 GB RAM、1 TiB SSD	最多可扫描5亿个文件。
大型(默认)	16个CPU、64 GB RAM、500 GiB SSD	最多可扫描2.5亿个文件。

在Azure或GCP中部署BlueXP 分类时、如果要使用较小的实例类型、请发送电子邮件至ng-contace-data-sSense@NetApp。com以获取帮助。

BlueXP分类的工作原理

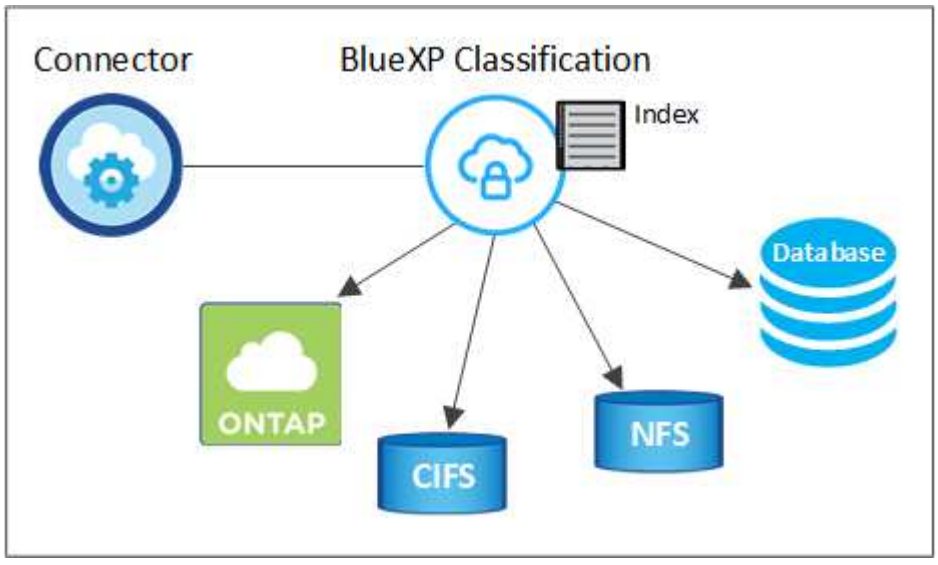
从较高层面来看、BlueXP分类的工作原理如下：

1. 您可以在BlueXP中部署BlueXP分类实例。
2. 您可以对一个或多个数据源启用高级别映射或深度扫描。
3. BlueXP分类使用AI学习流程扫描数据。
4. 您可以使用提供的信息板和报告工具帮助您开展合规和监管工作。

扫描的工作原理

启用BlueXP分类并选择要扫描的存储库(即卷、数据库架构或其他用户数据)后、它会立即开始扫描数据以确定个人数据和敏感数据。在大多数情况下、您应重点扫描实时生产数据、而不是备份、镜像或灾难恢复站点。然后、BlueXP分类会映射您的组织数据、对每个文件进行分类、并在数据中标识和提取实体和预定义模式。扫描的结果是个人信息，敏感个人信息，数据类别和文件类型的索引。

BlueXP分类可通过挂载NFS和CIFS卷与任何其他客户端一样连接到数据。NFS 卷会自动以只读方式访问，而您需要提供 Active Directory 凭据来扫描 CIFS 卷。



完成初始扫描后、BlueXP分类会以轮循方式持续扫描数据、以检测增量更改(这就是保持实例运行至关重要的原因)。

您可以在卷级别或数据库架构级别启用和禁用扫描。

映射扫描与分类扫描之间的区别是什么

您可以在BlueXP 分类中执行两种类型的扫描：

- 仅映射扫描仅提供数据的概览，并对选定的数据源执行扫描。与map和分类扫描相比、仅映射扫描所需时间更短、因为不会访问文件来查看其中的数据。
- 地图和分类扫描可对您的数据进行深度扫描。

通过仅映射扫描、您可以快速扫描数据并确定可能需要更多研究的数据源、然后可以对这些数据源执行地图和分类扫描。

下表显示了一些差异：

功能	对扫描进行映射和分类	仅映射扫描
扫描速度	慢	快速
定价	免费	免费
容量	限制为500 TB	限制为500 TB
文件类型和已用容量的列表	是	是
文件数和已用容量	是	是
文件的期限和大小	是	是
能够运行"数据映射报告"	是	是
数据调查页面以查看文件详细信息	是	否
搜索文件中的名称	是	否
创建"策略"以提供自定义搜索结果	是	否
能够运行其他报告	是	否
能够从文件中查看元数据*	否	是

*映射扫描期间从文件中提取以下元数据：

- Working environment
- Working environment type
- 存储库
- 文件类型
- Used capacity
- 文件数
- 文件大小
- 文件创建
- 文件上次访问
- 文件上次修改时间
- 文件发现时间

- 权限提取

监管信息板差异：

功能	映射和分类	映射
陈旧数据	是	是
非业务数据	是	是
文件重复	是	是
预定义策略	是	否
自定义策略	是	是
DDA报告	是	是
映射报告	是	是
灵敏度级别检测	是	否
具有广泛权限的敏感数据	是	否
打开权限	是	是
数据存在期限	是	是
数据大小	是	是
类别	是	否
文件类型	是	是

合规性信息板差异：

功能	映射和分类	映射
个人信息	是	否
敏感的个人信息	是	否
隐私风险评估报告	是	否
HIPAA 报告	是	否
PCI DSS 报告	是	否

调查筛选差异：

功能	映射和分类	映射
策略	是	是
Working environment type	是	是
Working environment	是	是
存储库	是	是
文件类型	是	是
文件大小	是	是
创建时间	是	是
发现时间	是	是
上次修改时间	是	是
上次访问	是	是
打开权限	是	是
文件目录路径	是	是
类别	是	否
敏感度	是	否
标识符数量	是	否
个人数据	是	否
敏感的个人数据	是	否
数据主题	是	否
重复	是	是
分类状态	是	状态始终为"洞察力有限"
扫描分析事件	是	是
文件哈希	是	是
具有访问权限的用户数	是	是
用户/组权限	是	是
文件所有者	是	是
目录类型	是	是

BlueXP分类扫描数据的速度

扫描速度受网络延迟、磁盘延迟、网络带宽、环境大小和文件分发大小的影响。

- 执行仅映射扫描时、BlueXP 分类每天可扫描100-150 Tib的数据。
- 执行地图和分类扫描时、BlueXP 分类每天可扫描15-40 Tib的数据。

BlueXP 分类分类的信息

BlueXP分类可收集数据(文件)、编制索引并为其分配类别。BlueXP分类索引的数据包括以下内容：

- 关于文件的标准元数据：文件类型、大小、创建和修改日期等。
- 个人数据：个人身份信息(Pi2)，如电子邮件地址、身份号码或信用卡号码。"了解有关个人数据的更多信息"(英文)
- 敏感个人数据：特殊类型的敏感个人信息(SPii)、如GDPR和其他隐私法规定义的健康数据、种族或政治观点。"了解有关敏感个人数据的更多信息"(英文)
- 类别：BlueXP 分类将其扫描的数据划分为不同类型的类别。类别是基于 AI 对每个文件的内容和元数据的分析而得出的主题。"了解有关类别的更多信息"(英文)
- **Types**：BlueXP 分类采用它扫描的数据并按文件类型进行细分。"了解有关类型的更多信息"(英文)
- 名称实体识别：BlueXP 分类使用AI从文档中提取人们的自然名称。"了解如何响应数据主体访问请求"(英文)

网络概述

BlueXP部署BlueXP分类实例、其中包含一个安全组、用于从连接器实例建立入站HTTP连接。

在SaaS模式下使用BlueXP时、与BlueXP的连接通过HTTPS提供、浏览器和BlueXP分类实例之间发送的私有数据通过使用TLS 1.2的端到端加密进行保护、这意味着NetApp和第三方无法读取。

出站规则完全开放。要安装和升级BlueXP分类软件以及发送使用情况指标、需要访问Internet。

如果您有严格的网络要求，"了解BlueXP分类所联系的端点"。

BlueXP 分类中的用户角色

为每个用户分配的角色在BlueXP 和BlueXP 分类中提供不同的功能。有关详细信息，请参阅以下内容：

- "BlueXP IAM角色"(在标准模式下使用BlueXP 时)
- "BlueXP 帐户角色"(在受限模式或专用模式下使用BlueXP 时)

部署BlueXP分类

您应使用哪种BlueXP分类部署?

您可以通过不同方式部署BlueXP分类。了解哪种方法符合您的需求。

BlueXP分类可通过以下方式部署：

- "使用BlueXP在云中部署"(英文)BlueXP将在与BlueXP Connector相同的云提供商网络中部署BlueXP分类实例。
- "在可访问Internet的Linux主机上安装"(英文)在网络中的Linux主机或云中可访问Internet的Linux主机上安装BlueXP分类。如果您希望使用同时位于内部的BlueXP分类实例扫描内部ONTAP系统、则此类安装可能是一个不错的选择、但这不是一项要求。
- "在内部站点的Linux主机上安装、无需访问Internet"也称为_private模式。_此类安装使用安装脚本、无法连

接到BlueXP SaaS层。

可以访问Internet的Linux主机上的安装以及不能访问Internet的Linux主机上的内部安装都使用安装脚本。该脚本首先会检查系统和环境是否满足前提条件。如果满足这些前提条件、安装将开始。如果要独立于运行BlueXP分类安装来验证前提条件、则可以下载一个单独的软件包、该软件包仅测试前提条件。

请参阅 "检查Linux主机是否已准备好安装BlueXP分类"。

使用**BlueXP**在云中部署**BlueXP**分类

完成几个步骤、在云中部署BlueXP分类。BlueXP将在与BlueXP Connector相同的云提供商网络中部署BlueXP分类实例。

请注意，您也可以"在可访问Internet的Linux主机上安装BlueXP分类"。如果您更喜欢使用同时位于内部的BlueXP分类实例扫描内部ONTAP 系统、则此类安装可能是一个不错的选择、但这不是一项要求。无论您选择哪种安装方法，软件的工作方式都完全相同。

快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。

1 创建接头

如果您还没有 Connector ，请立即创建一个 Connector 。请参阅 "在 AWS 中创建连接器"、 "在 Azure 中创建连接器"或 "在 GCP 中创建连接器"。

您也可以 "在内部安装 Connector"在网络中的Linux主机上或云中的Linux主机上运行。

2 查看前提条件

确保您的环境可以满足前提条件。这包括实例的出站Internet访问、连接器与BlueXP分类之间通过端口443进行的连接等。请参见完整列表(英文)

3 部署**BlueXP** 分类

启动安装向导以在云中部署BlueXP分类实例。

创建连接器

如果您还没有 Connector ，请在云提供商中创建一个 Connector 。请参阅 "在 AWS 中创建连接器"或 "在 Azure 中创建连接器"、或 "在 GCP 中创建连接器"。在大多数情况下，您可能在尝试激活BlueXP 分类之前设置了连接器，因为大多数，但在某些情况下，您需要立即设置一个连接器 "BlueXP功能需要使用Connector"。

在某些情况下，您必须使用部署在特定云提供商中的 Connector：

- 在AWS中的Cloud Volumes ONTAP或适用于ONTAP存储分段的Amazon FSx中扫描数据时、您可以使用AWS中的Connector。
- 在Azure或Azure NetApp Files 中扫描Cloud Volumes ONTAP 中的数据时、您可以使用Azure中的连接器。

- 对于Azure NetApp Files 、必须将其部署在与要扫描的卷相同的区域中。

- 在 GCP 的 Cloud Volumes ONTAP 中扫描数据时，您可以在 GCP 中使用连接器。

使用任何这些Cloud Connector时、都可以扫描内部ONTAP系统、NetApp文件共享和数据库。

请注意、您也可以 "在内部安装 Connector"在网络或云中的Linux主机上运行。一些计划在本机安装BlueXP分类的用户也可以选择在本机安装Connector。

如您所见，在某些情况下，您可能需要使用 "多个连接器"。

政府区域支持

如果Connector部署在政府区域(AWS GovCloud、Azure Gov或Azure DoD)中、则支持BlueXP分类。以这种方式部署时、BlueXP分类具有以下限制：

"请参见有关在政府区域部署Connector的详细信息"(英文)

查看前提条件

在云中部署BlueXP分类之前、请查看以下前提条件、以确保您的配置受支持。在云中部署BlueXP分类时、它与连接器位于同一子网中。

从**BlueXP**分类启用出站**Internet**访问

BlueXP分类需要出站Internet访问。如果您的虚拟或物理网络使用代理服务器进行Internet访问、请确保BlueXP分类实例具有出站Internet访问权限以联系以下端点。代理必须不透明-我们目前不支持透明代理。

根据您是在AWS、Azure还是GCP中部署BlueXP分类、查看下表。

AWS所需的端点

端点	目的
https://api.bluexp.netapp.com	与包括NetApp帐户在内的BlueXP服务进行通信。
\https：//https：NetApp-cloud-account.auth0.com https://auth0.com	与BlueXP网站通信以实现集中式用户身份验证。
https://cloud-compliance-support-NetApp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	提供对软件映像、清单和模板的访问。
https://kinesis.us-east-1.amazonaws.com	使 NetApp 能够从审计记录流化数据。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	启用BlueXP分类以访问和下载清单和模板、并发送日志和指标。

Azure所需端点

端点	目的
https://api.bluexp.netapp.com	与包括NetApp帐户在内的BlueXP服务进行通信。
\https：//https：NetApp-cloud-account.auth0.com https://auth0.com	与BlueXP网站通信以实现集中式用户身份验证。
https://support.compliance.api BlueXP ．NetApp．com/\https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	可用于访问软件映像，清单，模板以及发送日志和指标。
https://support.compliance.api BlueXP ．NetApp．com/	使 NetApp 能够从审计记录流化数据。

GCP所需的端点

端点	目的
https://api.bluexp.netapp.com	与包括NetApp帐户在内的BlueXP服务进行通信。
\https：//https：NetApp-cloud-account.auth0.com https://auth0.com	与BlueXP网站通信以实现集中式用户身份验证。

端点	目的
https://support.compliance.api BlueXP ．NetApp．com/\https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	可用于访问软件映像，清单，模板以及发送日志和指标。
https://support.compliance.api BlueXP ．NetApp．com/	使 NetApp 能够从审计记录流化数据。

确保**BlueXP**具有所需权限

确保BlueXP有权为BlueXP分类实例部署资源和创建安全组。您可以在中找到最新的BlueXP 权限 "NetApp提供的策略"。

确保**BlueXP Connector**可以访问**BlueXP**分类

确保连接器与BlueXP分类实例之间的连接。连接器的安全组必须允许通过端口443传入和传出BlueXP分类实例的流量。通过此连接、可以部署BlueXP分类实例、并可在合规性和监管选项卡中查看信息。在AWS和Azure中的政府地区支持BlueXP分类。

AWS和AWS GovCloud部署需要其他入站和出站安全组规则。有关详细信息、请参见。 "AWS 中连接器的规则"

Azure和Azure政府部署还需要其他入站和出站安全组规则。有关详细信息、请参见。 "Azure 中连接器的规则"

确保您可以保持**BlueXP**分类运行

BlueXP分类实例需要持续扫描数据。

确保**Web**浏览器连接到**BlueXP**分类

启用BlueXP分类后、确保用户从连接到BlueXP分类实例的主机访问BlueXP界面。

BlueXP分类实例使用专用IP地址来确保索引数据不可供Internet访问。因此、用于访问BlueXP的Web浏览器必须连接到该专用IP地址。此连接可以来自与云提供商(例如VPN)的直接连接、也可以来自与BlueXP分类实例位于同一网络中的主机。

检查 **vCPU** 限制

确保云提供商的vCPU限制允许部署具有所需核心数的实例。您需要验证运行BlueXP的区域中相关实例系列的vCPU限制。"请参见所需的实例类型"(英文)

有关 vCPU 限制的详细信息，请参见以下链接：

- "AWS 文档： Amazon EC2 服务配额"
- "Azure 文档：虚拟机 vCPU 配额"
- "Google Cloud 文档：资源配额"

在云中部署**BlueXP**分类

按照以下步骤在云中部署BlueXP分类实例。Connector将在云中部署实例、然后在该实例上安装BlueXP分类软

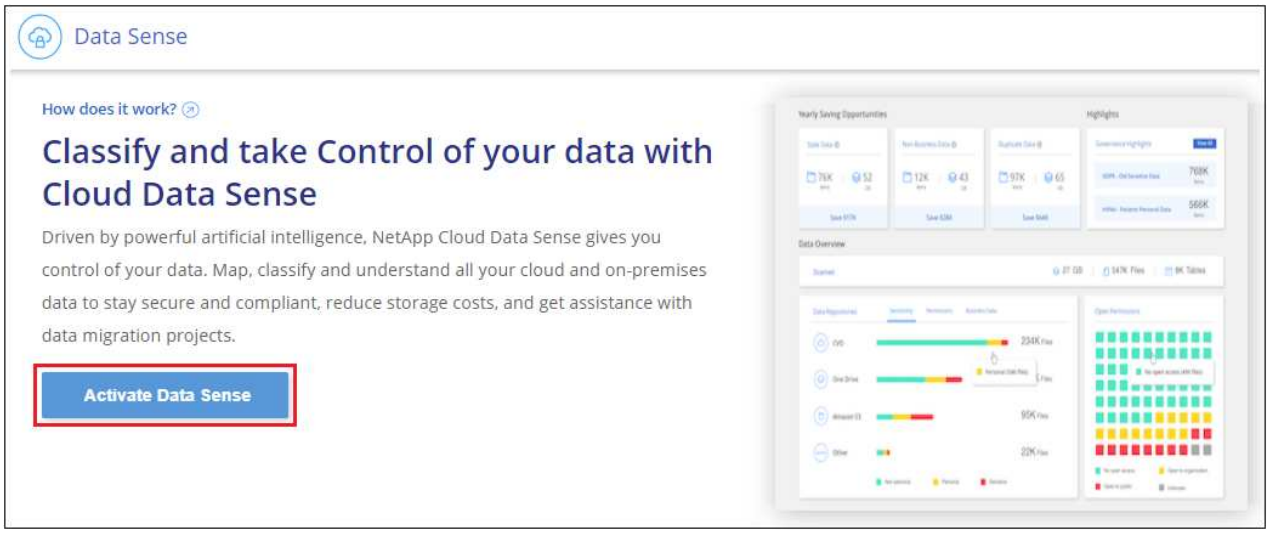
件。

在缺省实例类型不可用的区域中，BlueXP 分类在上运行"备用实例类型"。

在**AWS**中部署

步骤

1. 从BlueXP左侧导航菜单中、单击*监管>分类*。



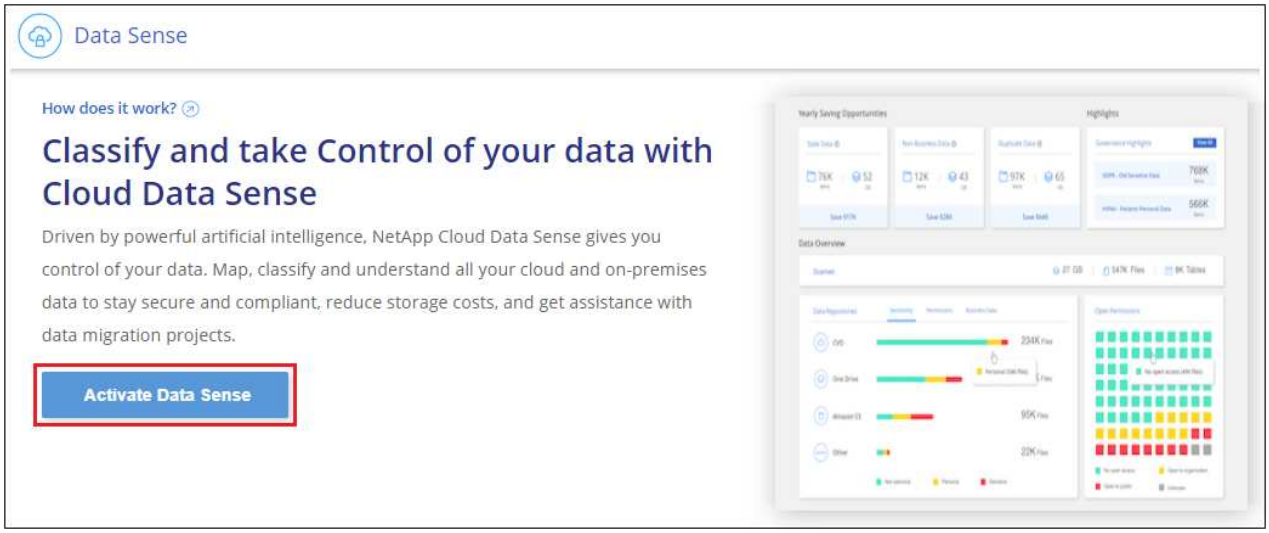
2. 单击 * 激活数据感知 * 。
3. 在_Installation_page中、单击*部署>部署*以使用"大型"实例大小并启动云部署向导。
4. 向导将在完成部署步骤时显示进度。如果遇到任何问题、它将停止并提示输入。

5. 部署实例并安装BlueXP分类后，单击*继续配置*转到_Configuration_页面。

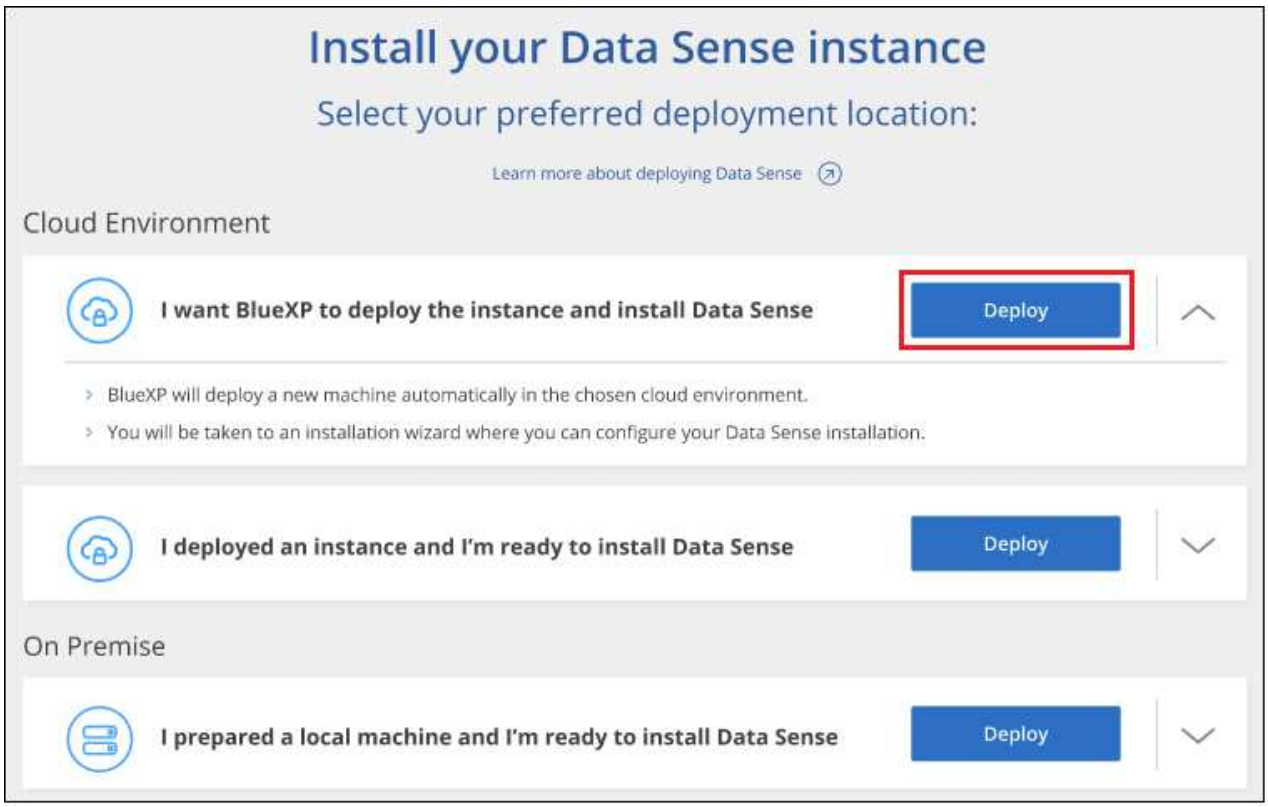
在**Azure**中部署

步骤

1. 从BlueXP左侧导航菜单中、单击*监管>分类*。
2. 单击 * 激活数据感知 * 。



3. 单击*部署*以启动云部署向导。



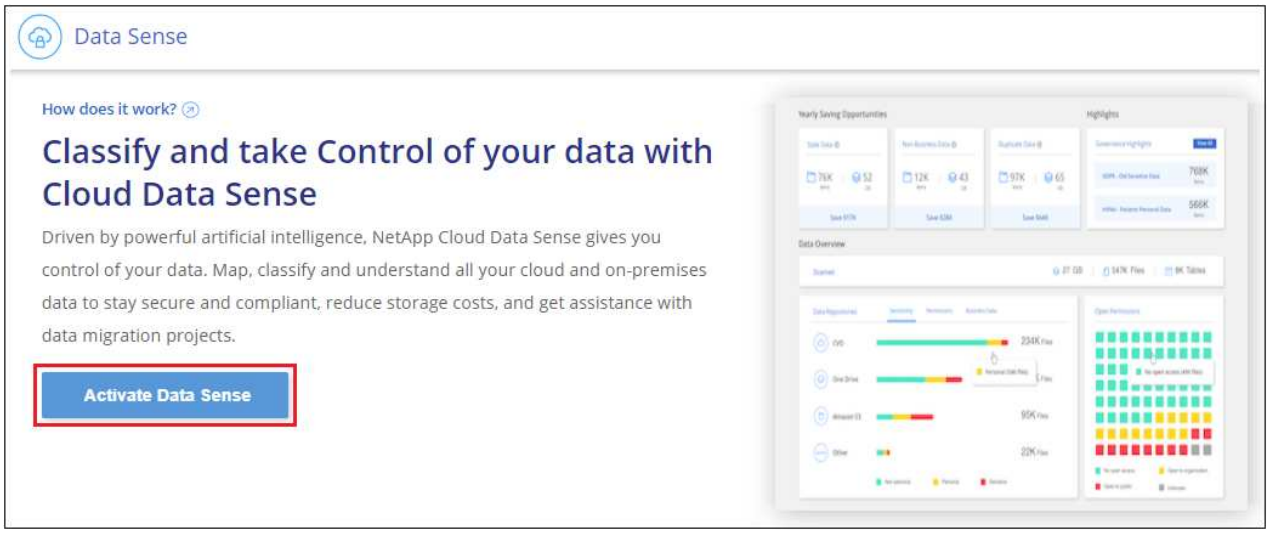
4. 向导将在完成部署步骤时显示进度。如果遇到任何问题、它将停止并提示输入。

5. 部署实例并安装BlueXP分类后，单击*继续配置*转到_Configuration_页面。

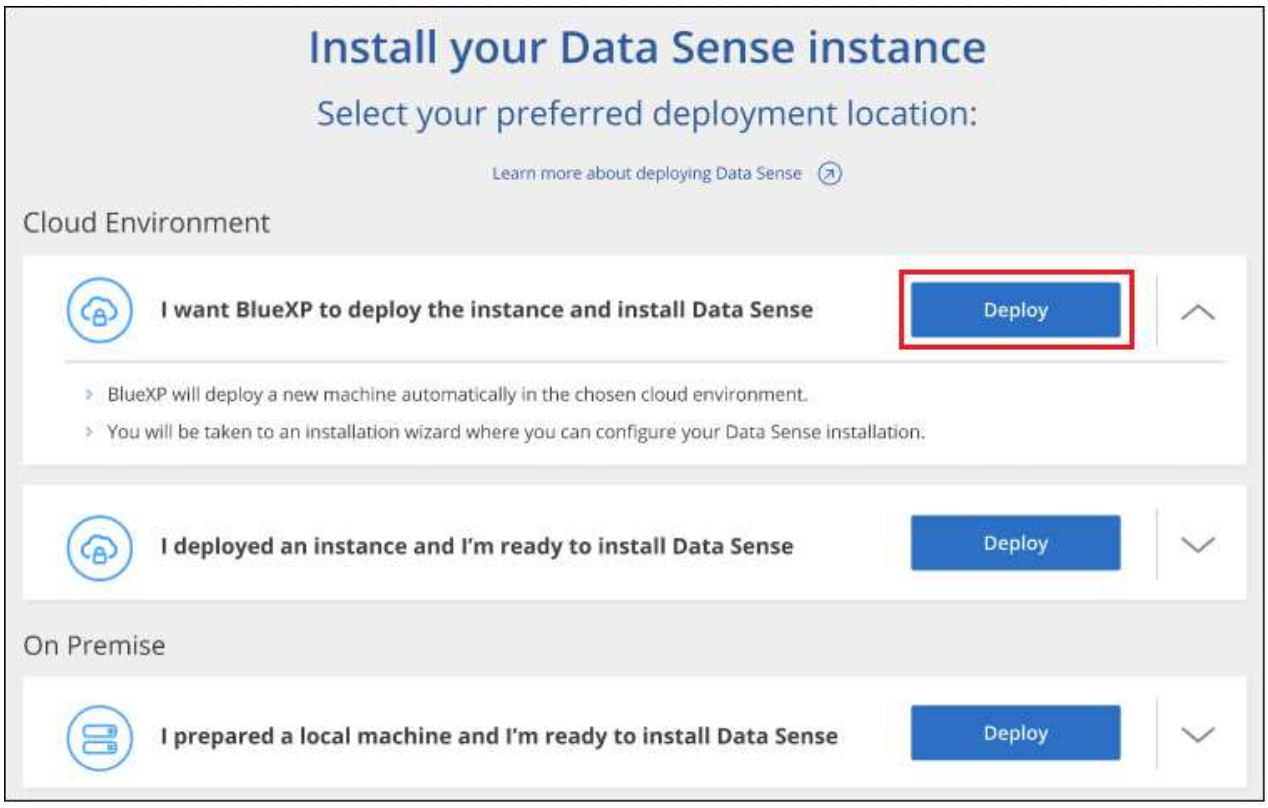
在**Google Cloud**中部署

步骤

1. 从BlueXP左侧导航菜单中、单击*监管>分类*。
2. 单击 * 激活数据感知 * 。



3. 单击*部署*以启动云部署向导。



4. 向导将在完成部署步骤时显示进度。如果遇到任何问题、它将停止并提示输入。

5. 部署实例并安装BlueXP分类后，单击*继续配置*转到_Configuration_页面。

结果

BlueXP在云提供商中部署BlueXP分类实例。

只要这些实例具有Internet连接、BlueXP Connector和BlueXP分类软件的升级就会自动完成。

下一步行动

在配置页面中，您可以选择要扫描的数据源。

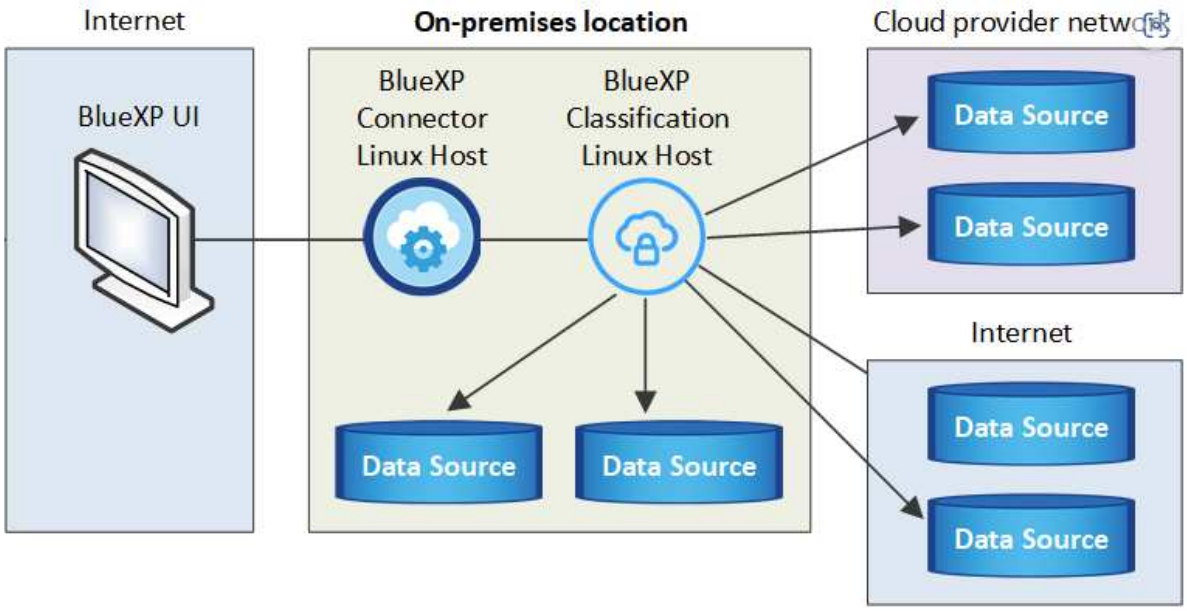
在可访问**Internet**的主机上安装**BlueXP**分类

完成几个步骤、在网络中的Linux主机或云中可访问Internet的Linux主机上安装BlueXP分类。在此安装过程中、您需要在网络或云中手动部署Linux主机。

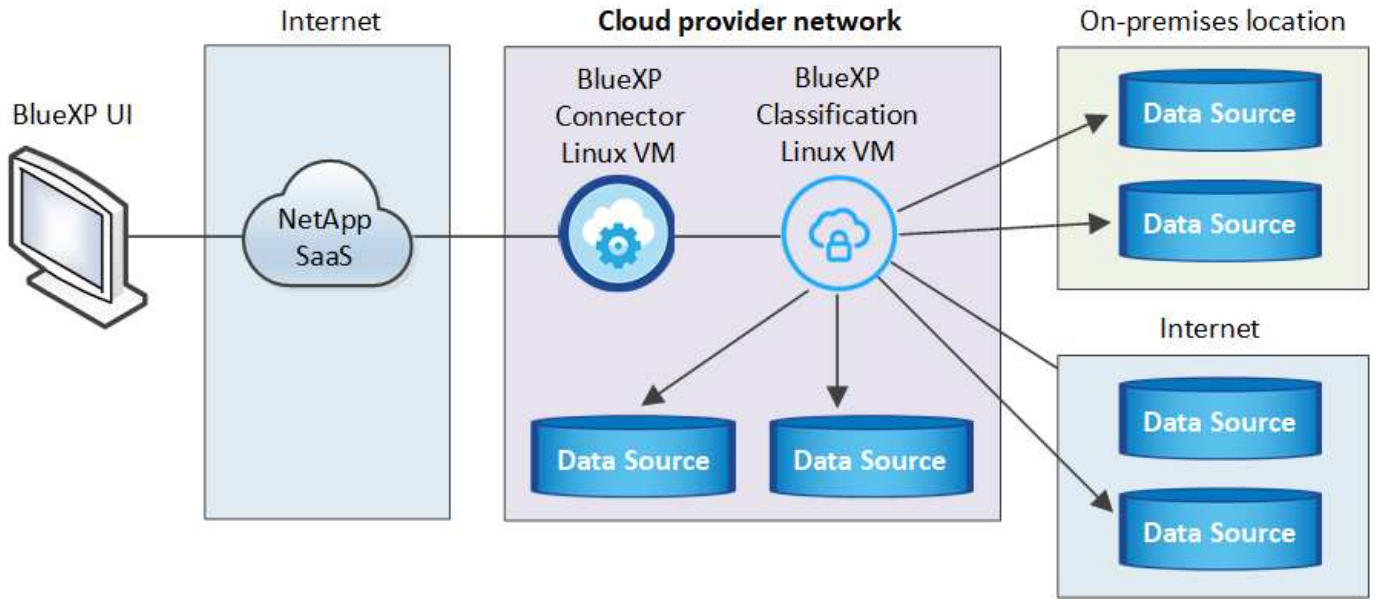
如果您更喜欢使用同时位于内部的BlueXP 分类实例扫描内部ONTAP系统、则内部安装可能是一个不错的选择、但这不是一项要求。无论您选择哪种安装方法，软件的工作方式都完全相同。

BlueXP分类安装脚本首先会检查系统和环境是否满足所需的前提条件。如果满足所有前提条件、则安装将开始。如果要独立于运行BlueXP分类安装来验证前提条件、则可以下载一个单独的软件包、该软件包仅测试前提条件。"请参见How to check if your Linux host is ready to install BlueXP classification"(英文)

Linux主机_in your premises_上的典型安装包含以下组件和连接。



在Linux主机_in the clones_上、典型安装包含以下组件和连接。



对于传统版本1.3及更早版本，如果需要在多个主机上安装BlueXP 分类，请参见"在无法访问Internet的多个主机上安装BlueXP分类"。

您也可以"在无法访问Internet的内部站点中安装BlueXP分类"。

快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。

1 创建接头

如果您还没有Connector、请 "在内部部署 Connector"在网络中的Linux主机上或云中的Linux主机上使用。

您还可以与云提供商一起创建Connector。请参阅 "在 AWS 中创建连接器"、 "在 Azure 中创建连接器"或 "在 GCP 中创建连接器"。

2 查看前提条件

确保您的环境可以满足前提条件。这包括实例的出站Internet访问、连接器与BlueXP分类之间通过端口443进行的连接等。请参见完整列表(英文)

您还需要一个符合的Linux系统以下要求。

3 下载并部署**BlueXP** 分类

从NetApp 支持站点 下载Cloud BlueXP分类软件、并将安装程序文件复制到您计划使用的Linux主机。然后启动安装向导并按照提示部署BlueXP分类实例。

创建连接器

在安装和使用BlueXP分类之前、需要BlueXP Connector。在大多数情况下，您可能在尝试激活BlueXP 分类之

前设置了连接器，因为大多数，但在某些情况下，您需要立即设置一个连接器 "BlueXP功能需要使用Connector"。

要在云提供商环境中创建一个，请参见 "在 AWS 中创建连接器"、 "在 Azure 中创建连接器"或 "在 GCP 中创建连接器"。

在某些情况下，您必须使用部署在特定云提供商中的 Connector：

- 在AWS中的Cloud Volumes ONTAP或Amazon FSx for ONTAP中扫描数据时、您可以使用AWS中的Connector。
- 在Azure或Azure NetApp Files 中扫描Cloud Volumes ONTAP 中的数据时、您可以使用Azure中的连接器。

  对于Azure NetApp Files 、必须将其部署在与要扫描的卷相同的区域中。

- 在 GCP 的 Cloud Volumes ONTAP 中扫描数据时，您可以在 GCP 中使用连接器。

可以使用这些Cloud Connector扫描内部ONTAP系统、NetApp文件共享和数据库帐户。

请注意、您也可以 "在内部部署 Connector"在网络中的Linux主机上或云中的Linux主机上运行。一些计划在本机安装BlueXP分类的用户也可以选择在本机安装Connector。

安装BlueXP分类时、您需要连接器系统的IP地址或主机名。如果您在内部安装了Connector、则可以获得此信息。如果Connector部署在云中、您可以从BlueXP控制台找到此信息：单击帮助图标、选择*支持*、然后单击*蓝XP连接器*。

准备 **Linux** 主机系统

BlueXP分类软件必须在满足特定操作系统要求、RAM要求、软件要求等的主机上运行。Linux主机可以位于您的网络中、也可以位于云中。

确保您可以保持BlueXP分类运行。BlueXP分类机需要持续扫描数据。

- 与其他应用程序共享的主机不支持BlueXP分类-该主机必须是专用主机。
- 在内部构建主机系统时、您可以根据计划进行BlueXP分类扫描的数据集大小在这些系统大小中进行选择。

系统大小	**CPU**	**RAM (**必须禁用交换内存**)**	磁盘
超大	32个CPU	128 GB RAM	• 1 TiB SSD (位于/上)或100 GiB (位于/opt上) • 在/var/lib/Docker上提供了»»»»»»»»»»»»»»»»»»»»»» • /tmp 上 5 GiB • *对于Podman，/tmp*上为5 GB • *对于Podman，/var/tmp*上为30 GB

系统大小	CPU	RAM (必须禁用交换内存)	磁盘
大型	16个CPU	64 GB RAM	• 500 GiB SSD (位于/上)或100 GiB (位于/opt上) • 395 GiB可从/var/lib/Docker或Podman /var/lib/containers或Podman /var/lib/containers获得 • /tmp 上 5 GiB • *对于Podman，/tmp*上为5 GB • *对于Podman，/var/tmp*上为30 GB

- 在云中为BlueXP分类安装部署计算实例时、我们建议使用满足上述"大型"系统要求的系统：
  - * Amazon Elelic计算云(Amazon EC2)实例类型*：建议使用"m6i.4x大"。"请参见其他AWS实例类型"(英文)
  - * Azure虚拟机大小*：建议使用"Standard_d16s_v3_"。"请参见其他Azure实例类型"(英文)
  - * GCP计算机类型*：我们建议使用"n2-standard-16"。"请参见其他GCP实例类型"(英文)
- **UNIX**文件夹权限：需要以下最低UNIX权限：

文件夹	最小权限
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/Docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- * 操作系统 * ：
  - 以下操作系统要求使用Docker容器引擎：
    - Red Hat Enterprise Linux 7.8和7.9版
    - Ubuntu 22.04 (需要BlueXP分类版本1.23或更高版本)
    - Ubuntu 24.04 (需要BlueXP分类版本1.23或更高版本)
  - 以下操作系统要求使用Podman容器引擎、并且需要BlueXP分类版本1.3或更高版本：
    - Red Hat Enterprise Linux 8.8、8.10、9.0、9.1、9.2、9.3、9.4和9.5版
  - 必须在主机系统上启用高级矢量扩展(AVX)。
- * Red Hat订阅管理*：主机必须向Red Hat订阅管理注册。如果未注册、系统将无法在安装期间访问存储库来更新所需的第三方软件。
- 其他软件：在安装BlueXP分类之前、必须在主机上安装以下软件：
  - 根据您使用的操作系统、您需要安装以下容器引擎之一：

- Docker引擎19.3.1或更高版本。 "查看安装说明"(英文)。
- Podman版本4或更高版本。要安装Podman，请输入 (`sudo yum install podman netavark -y`)。

- Python 3.6或更高版本。 "查看安装说明"(英文)。
  - **NTP**注意事项：NetApp建议将BlueXP分类系统配置为使用网络时间协议(NTP)服务。BlueXP分类系统和BlueXP Connector系统之间的时间必须同步。
- **Firewalld**注意事项：如果您计划使用 `firewalld`，建议您在安装BlueXP 分类之前启用它。运行以下命令进行配置 `firewalld`、使其与BlueXP 分类兼容：

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

如果您计划使用其他BlueXP分类主机作为扫描程序节点、请此时将这些规则添加到主系统：

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

请注意、每当启用或更新设置时、都必须重新启动Docker或Podman `firewalld`。

安装后无法更改BlueXP分类主机系统的IP地址。

从**BlueXP**分类启用出站**Internet**访问

BlueXP分类需要出站Internet访问。如果您的虚拟或物理网络使用代理服务器进行Internet访问、请确保BlueXP分类实例具有出站Internet访问权限以联系以下端点。

端点	目的
https://api.bluexp.netapp.com	与包括NetApp帐户在内的BlueXP服务进行通信。
\https：//https：NetApp-cloud-account.auth0.com https://auth0.com	与BlueXP网站通信以实现集中式用户身份验证。
https://support.compliance.api BlueXP ．NetApp．com/\https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	可用于访问软件映像，清单，模板以及发送日志和指标。

端点	目的
https://support.compliance.api BlueXP ．NetApp．com/	使 NetApp 能够从审计记录流化数据。
https://github.com/docker https://download.docker.com	提供Docker安装的必备软件包。
http://packages.ubuntu.com/ http://archive.ubuntu.com	提供Ubuntu安装的必备软件包。

验证是否已启用所有必需的端口

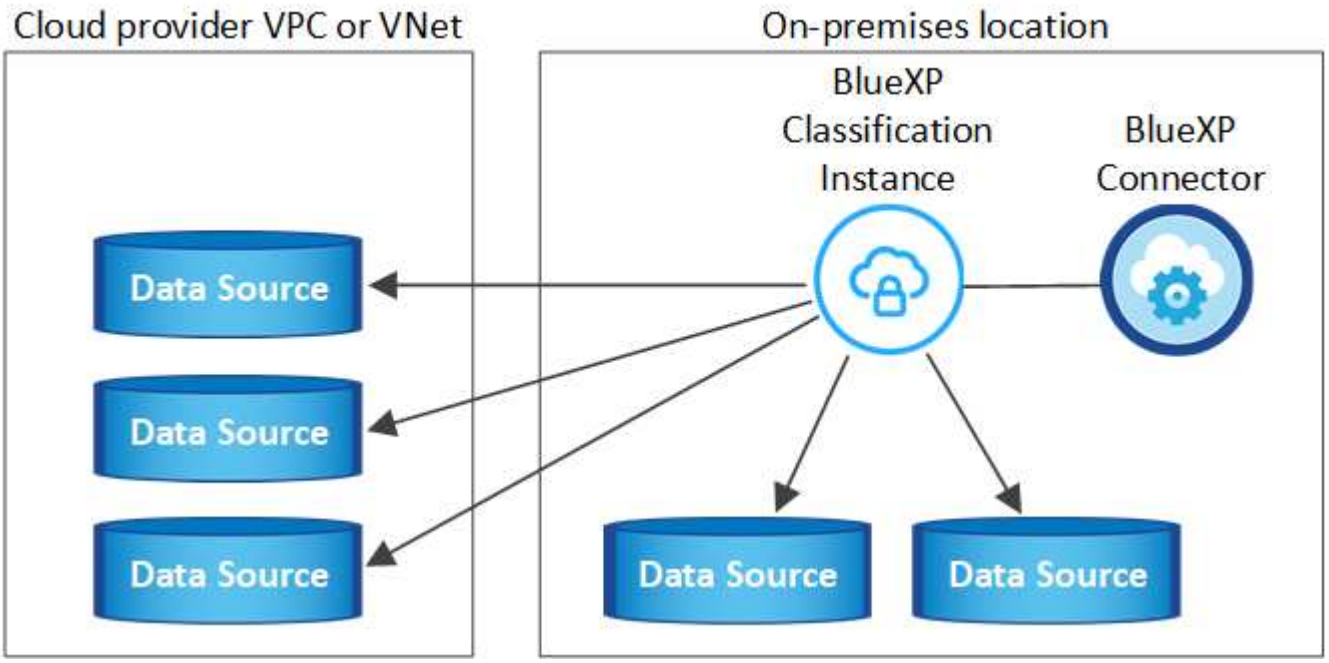
您必须确保所有必需的端口均已打开、可供Connector、BlueXP分类、Active Directory和数据源之间进行通信。

连接类型	端口	说明
连接器<> BlueXP分类	8080 (TCP)、443 (TCP)和80。9000	连接器的防火墙或路由规则必须允许通过端口443传入和传出BlueXP分类实例的流量。确保端口8080已打开、以便您可以在BlueXP中查看安装进度。如果在Linux主机上使用防火墙、则Ubuntu服务器中的内部进程需要端口9000。
Connector <> ONTAP 集群(NAS)	443 (TCP)	BlueXP使用HTTPS发现ONTAP 集群。如果使用自定义防火墙策略，则它们必须满足以下要求： • Connector 主机必须允许通过端口 443 进行出站 HTTPS 访问。如果Connector位于云中、则预定义的防火墙或路由规则允许所有出站通信。 • ONTAP 集群必须允许通过端口 443 进行入站 HTTPS 访问。默认的“管理”防火墙策略允许从所有 IP 地址进行入站 HTTPS 访问。如果您修改了此默认策略，或者创建了自己的防火墙策略，则必须将 HTTPS 协议与该策略关联，并启用从 Connector 主机进行访问。
BlueXP分类<> ONTAP 集群	• 对于NFS - 111 (tcp\udp)和2049 (tcp\udp) • 对于CIFS - 139 (TCP/UDP)和445 (TCP/UDP)	BlueXP分类需要与每个Cloud Volumes ONTAP 子网或内置ONTAP 系统建立网络连接。Cloud Volumes ONTAP 的防火墙或路由规则必须允许从BlueXP分类实例进行入站连接。 确保这些端口对BlueXP分类实例开放： • 对于NFS—111和2049 • 对于CIFS—139和445 NFS卷导出策略必须允许从BlueXP分类实例进行访问。

连接类型	端口	说明
BlueXP分类<> Active Directory	389 (TCP和UDP)、636 (TCP)、3268 (TCP)和3369 (TCP)	您必须已为公司中的用户设置 Active Directory 。此外、BlueXP分类需要Active Directory凭据才能扫描CIFS卷。 您必须具有 Active Directory 的信息： • DNS 服务器 IP 地址或多个 IP 地址 • 服务器的用户名和密码 • 域名（ Active Directory 名称） • 是否使用安全 LDAP （ LDAPS ） • LDAP 服务器端口（对于 LDAP ，通常为 389 ；对于安全 LDAP ，通常为 636 ）

在**Linux**主机上安装**BlueXP**分类

对于典型配置，您将在一个主机系统上安装该软件。请在此处查看这些步骤(英文)



有关部署BlueXP 分类之前的完整要求列表、请参见准备 Linux 主机系统和查看前提条件。

只要该实例具有Internet连接、BlueXP分类软件的升级就会自动进行。

如果软件安装在内部环境中、BlueXP分类当前无法扫描S3存储分段、Azure NetApp Files 或FSx for ONTAP。在这些情况下、您需要在云中为不同的数据源部署单独的BlueXP 分类连接器和实例 "在连接器之间切换"。

典型配置的单主机安装

在单个内部部署主机上安装BlueXP分类软件时、请查看相关要求并遵循以下步骤。

"观看此视频"以了解如何安装BlueXP 分类。

请注意、安装BlueXP分类时会记录所有安装活动。如果在安装期间遇到任何问题、您可以查看安装审核日志的内容。它会写入到 `/opt/netapp/install_logs/`。"请单击此处查看更多详细信息"(英文)

您需要的内容

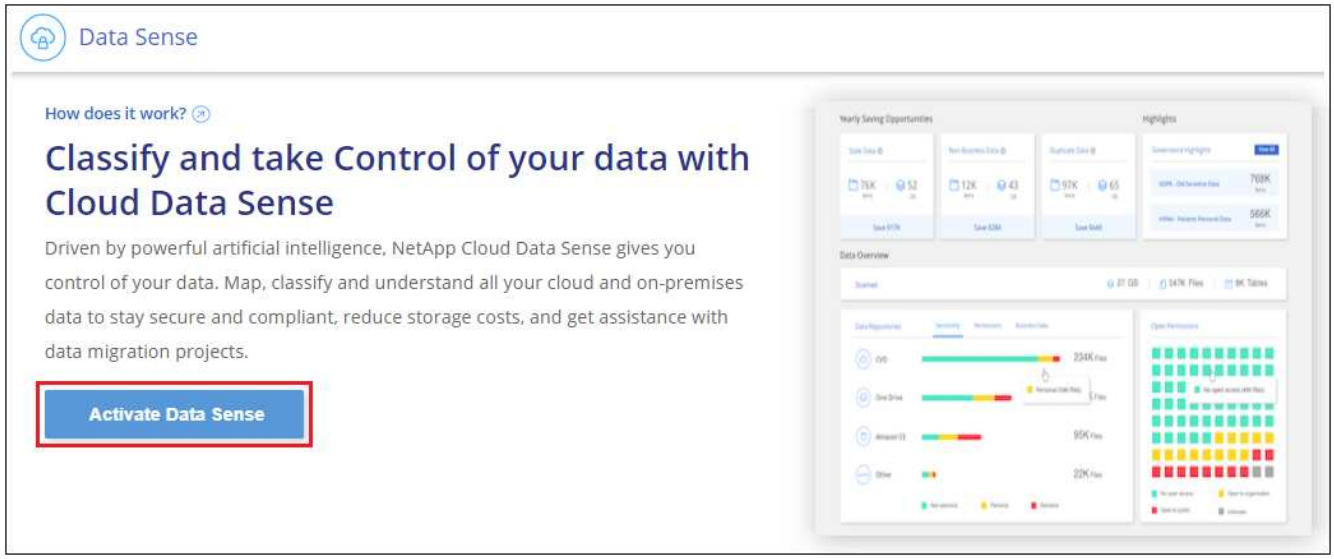
- 验证您的Linux系统是否符合主机要求。
- 确认系统已安装两个必备软件包(Docker Engine或Podman以及Python 3)。
- 确保您在 Linux 系统上具有 root 权限。
- 如果您使用代理访问Internet：
  - 您需要代理服务器信息(IP地址或主机名、连接端口、连接方案：HTTPS或http、用户名和密码)。
  - 如果代理正在执行TLS截取、您需要知道BlueXP分类Linux系统上存储TLS CA证书的路径。
  - 代理必须不透明-我们目前不支持透明代理。
  - 用户必须是本地用户。不支持域用户。
- 验证脱机环境是否满足所需的权限和连接。

步骤

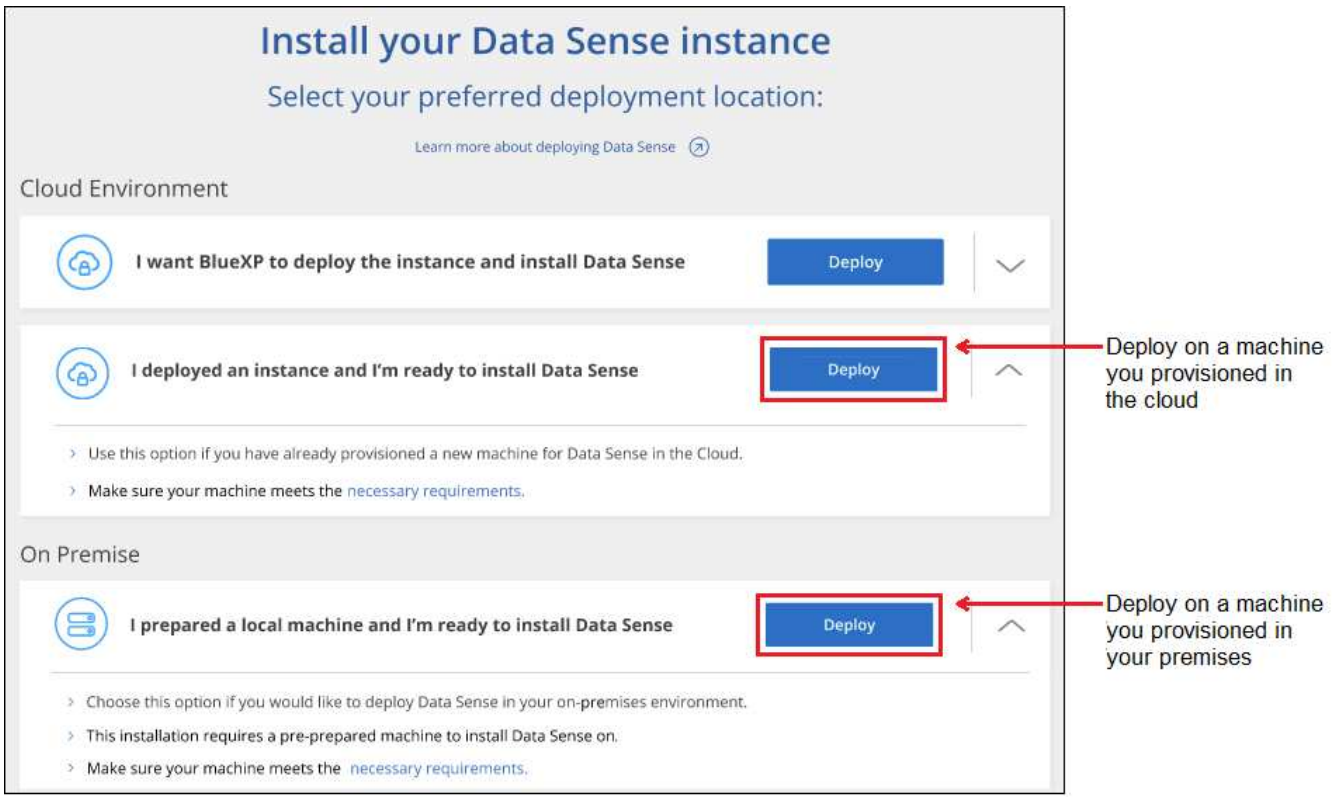
1. 从下载BlueXP 分类软件 "NetApp 支持站点"。您应选择的文件名为* datasENSE-installer-datas.tar.gz*<version>。
2. 将安装程序文件复制到要使用的Linux主机(使用 `scp`或其他方法)。
3. 解压缩主机上的安装程序文件，例如：

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. 在BlueXP中、选择*监管>分类*。
5. 单击 * 激活数据感知 * 。



6. 根据您是在云中准备的实例上还是在内部准备的实例上安装BlueXP分类、单击相应的*部署*按钮以启动BlueXP分类安装。



7. 此时将显示_Deploy Data sense on premises_对话框。复制提供的命令(例如： `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`)并将其粘贴到文本文件中，以便日后使用。然后单击*关闭*以关闭此对话框。
8. 在主机上、输入复制的命令、然后按照一系列提示进行操作、或者您也可以提供完整命令、其中包含所有必需的参数作为命令行参数。

   请注意、安装程序会执行预检查、以确保满足您的系统和网络要求、以便成功安装。 "观看此视频"了解预检消息和含义。

根据提示输入参数：	输入完整命令：
a. 粘贴从步骤7复制的命令： `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` 如果要在云实例(而不是内部环境)上安装，请添加 `--manual-cloud-install <cloud_provider>`。 b. 输入BlueXP分类主机的IP地址或主机名、以便连接器系统可以访问它。 c. 输入BlueXP Connector主机的IP地址或主机名、以便BlueXP分类系统可以访问它。 d. 根据提示输入代理详细信息。如果BlueXP Connector已使用代理、则无需在此再次输入此信息、因为BlueXP分类会自动使用连接器使用的代理。	或者、您也可以提前创建整个命令、并提供必要的主机和代理参数： `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

变量值：

- *account_id* = NetApp 帐户 ID
- _client_id =连接器客户端ID (如果客户端ID尚未添加后缀"clients"、请将其添加到该客户端ID)
- *user_token*= JWT用户访问令牌
- *ds_host*= BlueXP分类Linux系统的IP地址或主机名。
- *cm_host*= BlueXP Connector系统的IP地址或主机名。
- *cloud provider*=在云实例上安装时、根据云提供程序输入"AWs"、"Azure"或"GCP"。
- *proxy_host* = 代理服务器的 IP 或主机名（如果主机位于代理服务器之后）。
- *proxy_port* = 用于连接到代理服务器的端口（默认值为 80 ）。
- *proxy_scheme*= 连接方案： HTTPS 或 http （默认为 http ）。
- *proxy_user*= 已通过身份验证的用户，用于连接到代理服务器（如果需要基本身份验证）。用户必须是本地用户-不支持域用户。
- *proxy_password* = 指定用户名的密码。
- *ca_cert_dir*=包含其他TLS CA证书包的BlueXP分类Linux系统上的路径。仅当代理正在执行 TLS 截获时才需要。

结果

BlueXP分类安装程序会安装软件包、注册安装并安装BlueXP分类。安装可能需要 10 到 20 分钟。

如果主机和连接器实例之间通过端口8080建立了连接、您将在BlueXP的BlueXP分类选项卡中看到安装进度。

下一步行动

在配置页面中，您可以选择要扫描的数据源。

在无法访问**Internet**的**Linux**主机上安装**BlueXP**分类

完成几个步骤、在无法访问Internet的内部站点中的Linux主机上安装BlueXP分类、也称为_private mode_.此类安装使用安装脚本、无法连接到BlueXP SaaS层。

"了解BlueXP Connector和BlueXP分类的不同部署模式"(英文)

您也可以"在可访问Internet的内部站点中部署BlueXP分类"。

BlueXP分类安装脚本首先会检查系统和环境是否满足所需的前提条件。如果满足所有前提条件、则安装将开始。如果要独立于运行BlueXP分类安装来验证前提条件、则可以下载一个单独的软件包、该软件包仅测试前提条件。"请参见How to check if your Linux host is ready to install BlueXP classification"(英文)

> 对于传统版本1.3及更早版本，如果需要在多个主机上安装BlueXP 分类，请参见"在无法访问Internet的多个主机上安装BlueXP分类"。

支持的数据源

如果安装的是私有模式(有时称为"脱机"或"非公开"站点)、BlueXP分类只能扫描内部站点本地数据源中的数据。此时、BlueXP分类可以扫描以下*本地*数据源：

- 内部部署 ONTAP 系统
- 数据库架构

在私有模式下部署BlueXP分类时、当前不支持扫描Cloud Volumes ONTAP、Azure NetApp Files或FSx for ONTAP帐户。

限制

如果BlueXP分类功能部署在无法访问Internet的站点中、则大多数BlueXP分类功能都有效。但是，不支持某些需要访问 Internet 的功能，例如：

- 为不同用户设置BlueXP角色(例如、帐户管理员或合规性查看器)
- 使用BlueXP复制和同步功能复制和同步源文件
- 从BlueXP自动升级软件

  BlueXP Connector和BlueXP分类都需要定期手动升级才能启用新功能。您可以在BlueXP分类UI页面底部看到BlueXP分类版本。选中"BlueXP分类发行说明"以查看每个版本中的新增功能以及是否需要这些功能。然后，您可以按照和升级BlueXP分类软件的步骤进行操作 "升级BlueXP Connector"。

快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。

1 安装**BlueXP** 连接器

如果尚未在专用模式下安装Connector、请立即在Linux主机上安装 "部署连接器"。

2 查看**BlueXP** 分类前提条件

确保您的Linux系统符合主机要求，安装了所有必需的软件，并且脱机环境符合要求权限和连接。

3 下载并部署**BlueXP** 分类

从NetApp 支持站点 下载BlueXP分类软件、并将安装程序文件复制到要使用的Linux主机。然后启动安装向导并按照提示部署BlueXP分类实例。

安装**BlueXP Connector**

如果尚未在私有模式下安装BlueXP 连接器、请在脱机站点的Linux主机上安装 "部署连接器"。

准备 **Linux** 主机系统

BlueXP分类软件必须在满足特定操作系统要求、RAM要求、软件要求等的主机上运行。

- 与其他应用程序共享的主机不支持BlueXP分类-该主机必须是专用主机。
- 在内部构建主机系统时、您可以根据计划进行BlueXP分类扫描的数据集大小在这些系统大小中进行选择。

系统大小	**CPU**	**RAM (**必须禁用交换内存**)**	磁盘
超大	32个CPU	128 GB RAM	• 1 TiB SSD (位于/上)或100 GiB (位于/opt上) • 在/var/lib/Docker上提供了»»»»»»»»»»»»»»»»»»»»»» • /tmp 上 5 GiB • *对于Podman，/tmp*上为5 GB • *对于Podman，/var/tmp*上为30 GB
大型	16个CPU	64 GB RAM	• 500 GiB SSD (位于/上)或100 GiB (位于/opt上) • 395 GiB可从/var/lib/Docker或Podman /var/lib/containers或Podman /var/lib/containers获得 • /tmp 上 5 GiB • *对于Podman，/tmp*上为5 GB • *对于Podman，/var/tmp*上为30 GB

- 在云中为BlueXP分类安装部署计算实例时、我们建议使用满足上述"大型"系统要求的系统：

- * Amazon Elelic计算云(Amazon EC2)实例类型*：建议使用"m6i.4x大"。"请参见其他AWS实例类型"(英文)
- * Azure虚拟机大小*：建议使用"Standard_d16s_v3_"。"请参见其他Azure实例类型"(英文)
- * GCP计算机类型*：我们建议使用"n2-standard-16"。"请参见其他GCP实例类型"(英文)

- **UNIX**文件夹权限：需要以下最低UNIX权限：

文件夹	最小权限
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/Docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- * 操作系统 * ：
  - 以下操作系统要求使用Docker容器引擎：
    - Red Hat Enterprise Linux 7.8和7.9版
    - Ubuntu 22.04 (需要BlueXP分类版本1.23或更高版本)
    - Ubuntu 24.04 (需要BlueXP分类版本1.23或更高版本)
  - 以下操作系统要求使用Podman容器引擎、并且需要BlueXP分类版本1.3或更高版本：
    - Red Hat Enterprise Linux 8.8、8.10、9.0、9.1、9.2、9.3、9.4和9.5版
  - 必须在主机系统上启用高级矢量扩展(AVX)。
- * Red Hat订阅管理*：主机必须向Red Hat订阅管理注册。如果未注册、系统将无法在安装期间访问存储库来更新所需的第三方软件。
- 其他软件：在安装BlueXP分类之前、必须在主机上安装以下软件：
  - 根据您使用的操作系统、您需要安装以下容器引擎之一：
    - Docker引擎19.3.1或更高版本。 "查看安装说明"(英文)。
    - Podman版本4或更高版本。要安装Podman，请输入 (`sudo yum install podman netavark -y`)。
- Python 3.6或更高版本。 "查看安装说明"(英文)。
  - **NTP**注意事项：NetApp建议将BlueXP分类系统配置为使用网络时间协议(NTP)服务。BlueXP分类系统和BlueXP Connector系统之间的时间必须同步。
- **Firewalld**注意事项：如果您计划使用 `firewalld`，建议您在安装BlueXP 分类之前启用它。运行以下命令进行配置 `firewalld`、使其与BlueXP 分类兼容：

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

请注意、每当启用或更新设置时、都必须重新启动Docker或Podman `firewalld`。

安装后无法更改BlueXP分类主机系统的IP地址。

验证**BlueXP**和**BlueXP**分类前提条件

在部署BlueXP分类之前、请查看以下前提条件、以确保您的配置受支持。

- 确保Connector有权为BlueXP分类实例部署资源和创建安全组。您可以在中找到最新的BlueXP 权限 "NetApp 提供的策略"。
- 确保您可以保持BlueXP分类运行。BlueXP分类实例需要持续扫描数据。
- 确保Web浏览器连接到BlueXP分类。启用BlueXP分类后、确保用户从连接到BlueXP分类实例的主机访问BlueXP界面。

  BlueXP分类实例使用专用IP地址来确保索引数据不可供其他人访问。因此、用于访问BlueXP的Web浏览器必须连接到该专用IP地址。此连接可以来自与BlueXP分类实例位于同一网络中的主机。

验证是否已启用所有必需的端口

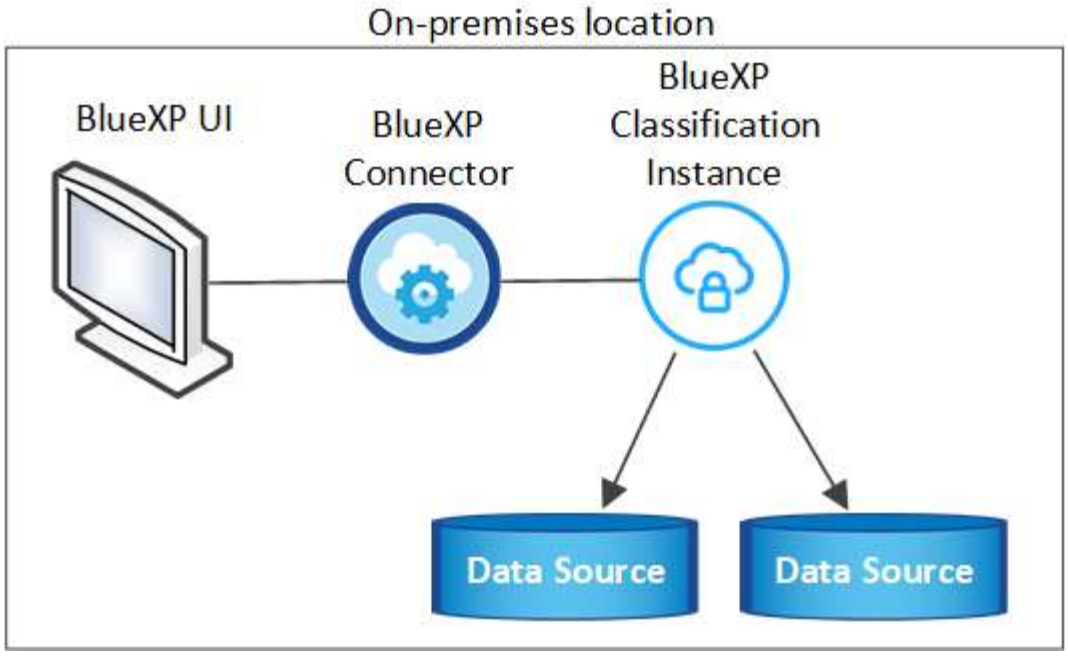
您必须确保所有必需的端口均已打开、可供Connector、BlueXP分类、Active Directory和数据源之间进行通信。

连接类型	端口	说明
连接器<> BlueXP分类	8080 (TCP)、6000 (TCP)、443 (TCP)和80 。9000	连接器的安全组必须允许通过端口6000和443传入和传出BlueXP分类实例的流量。 • 需要端口6000、以便BlueXP分类BYOL许可证在非公开站点中工作。 • 端口8080应处于打开状态、以便您可以在BlueXP中查看安装进度。 • 如果在Linux主机上使用防火墙、则Ubuntu服务器中的内部进程需要端口9000。

连接类型	端口	说明
Connector <> ONTAP 集群(NAS)	443 (TCP)	BlueXP使用HTTPS发现ONTAP 集群。如果使用自定义防火墙策略，则它们必须满足以下要求： • Connector 主机必须允许通过端口 443 进行出站 HTTPS 访问。如果 Connector 位于云中，则预定义的安全组允许所有出站通信。 • ONTAP 集群必须允许通过端口 443 进行入站 HTTPS 访问。默认的“管理”防火墙策略允许从所有 IP 地址进行入站 HTTPS 访问。如果您修改了此默认策略，或者创建了自己的防火墙策略，则必须将 HTTPS 协议与该策略关联，并启用从 Connector 主机进行访问。
BlueXP分类<> ONTAP 集群	• 对于NFS - 111 (tcp\udp)和2049 (tcp\udp) • 对于CIFS - 139 (TCP/UDP)和445 (TCP/UDP)	BlueXP分类需要与每个Cloud Volumes ONTAP 子网或内置ONTAP 系统建立网络连接。Cloud Volumes ONTAP 的安全组必须允许从BlueXP分类实例进行入站连接。 确保这些端口对BlueXP分类实例开放： • 对于NFS—111和2049 • 对于CIFS—139和445 NFS卷导出策略必须允许从BlueXP分类实例进行访问。
BlueXP分类<> Active Directory	389 (TCP和UDP)、636 (TCP)、3268 (TCP)和3369 (TCP)	您必须已为公司中的用户设置 Active Directory 。此外、BlueXP分类需要Active Directory凭据才能扫描CIFS卷。 您必须具有 Active Directory 的信息： • DNS 服务器 IP 地址或多个 IP 地址 • 服务器的用户名和密码 • 域名（ Active Directory 名称） • 是否使用安全 LDAP （ LDAPS ） • LDAP 服务器端口（对于 LDAP ，通常为 389 ；对于安全 LDAP ，通常为 636 ）
如果在Linux主机上使用了防火墙	9000	Ubuntu服务器中的内部流程需要此功能。

在内部**Linux**主机上安装**BlueXP**分类

对于典型配置，您将在一个主机系统上安装该软件。



典型配置的单主机安装

在脱机环境中的单个内部主机上安装BlueXP分类软件时、请按照以下步骤进行操作。

请注意、安装BlueXP分类时会记录所有安装活动。如果在安装期间遇到任何问题、您可以查看安装审核日志的内容。它会写入到 `/opt/netapp/install_logs/`。"请单击此处查看更多详细信息"(英文)

您需要的内容

- 验证您的Linux系统是否符合主机要求。
- 确认已安装两个必备软件包(Docker Engine或Podman以及Python 3)。
- 确保您在 Linux 系统上具有 root 权限。
- 验证脱机环境是否满足所需的权限和连接。

步骤

1. 在已配置Internet的系统上，从下载BlueXP 分类软件 "NetApp 支持站点"。您应选择的文件名为 * Datasis-offline-bundle-<version>.tar.gz* 。
2. 将安装程序捆绑包复制到计划在专用模式下使用的Linux主机。
3. 解压缩主机上的安装程序包，例如：

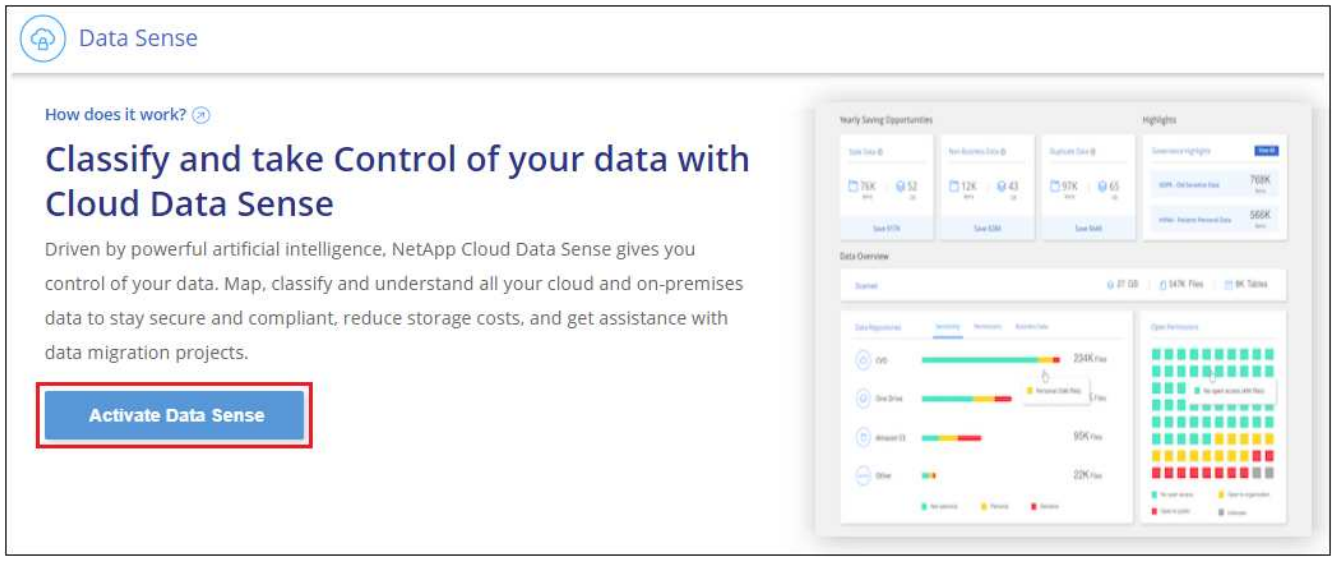
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

此操作将提取所需的软件和实际安装文件* cc_onprem_installer.tar.gz*。

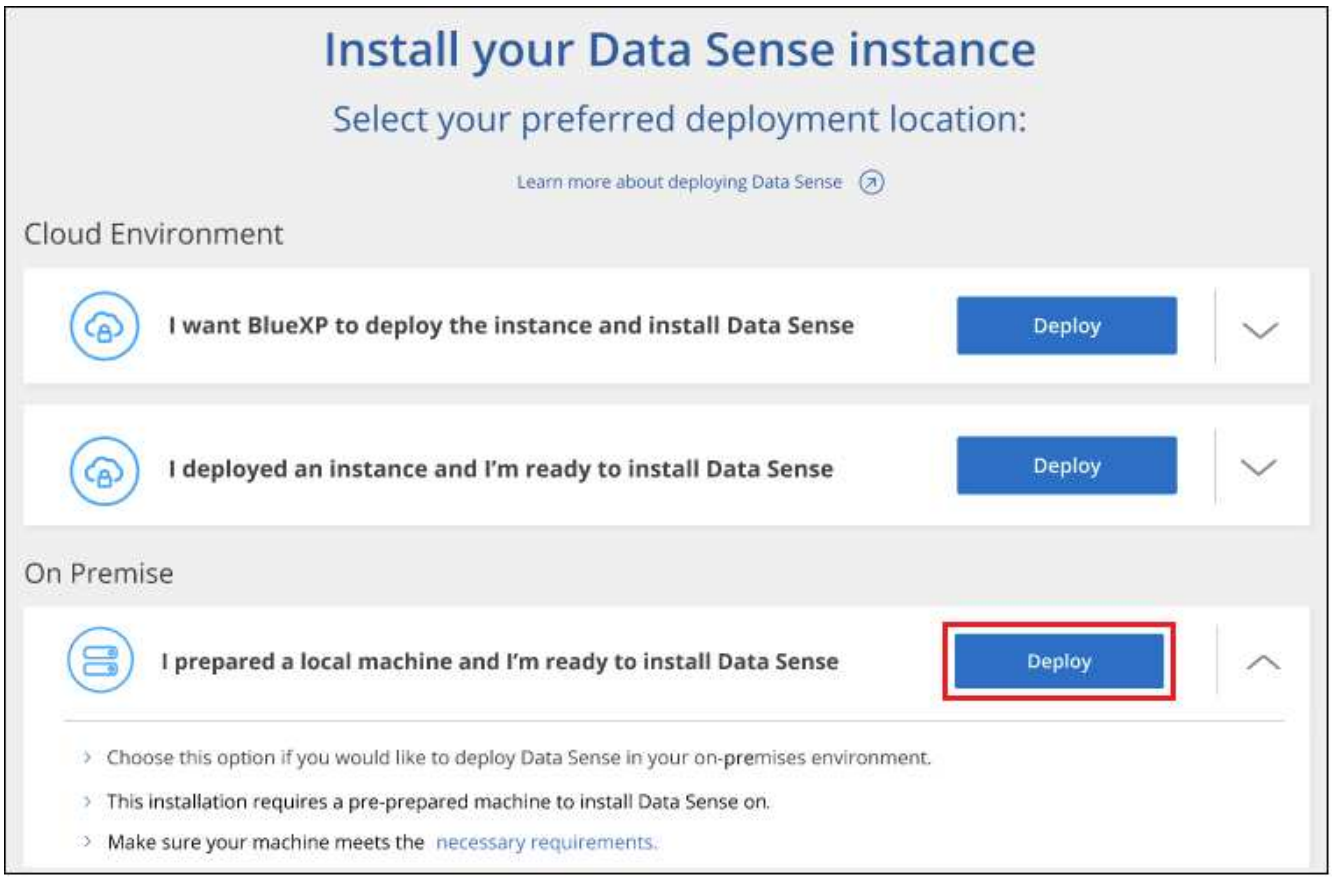
4. 解压缩主机上的安装文件，例如：

```
tar -xzf cc_onprem_installer.tar.gz
```

5. 启动BlueXP并选择*监管>分类*。
6. 单击 * 激活数据感知 * 。



7. 单击*部署*以启动内部安装。



8. 此时将显示_Deploy Data sense on premises_对话框。复制提供的命令(例如： `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`)并将其粘贴到文本文件中，以便日后使用。然后单击*关闭*以关闭此对话框。
9. 在主机上、输入复制的命令、然后按照一系列提示进行操作、或者您也可以提供完整命令、其中包含所有必

需的参数作为命令行参数。

请注意、安装程序会执行预检、以确保满足您的系统和网络要求、以便成功安装。

根据提示输入参数：	输入完整命令：
a. 粘贴您从第8步复制的信息： `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. 输入BlueXP分类主机的IP地址或主机名、以便连接器系统可以访问它。 c. 输入BlueXP Connector主机的IP地址或主机名、以便BlueXP分类系统可以访问它。	或者、您也可以提前创建整个命令、并提供必要的主机参数： `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

变量值：

- *account_id* = NetApp 帐户 ID
- _client_id =连接器客户端ID (如果客户端ID尚未添加后缀"clients"、请将其添加到该客户端ID)
- *user_token*= JWT用户访问令牌
- *ds_host*= BlueXP分类系统的IP地址或主机名。
- *cm_host*= BlueXP Connector系统的IP地址或主机名。

结果

BlueXP分类安装程序会安装软件包、注册安装并安装BlueXP分类。安装可能需要 10 到 20 分钟。

如果主机和连接器实例之间通过端口8080建立了连接、您将在BlueXP的BlueXP分类选项卡中看到安装进度。

下一步行动

从配置页面中、您可以选择要扫描的本地"内部 ONTAP 集群"和"数据库"。

升级**BlueXP**分类软件

由于BlueXP分类软件定期更新新功能、因此您应进入例行程序定期检查新版本、以确保您使用的是最新的软件和功能。您需要手动升级BlueXP分类软件、因为没有Internet连接、无法自动执行升级。

开始之前

- 我们建议您将BlueXP 连接器软件升级到最新可用版本。 "请参见 Connector 升级步骤"(英文)。
- 从BlueXP分类版本1.24开始、您可以升级到任何未来的软件版本。

  如果BlueXP分类软件运行的版本早于1.24、则一次只能升级一个主要版本。例如、如果您安装了1.21.x版、则只能升级到1.22.x如果您有几个主要版本，则需要多次升级此软件。

步骤

1. 在已配置Internet的系统上，从下载BlueXP 分类软件 "NetApp 支持站点"。您应选择的文件名为 * Datasis-offline-bundle-<version>.tar.gz* 。

2. 将软件包复制到非公开站点上安装了BlueXP分类的Linux主机。
3. 解压缩主机上的软件包，例如：

```
tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
```

此操作将提取安装文件* cc_onprem_installer.tar.gz*。

4. 解压缩主机上的安装文件，例如：

```
tar -xzf cc_onprem_installer.tar.gz
```

此操作将提取升级脚本 * 启动 _didssite_upgrade.sh* 以及任何所需的第三方软件。

5. 在主机上运行升级脚本，例如：

```
start_darksite_upgrade.sh
```

结果

在主机上升级BlueXP分类软件。更新可能需要 5 到 10 分钟。

您可以通过检查BlueXP分类UI页面底部的版本来验证软件是否已更新。

检查**Linux**主机是否已准备好安装**BlueXP**分类

在Linux主机上手动安装BlueXP 分类之前、可以选择在此主机上运行一个脚本、以验证安装BlueXP 分类的所有前提条件是否都已满足。您可以在网络中的Linux主机或云中的Linux主机上运行此脚本。主机可以连接到Internet、也可以位于无法访问Internet的站点(*dark site*）中。

BlueXP分类安装脚本中还有一个必备测试脚本。此处介绍的脚本专为希望独立于运行BlueXP分类安装脚本来验证Linux主机的用户而设计。

入门

您将执行以下任务。

1. 如果您尚未安装BlueXP Connector、也可以安装它。您可以在不安装Connector的情况下运行测试脚本、但该脚本会检查Connector与BlueXP分类主机之间的连接、因此建议您使用Connector。
2. 准备主机并验证它是否满足所有要求。
3. 从BlueXP分类主机启用出站Internet访问。
4. 验证是否已在所有系统上启用所有必需的端口。
5. 下载并运行前提条件测试脚本。

创建连接器

在安装和使用BlueXP分类之前、需要BlueXP Connector。但是、您可以在不使用Connector的情况下运行Prerequisites脚本。

您可以在网络中的Linux主机上、也可以 "在内部安装 Connector"在云中的Linux主机上。一些计划在本机安装BlueXP分类的用户也可以选择在本机安装Connector。

要在云提供商环境中创建Connector，请参见 "在 AWS 中创建连接器"、 "在 Azure 中创建连接器"或 "在 GCP 中创建连接器"。

运行Prerequisites脚本时、您需要连接器系统的IP地址或主机名。如果您在内部安装了Connector、则可以获得此信息。如果Connector部署在云中、您可以从BlueXP控制台找到此信息：单击帮助图标、选择*支持*、然后单击*蓝XP连接器*。

验证主机要求

BlueXP分类软件必须在满足特定操作系统要求、RAM要求、软件要求等的主机上运行。

- 与其他应用程序共享的主机不支持BlueXP分类-该主机必须是专用主机。
- 在内部构建主机系统时、您可以根据计划进行BlueXP分类扫描的数据集大小在这些系统大小中进行选择。

系统大小	**CPU**	**RAM (必须禁用交换内存)**	磁盘
超大	32个CPU	128 GB RAM	• 1 TiB SSD (位于/上)或100 GiB (位于/opt上) • 在/var/lib/Docker上提供了»»»»»»»»»»»»»»»»»»»»» • /tmp 上 5 GiB • *对于Podman，/tmp*上为5 GB • *对于Podman，/var/tmp*上为30 GB
大型	16个CPU	64 GB RAM	• 500 GiB SSD (位于/上)或100 GiB (位于/opt上) • 395 GiB可从/var/lib/Docker或Podman /var/lib/containers或Podman /var/lib/containers获得 • /tmp 上 5 GiB • *对于Podman，/tmp*上为5 GB • *对于Podman，/var/tmp*上为30 GB

- 在云中为BlueXP分类安装部署计算实例时、我们建议使用满足上述"大型"系统要求的系统：

- * Amazon Elelic计算云(Amazon EC2)实例类型*：建议使用"m6i.4x大"。"请参见其他AWS实例类型"(英文)
- * Azure虚拟机大小*：建议使用"Standard_d16s_v3_"。"请参见其他Azure实例类型"(英文)
- * GCP计算机类型*：我们建议使用"n2-standard-16"。"请参见其他GCP实例类型"(英文)

- **UNIX**文件夹权限：需要以下最低UNIX权限：

文件夹	最小权限
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/Docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- * 操作系统 * ：
  - 以下操作系统要求使用Docker容器引擎：
    - Red Hat Enterprise Linux 7.8和7.9版
    - Ubuntu 22.04 (需要BlueXP分类版本1.23或更高版本)
    - Ubuntu 24.04 (需要BlueXP分类版本1.23或更高版本)
  - 以下操作系统要求使用Podman容器引擎、并且需要BlueXP分类版本1.3或更高版本：
    - Red Hat Enterprise Linux 8.8、8.10、9.0、9.1、9.2、9.3、9.4和9.5版
  - 必须在主机系统上启用高级矢量扩展(AVX)。
- * Red Hat订阅管理*：主机必须向Red Hat订阅管理注册。如果未注册、系统将无法在安装期间访问存储库来更新所需的第三方软件。
- 其他软件：在安装BlueXP分类之前、必须在主机上安装以下软件：
  - 根据您使用的操作系统、您需要安装以下容器引擎之一：
    - Docker引擎19.3.1或更高版本。 "查看安装说明"(英文)。
    - Podman版本4或更高版本。要安装Podman，请输入 (`sudo yum install podman netavark -y`)。
- Python 3.6或更高版本。 "查看安装说明"(英文)。
  - **NTP**注意事项：NetApp建议将BlueXP分类系统配置为使用网络时间协议(NTP)服务。BlueXP分类系统和BlueXP Connector系统之间的时间必须同步。
- **Firewalld**注意事项：如果您计划使用 `firewalld`，建议您在安装BlueXP 分类之前启用它。运行以下命令进行配置 `firewalld`、使其与BlueXP 分类兼容：

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

如果您计划使用其他BlueXP分类主机作为扫描程序节点(在分布式模型中)、请此时将这些规则添加到主系统：

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

请注意、每当启用或更新设置时、都必须重新启动Docker或Podman `firewalld`。

从**BlueXP**分类启用出站**Internet**访问

BlueXP分类需要出站Internet访问。如果您的虚拟或物理网络使用代理服务器进行Internet访问、请确保BlueXP分类实例具有出站Internet访问权限以联系以下端点。

对于安装在无Internet连接站点中的主机系统、不需要此部分。

端点	目的
https://api.bluexp.netapp.com	与包括NetApp帐户在内的BlueXP服务进行通信。
\https：//https：NetApp-cloud-account.auth0.com https://auth0.com	与BlueXP网站通信以实现集中式用户身份验证。
https://support.compliance.api BlueXP ．NetApp．com/\https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	可用于访问软件映像，清单，模板以及发送日志和指标。
https://support.compliance.api BlueXP ．NetApp．com/	使 NetApp 能够从审计记录流化数据。
https://github.com/docker https://download.docker.com	提供Docker安装的必备软件包。
http://packages.ubuntu.com/ http://archive.ubuntu.com	提供Ubuntu安装的必备软件包。

验证是否已启用所有必需的端口

您必须确保所有必需的端口均已打开、可供Connector、BlueXP分类、Active Directory和数据源之间进行通信。

连接类型	端口	说明
连接器<> BlueXP分类	8080 (TCP)、443 (TCP)和80。9000	连接器的防火墙或路由规则必须允许通过端口443传入和传出BlueXP分类实例的流量。确保端口8080已打开、以便您可以在BlueXP中查看安装进度。如果在Linux主机上使用防火墙、则Ubuntu服务器中的内部进程需要端口9000。
Connector <> ONTAP 集群(NAS)	443 (TCP)	BlueXP使用HTTPS发现ONTAP 集群。如果使用自定义防火墙策略、则Connector主机必须允许通过端口443进行出站HTTPS访问。如果Connector位于云中、则预定义的防火墙或路由规则允许所有出站通信。

运行**BlueXP**分类前提条件脚本

按照以下步骤运行BlueXP分类前提条件脚本。

"观看此视频"了解如何运行前提条件脚本并解读结果。

您需要的内容

- 验证您的Linux系统是否符合主机要求。
- 确认系统已安装两个必备软件包(Docker Engine或Podman以及Python 3)。
- 确保您在 Linux 系统上具有 root 权限。

步骤

1. 从下载BlueXP 分类前提条件脚本 "NetApp 支持站点"。您应选择的文件名为*独立-前提条件-测试人员-tester-tester*<version>。
2. 将文件复制到要使用的Linux主机(使用或其他方法) `scp`。
3. 分配运行脚本的权限。

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. 使用以下命令运行此脚本。

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

只有在无法访问Internet的主机上运行脚本时、才添加选项"-d暗 站点"。如果主机未连接到Internet、则会跳过某些前提条件测试。

5. 该脚本会提示您输入BlueXP分类主机的IP地址。
   - 输入IP地址或主机名。

6. 此脚本将提示您是否已安装BlueXP Connector。
   - 如果您没有安装Connector、请输入*。
   - 如果安装了Connector、请输入*。然后、输入BlueXP Connector的IP地址或主机名、以便测试脚本可以测试此连接。
7. 该脚本会在系统上运行各种测试、并在执行过程中显示结果。完成后，它会将会话日志写入目录中 `/opt/netapp/install_logs`名为的文件 `prerequisites-test-<timestamp>.log`。

结果

如果所有前提条件测试均成功运行、则可以在准备就绪后在主机上安装BlueXP分类。

如果发现任何问题、则将其归类为"建议"或"必需"以进行修复。建议的问题通常是会使BlueXP分类扫描和分类任务运行速度变慢的项目。这些项目不需要更正、但您可能需要解决这些问题。

如果存在任何"必需"问题、应修复这些问题并重新运行前提条件测试脚本。

激活对数据源的扫描

扫描具有**BlueXP** 分类的**Azure NetApp Files**卷

完成几个步骤即可开始使用适用于Azure NetApp Files 的BlueXP分类。

发现要扫描的**Azure NetApp Files**系统

如果您要扫描的Azure NetApp Files 系统尚未作为工作环境在BlueXP中、您可以此时将其添加到画布中。

"了解如何在BlueXP中发现Azure NetApp Files 系统"(英文)

部署**BlueXP**分类实例

"部署BlueXP分类"如果尚未部署实例。

扫描Azure NetApp Files 卷时、必须在云中部署BlueXP分类、并且必须将其部署在与要扫描的卷相同的区域。

*注意：*扫描Azure NetApp Files 卷时、当前不支持在内部位置部署BlueXP分类。

在您的工作环境中启用**BlueXP** 分类

您可以在Azure NetApp Files 卷上启用BlueXP分类。

1. 从BlueXP左侧导航菜单中、单击*监管>分类*。
2. 从BlueXP 分类菜单中，选择*Configuration*。

3. 选择要如何扫描每个工作环境中的卷。"了解映射和分类扫描"：
   - 要映射所有卷，请选择*映射所有卷*。
   - 要映射所有卷并对其进行分类，请选择*映射所有卷并对其进行分类*。
   - 要自定义每个卷的扫描，请选择*或为每个卷选择扫描类型*，然后选择要映射和/或分类的卷。

     有关详细信息、请参见。 对卷启用和禁用合规性扫描
4. 在确认对话框中，选择*Approve*以使BlueXP 分类开始扫描卷。

结果

BlueXP分类开始扫描您在工作环境中选择的卷。一旦BlueXP分类完成初始扫描、结果将显示在Compliance信息板中。所需时间取决于数据量—可能需要几分钟或几小时。

- 默认情况下、如果BlueXP分类在CIFS中没有写入属性权限或在NFS中没有写入权限、则系统不会扫描卷中的文件、因为BlueXP分类无法将"上次访问时间"还原为原始时间戳。如果您不关心上次访问时间是否已重置、请单击*或为每个卷选择扫描类型*。生成的页面包含一个您可以启用的设置、以便BlueXP分类将扫描卷、而不管权限如何。
- BlueXP分类仅扫描卷下的一个文件共享。如果卷中有多个共享、则需要将这些其他共享作为一个共享组单独扫描。"请参见有关此BlueXP分类限制的更多详细信息"(英文)

验证**BlueXP** 分类是否有权访问卷

通过检查网络连接、安全组和导出策略、确保BlueXP分类可以访问卷。您需要为BlueXP分类提供CIFS凭据、以便它可以访问CIFS卷。

对于Azure NetApp Files 、BlueXP分类只能扫描与BlueXP位于同一区域的卷。

步骤

1. 确保BlueXP分类实例与包含Azure NetApp Files 卷的每个网络之间具有网络连接。
2. 确保以下端口对BlueXP分类实例开放：
   - 对于 NFS —端口 111 和 2049 。
   - 对于 CIFS —端口 139 和 445 。
3. 确保NFS卷导出策略包含BlueXP分类实例的IP地址、以便它可以访问每个卷上的数据。
4. 如果使用CIFS、请提供BlueXP分类和Active Directory凭据、以便它可以扫描CIFS卷。
   a. 从BlueXP 左侧导航菜单中、选择*监管>分类*。

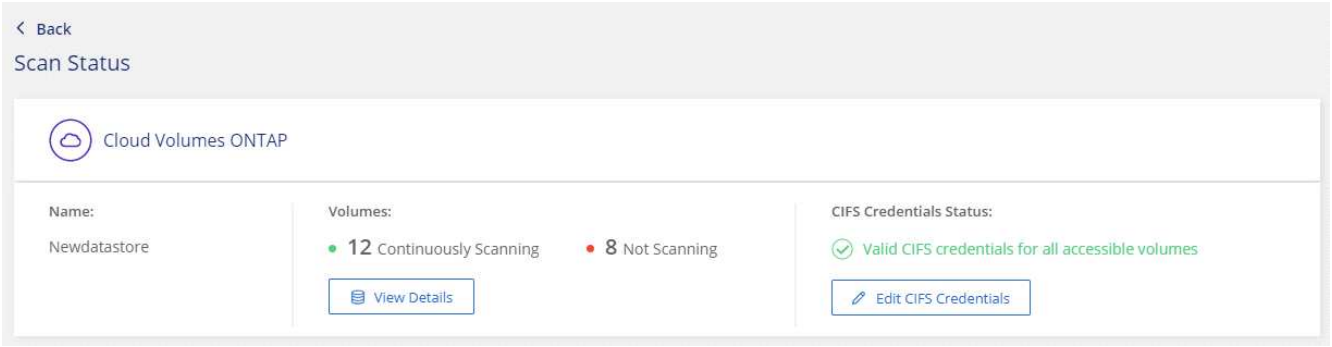
5. 从BlueXP 分类菜单中，选择*Configuration*。

a. 对于每个工作环境，请选择*编辑CIFS凭据*并输入BlueXP 分类访问系统上的CIFS卷所需的用户名和密码。

这些凭据可以是只读的、但提供管理员凭据可确保BlueXP分类可以读取需要提升权限的任何数据。这些凭据存储在BlueXP分类实例上。

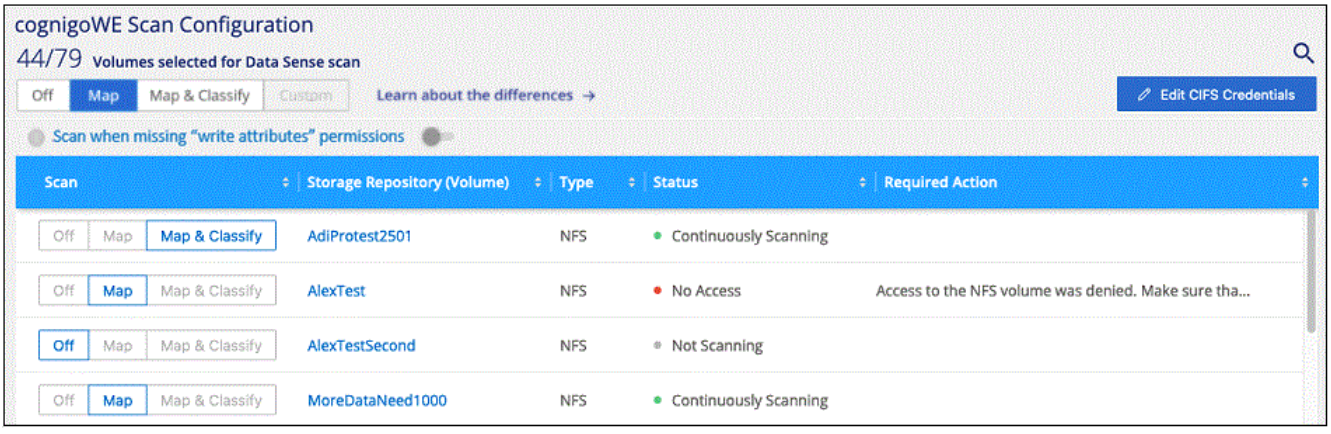
如果要确保文件"上次访问时间"在BlueXP分类扫描中保持不变、建议用户在CIFS中具有写入属性权限或在NFS中具有写入权限。如果可能、我们建议将Active Directory配置的用户设置为组织中有权访问所有文件的父组的一部分。

输入凭据后，您应看到一条消息，指出所有 CIFS 卷均已成功通过身份验证。



6. 在配置页面上、选择*查看详细信息*以查看每个CIFS和NFS卷的状态并更正任何错误。

例如、下图显示了四个卷；其中一个卷由于BlueXP分类实例和卷之间的网络连接问题而无法扫描BlueXP分类。

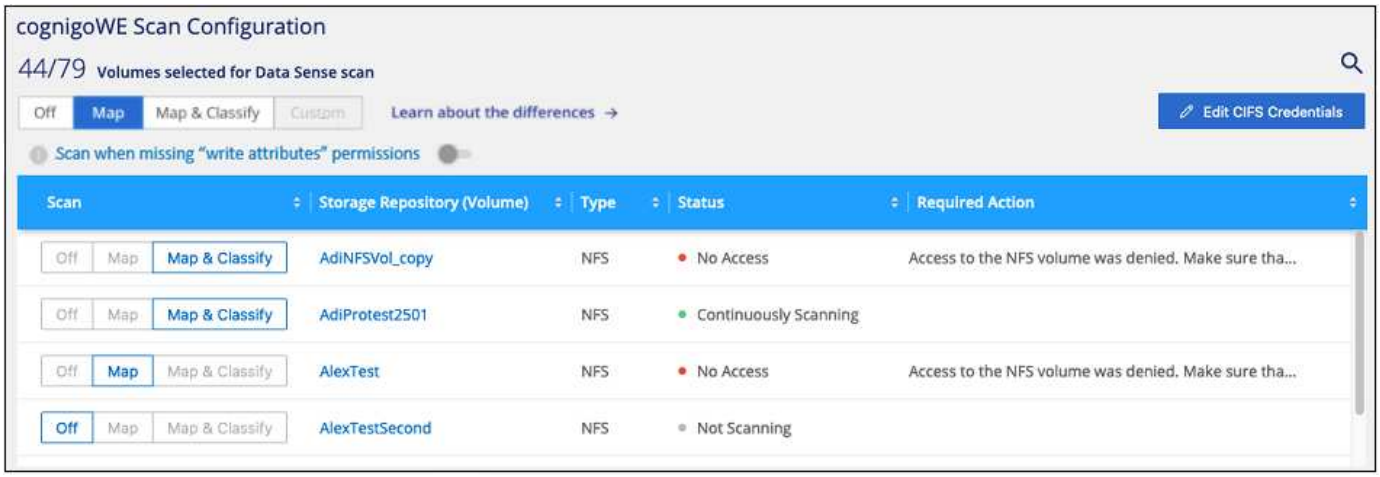


对卷启用和禁用合规性扫描

您可以随时从 " 配置 " 页面在工作环境中启动或停止仅映射扫描或映射和分类扫描。您也可以从仅映射扫描更改为映射和分类扫描，反之亦然。建议您扫描所有卷。

只有在标题区域中设置了 * 映射 * 或 * 映射和分类 * 设置后，才会自动扫描添加到工作环境中的新卷。如果在标题区域中设置为 * 自定义 * 或 * 关闭 * ，则需要在工作环境中添加的每个新卷上激活映射和 / 或完全扫描。

默认情况下、页面顶部的*缺少"写入属性"权限时扫描*开关处于禁用状态。这意味着、如果BlueXP分类在CIFS中没有写入属性权限、或者在NFS中没有写入权限、则系统将不会扫描文件、因为BlueXP分类无法将"上次访问时间"还原为原始时间戳。如果您不关心上次访问时间是否已重置、请打开此开关、无论权限如何、所有文件都将被扫描。"了解更多信息。"(英文)



步骤

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 执行以下操作之一：
   - 要对卷启用仅映射扫描，请在卷区域中选择*Map*。要在所有卷上启用，请在标题区域中选择*Map*。
   - 要对卷启用完全扫描，请在卷区域中选择*映射和分类*。要在所有卷上启用，请在标题区域中选择*映射和分类*。
   - 要禁用对卷的扫描，请在卷区域中选择*off*。要禁用对所有卷的扫描，请在标题区域中选择*off*。

扫描具有BlueXP 分类的ONTAP卷的Amazon FSx

完成几个步骤即可开始扫描具有BlueXP分类的Amazon FSx for ONTAP 卷。

开始之前

- 要部署和管理BlueXP分类、您需要AWS中的主动连接器。
- 创建工作环境时选择的安全组必须允许来自BlueXP分类实例的流量。您可以使用连接到 FSX for ONTAP 文件系统的 ENI 来查找关联的安全组，并使用 AWS 管理控制台对其进行编辑。

  "适用于 Linux 实例的 AWS 安全组"

"适用于 Windows 实例的 AWS 安全组"

"AWS 弹性网络接口（ ENI ）"

- 确保以下端口对BlueXP分类实例开放：
  - 对于 NFS —端口 111 和 2049 。
  - 对于 CIFS —端口 139 和 445 。

部署**BlueXP**分类实例

"部署BlueXP分类"如果尚未部署实例。

您应在与Connector for AWS和要扫描的FSx卷相同的AWS网络中部署BlueXP分类。

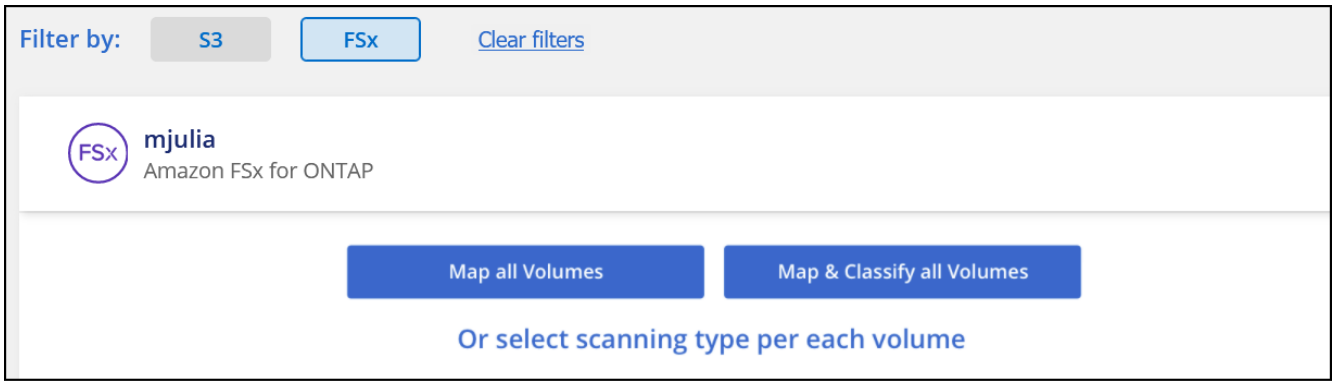
*注意：*扫描FSx卷时、当前不支持在内部位置部署BlueXP分类。

只要该实例具有Internet连接、BlueXP分类软件的升级就会自动进行。

在您的工作环境中启用**BlueXP** 分类

您可以为FSx for ONTAP 卷启用BlueXP分类。

1. 从BlueXP 左侧导航菜单中、选择*监管>分类*。
2. 从BlueXP 分类菜单中，选择*Configuration*。



3. 选择要如何扫描每个工作环境中的卷。"了解映射和分类扫描"：
   - 要映射所有卷，请单击 * 映射所有卷 * 。
   - 要映射所有卷并对其进行分类，请单击 * 映射并分类所有卷 * 。
   - 要自定义每个卷的扫描，请单击 * 或选择每个卷的扫描类型 * ，然后选择要映射和 / 或分类的卷。
4. 在确认对话框中、单击*批准*以使BlueXP分类开始扫描卷。

结果

BlueXP分类开始扫描您在工作环境中选择的卷。一旦BlueXP分类完成初始扫描、结果将显示在Compliance信息板中。所需时间取决于数据量—可能需要几分钟或几小时。

- 默认情况下、如果BlueXP分类在CIFS中没有写入属性权限或在NFS中没有写入权限、则系统不会扫描卷中的文件、因为BlueXP分类无法将"上次访问时间"还原为原始时间戳。如果您不关心上次访问时间是否已重置、请单击*或为每个卷选择扫描类型*。生成的页面包含一个您可以启用的设置、以便BlueXP分类将扫描卷、而不管权限如何。
- BlueXP分类仅扫描卷下的一个文件共享。如果卷中有多个共享、则需要将这些其他共享作为一个共享组单独扫描。"请参见有关此BlueXP分类限制的更多详细信息"(英文)

验证BlueXP 分类是否有权访问卷

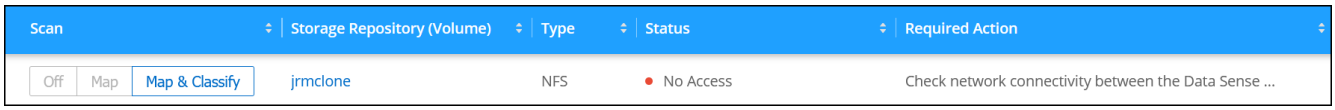
通过检查网络连接、安全组和导出策略、确保BlueXP分类可以访问卷。

您需要为BlueXP分类提供CIFS凭据、以便它可以访问CIFS卷。

步骤

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 在配置页上，选择*View Details*以查看状态并更正任何错误。

   例如、下图显示了由于BlueXP分类实例和卷之间的网络连接问题而无法扫描的卷BlueXP分类。



3. 确保BlueXP分类实例与包含FSx for ONTAP 卷的每个网络之间具有网络连接。

   对于FSx for ONTAP 、BlueXP分类只能扫描与BlueXP位于同一区域的卷。

4. 确保NFS卷导出策略包含BlueXP分类实例的IP地址、以便它可以访问每个卷上的数据。
5. 如果使用CIFS、请提供BlueXP分类和Active Directory凭据、以便它可以扫描CIFS卷。

   a. 从BlueXP 分类菜单中，选择*Configuration*。

   b. 对于每个工作环境，请选择*编辑CIFS凭据*并输入BlueXP 分类访问系统上的CIFS卷所需的用户名和密码。

      这些凭据可以是只读的、但提供管理员凭据可确保BlueXP分类可以读取需要提升权限的任何数据。这些凭据存储在BlueXP分类实例上。

      如果要确保文件"上次访问时间"在BlueXP分类扫描中保持不变、建议用户在CIFS中具有写入属性权限或在NFS中具有写入权限。如果可能、我们建议将Active Directory配置的用户设置为组织中有权访问所有文件的父组的一部分。

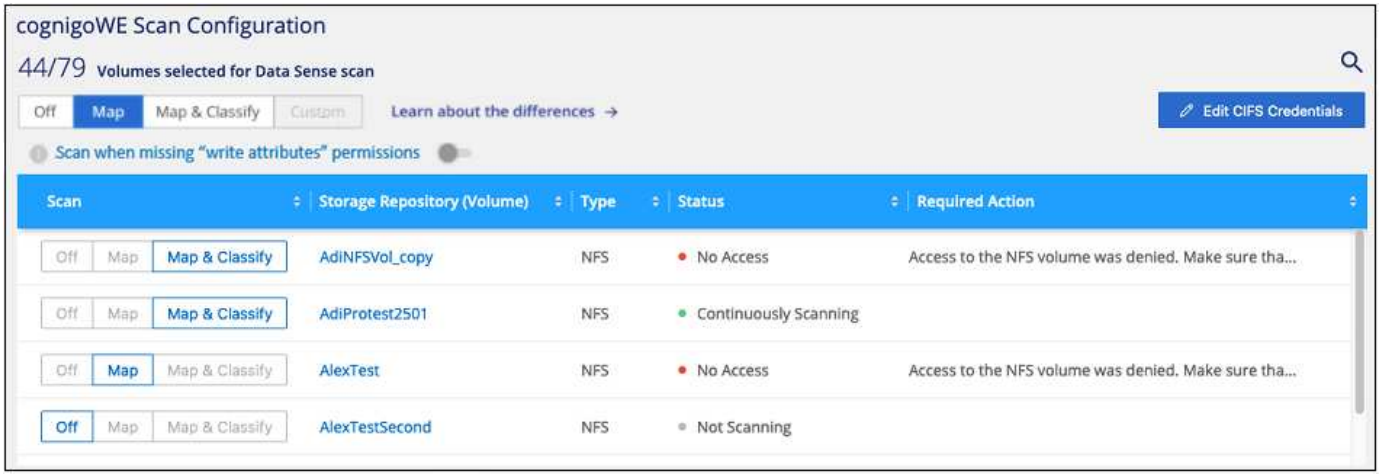
   输入凭据后，您应看到一条消息，指出所有 CIFS 卷均已成功通过身份验证。

对卷启用和禁用合规性扫描

您可以随时从 " 配置 " 页面在工作环境中启动或停止仅映射扫描或映射和分类扫描。您也可以从仅映射扫描更改为映射和分类扫描，反之亦然。建议您扫描所有卷。

默认情况下、页面顶部的*缺少"写入属性"权限时扫描*开关处于禁用状态。这意味着、如果BlueXP分类在CIFS中

没有写入属性权限、或者在NFS中没有写入权限、则系统将不会扫描文件、因为BlueXP分类无法将"上次访问时间"还原为原始时间戳。如果您不关心上次访问时间是否已重置、请打开此开关、无论权限如何、所有文件都将被扫描。"了解更多信息。"(英文)



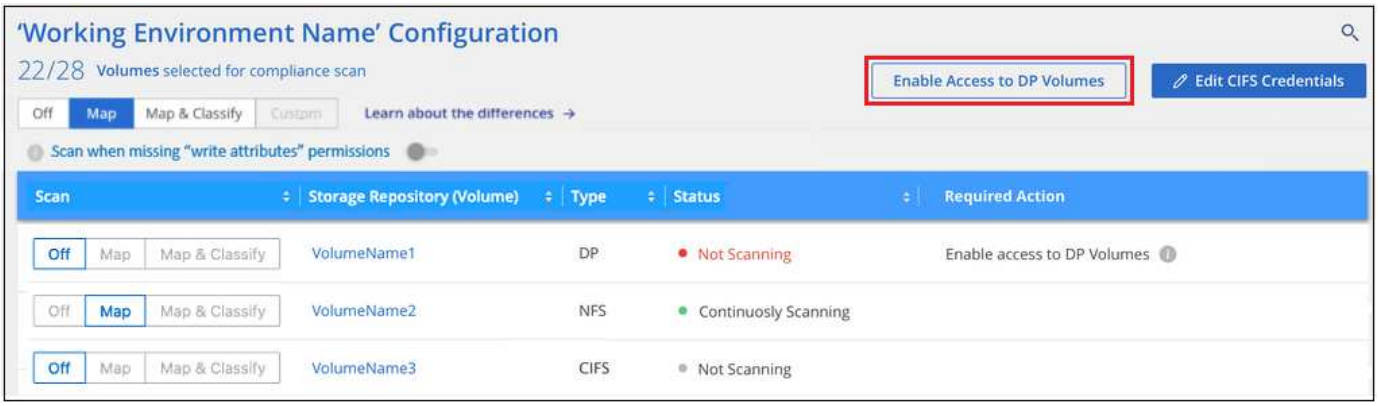
1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 在配置页面中、找到包含要扫描的卷的工作环境。
3. 执行以下操作之一：
   - 要对卷启用仅映射扫描，请在卷区域中选择*Map*。或者，要在所有卷上启用，请在标题区域中选择*Map*。要对卷启用完全扫描，请在卷区域中选择*映射和分类*。或者、要在所有卷上启用、请在标题区域中选择*映射和分类*。
   - 要禁用对卷的扫描，请在卷区域中选择*off*。要禁用对所有卷的扫描，请在标题区域中选择*off*。

只有在标题区域中设置了 * 映射 * 或 * 映射和分类 * 设置后，才会自动扫描添加到工作环境中的新卷。如果在标题区域中设置为 * 自定义 * 或 * 关闭 * ，则需要在工作环境中添加的每个新卷上激活映射和 / 或完全扫描。

扫描数据保护卷

默认情况下、不会扫描数据保护(DP)卷、因为这些卷不会对外公开、BlueXP分类无法访问它们。这些卷是从适用于 ONTAP 的 FSX 文件系统执行 SnapMirror 操作的目标卷。

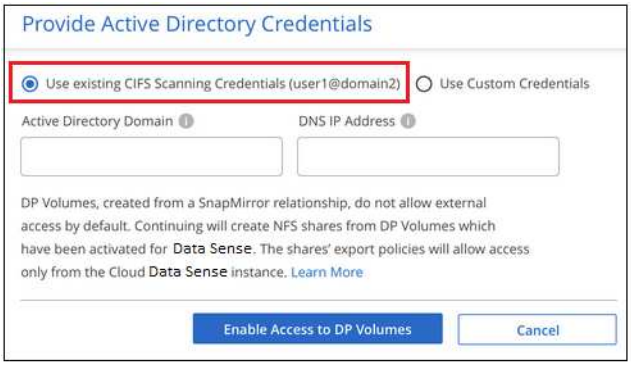
最初，卷列表会将这些卷标识为 *Type* * dp* ，并显示 *Status* * 未扫描 * 和 *Required Action* * Enable Access to DP volumes* 。

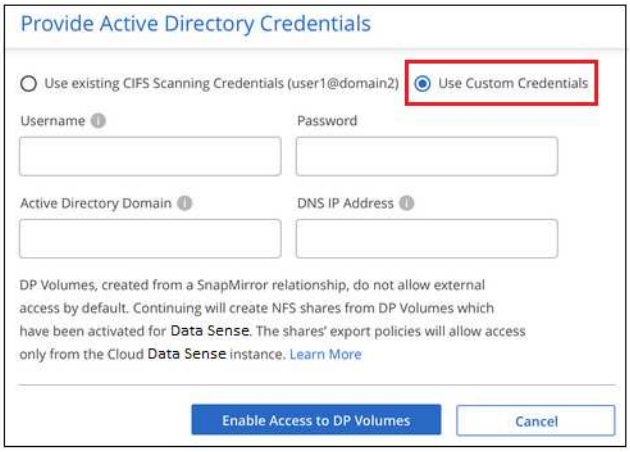


步骤

如果要扫描这些数据保护卷：

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 选择页面顶部的*启用对DP卷的访问*。
3. 查看确认消息并再次选择*启用对DP卷的访问*。
   - 系统将启用最初在源 FSX for ONTAP 文件系统中创建为 NFS 卷的卷。
   - 最初在源 FSX for ONTAP 文件系统中创建为 CIFS 卷的卷需要输入 CIFS 凭据才能扫描这些 DP 卷。如果您已输入Active Directory凭据以便BlueXP分类可以扫描CIFS卷、则可以使用这些凭据、也可以指定一组不同的管理员凭据。





4. 激活要扫描的每个DP卷。

结果

启用后、BlueXP分类会从已激活扫描的每个DP卷创建一个NFS共享。共享导出策略仅允许从BlueXP分类实例进行访问。

如果在最初启用对DP卷的访问后添加了一些CIFS数据保护卷、则配置页面顶部会显示按钮*启用对CIFS DP*的访问。选择此按钮并添加CIFS凭据、以允许访问这些CIFS DP卷。

Active Directory凭据仅会注册到第一个CIFS DP卷的Storage VM中、因此系统将扫描该SVM上的所有DP卷。驻留在其他 SVM 上的任何卷都不会注册 Active Directory 凭据，因此不会扫描这些 DP 卷。

扫描具有**BlueXP** 分类的**Cloud Volumes ONTAP**和内部**ONTAP**卷

完成几个步骤、开始使用BlueXP分类扫描Cloud Volumes ONTAP 和内部ONTAP 卷。

部署**BlueXP**分类实例

如果尚未部署实例、请部署BlueXP分类。

如果您要扫描可通过Internet访问的Cloud Volumes ONTAP和内部ONTAP系统，则可以"在云中部署BlueXP分类"或"位于可访问 Internet 的内部位置"。

如果您要扫描安装在无法访问Internet的非公开站点上的内部ONTAP系统，则需要"在无法访问Internet的同一内部位置部署BlueXP分类"。这还要求在同一内部位置部署BlueXP Connector。

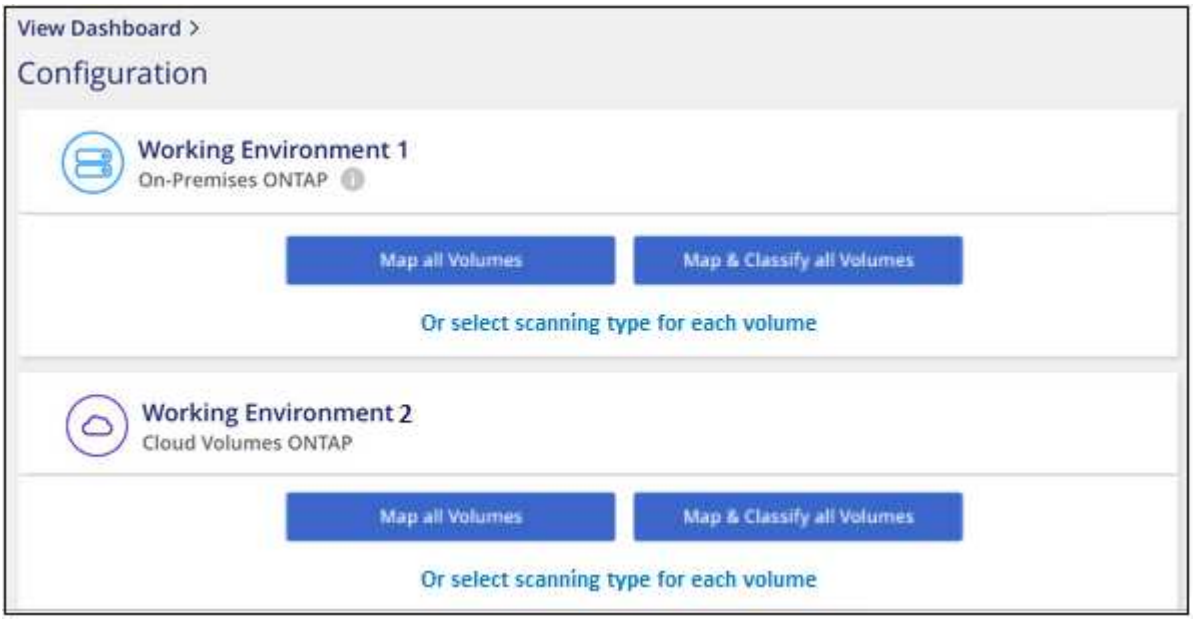
确保以下端口对BlueXP分类实例开放：

- 对于NFS—端口111和2049。
- 对于CIFS—端口139和445。

在您的工作环境中启用**BlueXP** 分类

您可以在任何受支持的云提供商的Cloud Volumes ONTAP 系统上以及内部ONTAP 集群上启用BlueXP分类。

1. 从BlueXP 左侧导航菜单中、选择*监管>分类*。
2. 从BlueXP 分类菜单中，选择*Configuration*。



3. 选择要如何扫描每个工作环境中的卷。"了解映射和分类扫描"：
   - 要映射所有卷，请选择*映射所有卷*。
   - 要映射所有卷并对其进行分类，请选择*映射所有卷并对其进行分类*。
   - 要自定义每个卷的扫描，请选择*或为每个卷选择扫描类型*，然后选择要映射和/或分类的卷。

     有关详细信息、请参见。 对卷启用和禁用合规性扫描
4. 在确认对话框中、单击*批准*以使BlueXP分类开始扫描卷。

结果

BlueXP分类开始扫描您在工作环境中选择的卷。一旦BlueXP分类完成初始扫描、结果将显示在Compliance信息板中。所需时间取决于数据量—可能需要几分钟或几小时。

- 默认情况下、如果BlueXP分类在CIFS中没有写入属性权限或在NFS中没有写入权限、则系统不会扫描卷中的文件、因为BlueXP分类无法将"上次访问时间"还原为原始时间戳。如果您不关心上次访问时间是否已重置、请单击*或为每个卷选择扫描类型*。生成的页面包含一个您可以启用的设置、以便BlueXP分类将扫描卷、而不管权限如何。
- BlueXP分类仅扫描卷下的一个文件共享。如果卷中有多个共享、则需要将这些其他共享作为一个共享组单独扫描。"请参见有关此BlueXP分类限制的更多详细信息"(英文)

验证BlueXP 分类是否有权访问卷

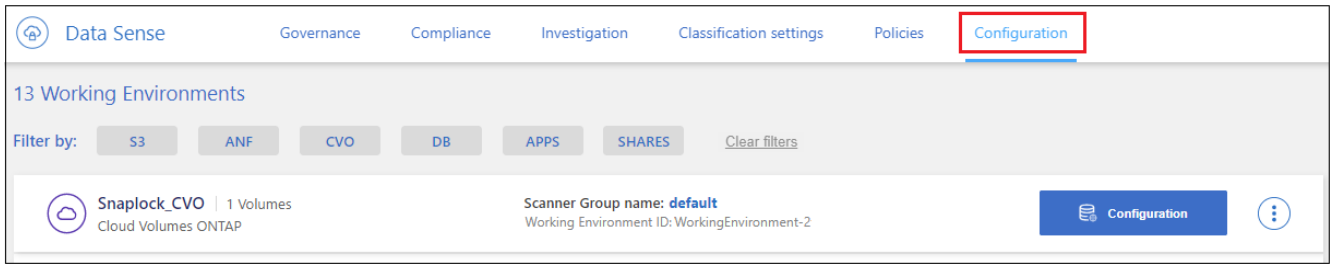
通过检查网络连接、安全组和导出策略、确保BlueXP分类可以访问卷。您需要为BlueXP分类提供CIFS凭据、以便它可以访问CIFS卷。

步骤

1. 确保BlueXP分类实例与包含Cloud Volumes ONTAP 或内部ONTAP 集群卷的每个网络之间具有网络连接。
2. 确保Cloud Volumes ONTAP 的安全组允许来自BlueXP分类实例的入站流量。

   您可以为来自BlueXP分类实例的IP地址的流量打开安全组、也可以为来自虚拟网络内部的所有流量打开安全组。

3. 确保NFS卷导出策略包含BlueXP分类实例的IP地址、以便它可以访问每个卷上的数据。
4. 如果使用CIFS、请提供BlueXP分类和Active Directory凭据、以便它可以扫描CIFS卷。
   a. 从BlueXP 左侧导航菜单中、选择*监管>分类*。
5. 从BlueXP 分类菜单中，选择*Configuration*。

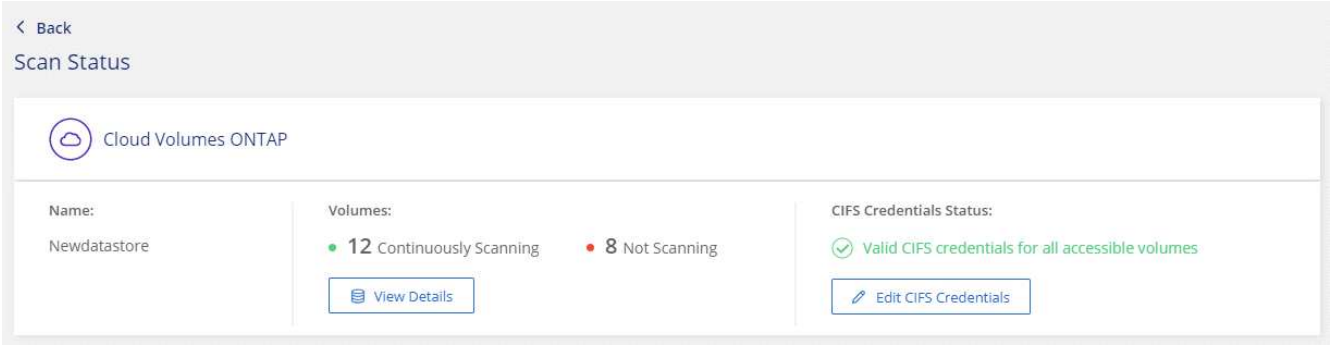


   a. 对于每个工作环境，请选择*编辑CIFS凭据*并输入BlueXP 分类访问系统上的CIFS卷所需的用户名和密码。

      这些凭据可以是只读的、但提供管理员凭据可确保BlueXP分类可以读取需要提升权限的任何数据。这些凭据存储在BlueXP分类实例上。

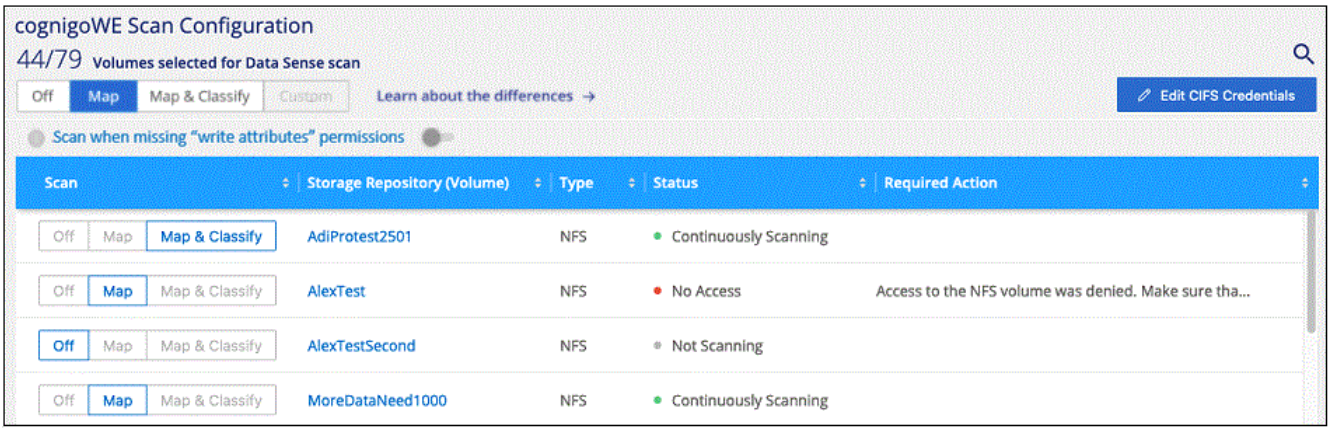
      如果要确保文件"上次访问时间"在BlueXP分类扫描中保持不变、建议用户在CIFS中具有写入属性权限或在NFS中具有写入权限。如果可能、我们建议将Active Directory配置的用户设置为组织中有权访问所有文件的父组的一部分。

      输入凭据后，您应看到一条消息，指出所有 CIFS 卷均已成功通过身份验证。



6. 在配置页面上、选择*查看详细信息*以查看每个CIFS和NFS卷的状态并更正任何错误。

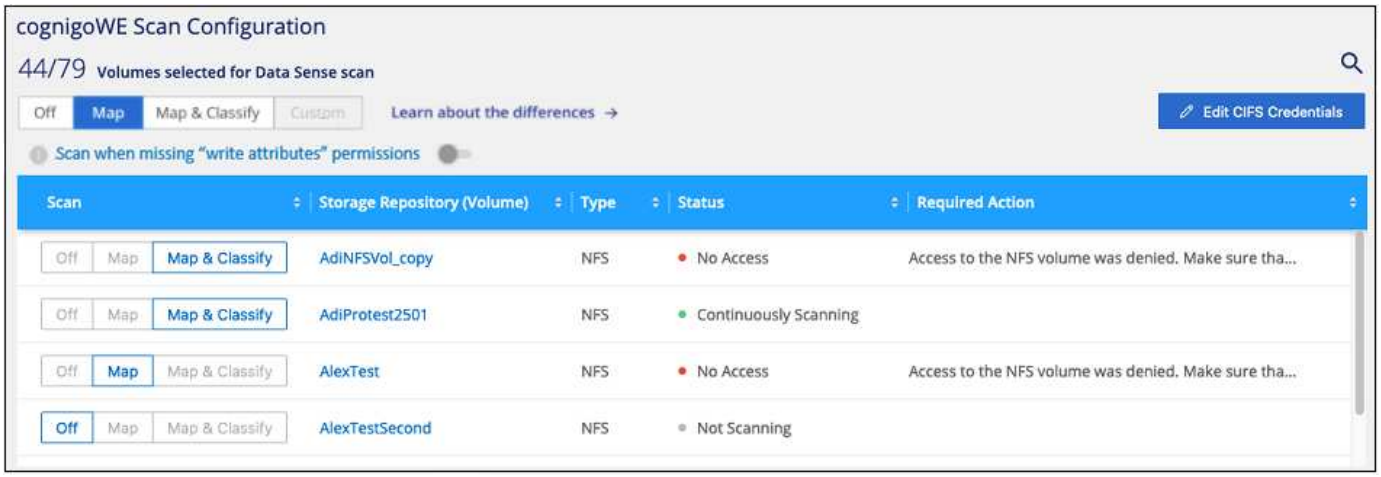
   例如、下图显示了四个卷；其中一个卷由于BlueXP分类实例和卷之间的网络连接问题而无法扫描BlueXP分类。



对卷启用和禁用合规性扫描

您可以随时从 " 配置 " 页面在工作环境中启动或停止仅映射扫描或映射和分类扫描。您也可以从仅映射扫描更改为映射和分类扫描，反之亦然。建议您扫描所有卷。

默认情况下、页面顶部的*缺少"写入属性"权限时扫描*开关处于禁用状态。这意味着、如果BlueXP分类在CIFS中没有写入属性权限、或者在NFS中没有写入权限、则系统将不会扫描文件、因为BlueXP分类无法将"上次访问时间"还原为原始时间戳。如果您不关心上次访问时间是否已重置、请打开此开关、无论权限如何、所有文件都将被扫描。"了解更多信息。"(英文)



步骤

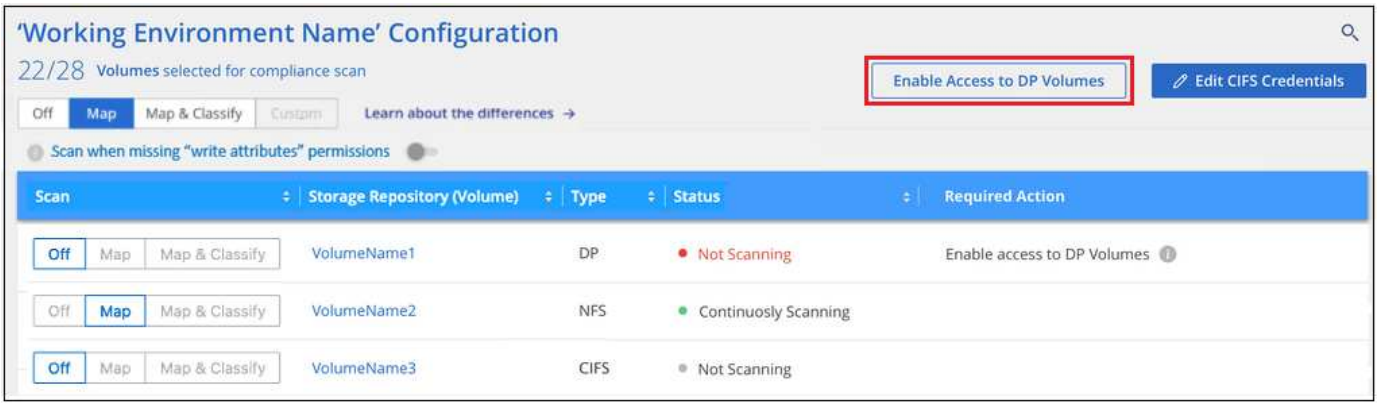
1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 执行以下操作之一：
   - 要对卷启用仅映射扫描，请在卷区域中选择*Map*。或者，要在所有卷上启用，请在标题区域中选择*Map*。要对卷启用完全扫描，请在卷区域中选择*映射和分类*。或者、要在所有卷上启用、请在标题区域中选择*映射和分类*。
   - 要禁用对卷的扫描，请在卷区域中选择*off*。要禁用对所有卷的扫描，请在标题区域中选择*off*。

只有在标题区域中设置了 * 映射 * 或 * 映射和分类 * 设置后，才会自动扫描添加到工作环境中的新卷。如果此选项在标题区域中设置为*Custom*或*Off*，则需要对工作环境中添加的每个新卷激活映射和/或完全扫描。

扫描数据保护卷

默认情况下、不会扫描数据保护(DP)卷、因为这些卷不会对外公开、BlueXP分类无法访问它们。这些卷是从内部 ONTAP 系统或 Cloud Volumes ONTAP 系统执行 SnapMirror 操作的目标卷。

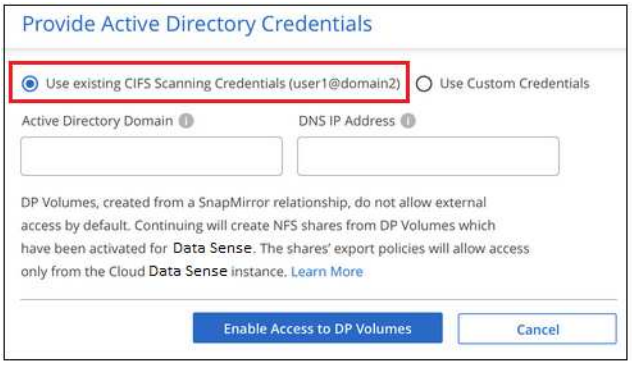
最初，卷列表会将这些卷标识为 *Type* * dp* ，并显示 *Status* * 未扫描 * 和 *Required Action* * Enable Access to DP volumes* 。

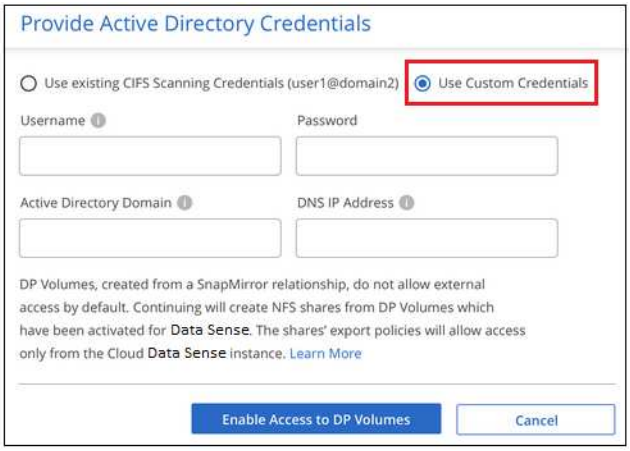


步骤

如果要扫描这些数据保护卷：

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 单击页面顶部的 * 启用对 DP 卷的访问 * 。
3. 查看确认消息并再次选择*启用对DP卷的访问*。
   - 系统会启用最初在源 ONTAP 系统中创建为 NFS 卷的卷。
   - 最初在源 ONTAP 系统中创建为 CIFS 卷的卷需要输入 CIFS 凭据才能扫描这些 DP 卷。如果您已输入Active Directory凭据以便BlueXP分类可以扫描CIFS卷、则可以使用这些凭据、也可以指定一组不同的管理员凭据。





4. 激活要扫描的每个DP卷。

结果

启用后、BlueXP分类会从已激活扫描的每个DP卷创建一个NFS共享。共享导出策略仅允许从BlueXP分类实例进行访问。

如果在最初启用对DP卷的访问后添加了一些CIFS数据保护卷、则配置页面顶部会显示按钮*启用对CIFS DP*的访问。单击此按钮并添加 CIFS 凭据，以便能够访问这些 CIFS DP 卷。

Active Directory凭据仅会注册到第一个CIFS DP卷的Storage VM中、因此系统将扫描该SVM上的所有DP卷。驻留在其他 SVM 上的任何卷都不会注册 Active Directory 凭据，因此不会扫描这些 DP 卷。

扫描具有**BlueXP** 分类的数据库架构

完成几个步骤、开始使用BlueXP分类扫描数据库架构。

查看前提条件

在启用BlueXP分类之前、请查看以下前提条件、以确保您的配置受支持。

支持的数据库

BlueXP分类可以扫描以下数据库中的架构：

- Amazon Relational Database Service （ Amazon RDS ）
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server （ MSSQL ）

数据库中必须启用 * 统计信息收集功能。

无论数据库托管在何处、都可以扫描连接到BlueXP分类实例的任何数据库。要连接到数据库，您只需提供以下信息：

- IP 地址或主机名
- 端口
- 服务名称（仅用于访问 Oracle 数据库）
- 允许对模式进行读取访问的凭据

  选择用户名和密码时、请务必选择对要扫描的所有架构和表具有完全读取权限的用户名和密码。我们建议您为BlueXP分类系统创建一个具有所有必需权限的专用用户。

- 注： * 对于 MongoDB ，需要只读管理员角色。

部署**BlueXP**分类实例

如果尚未部署实例、请部署BlueXP分类。

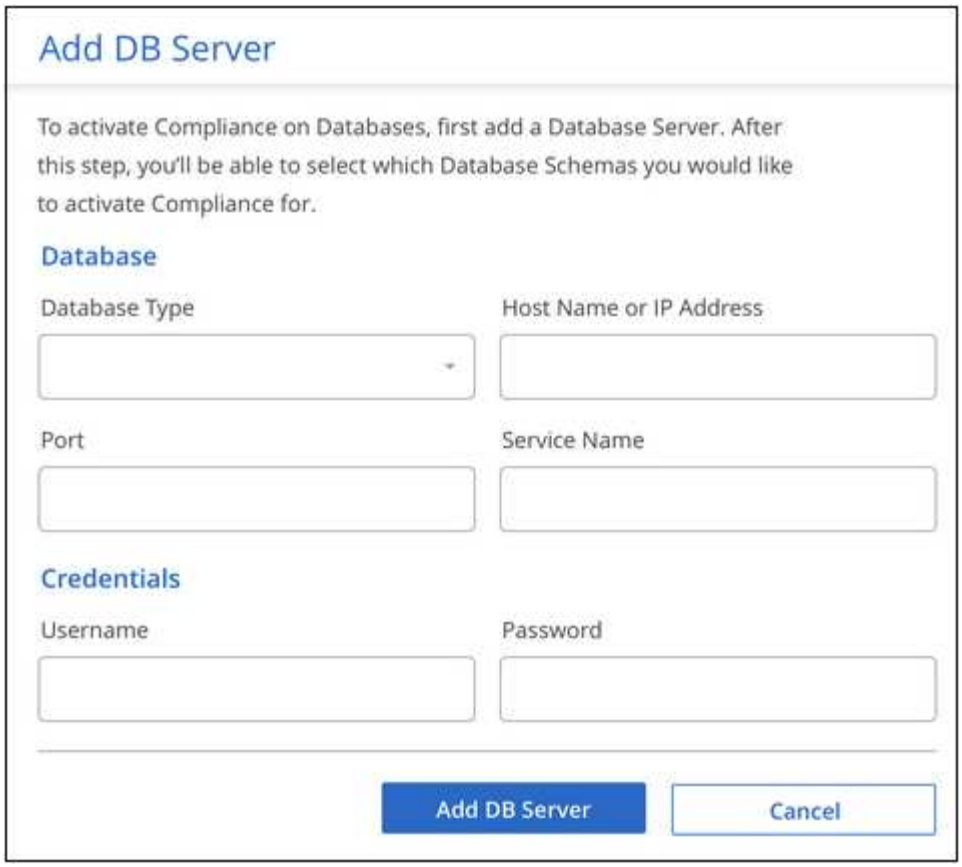
如果正在扫描可通过Internet访问的数据库架构，则可以"在云中部署BlueXP分类"或"在可访问Internet的内部位置部署BlueXP分类"。

如果要扫描安装在无法访问Internet的非公开站点上的数据库架构，则需要"在无法访问Internet的同一内部位置部署BlueXP分类"。这还要求在同一内部位置部署BlueXP Connector。

添加数据库服务器

添加架构所在的数据库服务器。

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 从“配置”页中，选择*Add Working Environment **>*Add Database Server**。
3. 输入所需信息以标识数据库服务器。
   a. 选择数据库类型。
   b. 输入要连接到数据库的端口和主机名或 IP 地址。
   c. 对于 Oracle 数据库，输入服务名称。
   d. 输入凭据、以便BlueXP分类可以访问服务器。
   e. 单击 * 添加数据库服务器 * 。



数据库将添加到工作环境列表中。

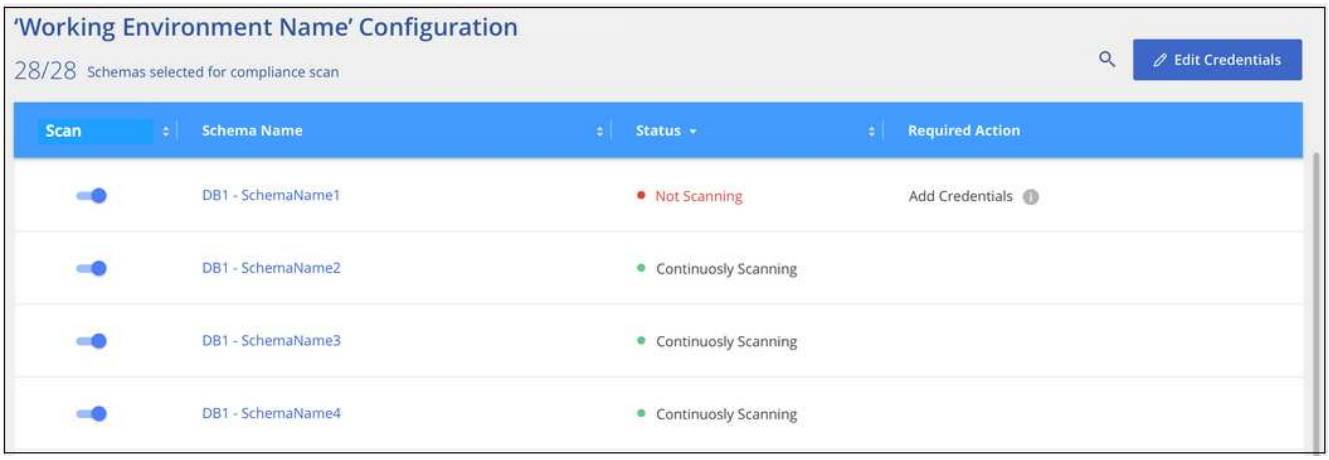
对数据库架构启用和禁用合规性扫描

您可以随时停止或开始对架构进行完全扫描。

没有为数据库架构选择仅映射扫描的选项。

1. 从“配置”页中，选择要配置的数据库的*Configuration*按钮。

2. 向右移动滑块以选择要扫描的架构。



结果

BlueXP分类开始扫描您启用的数据库架构。如果存在任何错误，它们将显示在状态列中，并显示修复此错误所需的操作。

BlueXP 分类每天扫描一次数据库；数据库不会像其他数据源一样连续扫描。

扫描具有**BlueXP** 分类的文件共享

完成几个步骤、开始扫描Google Cloud NetApp卷和旧版NetApp 7-模式系统中的NFS或CIFS文件共享。这些文件共享可以驻留在内部或云中。

BlueXP分类核心版本不支持从非NetApp文件共享扫描数据。

查看文件共享要求

在启用BlueXP分类之前、请查看以下前提条件、以确保您的配置受支持。

- 共享可以托管在任何位置，包括云或内部。可以将旧版NetApp 7-模式存储系统中的CIFS共享扫描为文件共享。

  请注意、BlueXP分类无法从7-模式系统提取权限或"上次访问时间"。此外、由于某些Linux版本与7-模式系统上的CIFS共享之间存在已知问题描述 、因此必须将共享配置为仅使用启用了NTLM身份验证的SMB v1。

- BlueXP分类实例和共享之间需要有网络连接。
- 确保这些端口对BlueXP分类实例开放：
  - 对于 NFS —端口 111 和 2049 。
  - 对于 CIFS —端口 139 和 445 。
- 您可以将DFS (Distributed File System、分布式文件系统)共享添加为常规CIFS共享。但是、由于BlueXP分类不知道共享是基于多个服务器/卷构建的、并将其组合为一个CIFS共享、因此、如果此消息实际上仅显示适用场景位于其他服务器/卷上的其中一个文件夹/共享、则您可能会收到有关此共享的权限或连接错误。
- 对于 CIFS （ SMB ）共享，请确保您具有 Active Directory 凭据来提供对共享的读取访问权限。如果BlueXP分类需要扫描任何需要提升权限的数据、则首选使用管理员凭据。

  如果要确保文件"上次访问时间"在BlueXP分类扫描中保持不变、建议用户在CIFS中具有写入属性权限或

在NFS中具有写入权限。如果可能、我们建议将Active Directory配置的用户设置为组织中有权访问所有文件的父组的一部分。

- 您将需要以格式添加的共享列表 `<host_name>:/<share_path>`。您可以单独输入共享，也可以提供要扫描的文件共享的行分隔列表。

部署**BlueXP**分类实例

如果尚未部署实例、请部署BlueXP分类。

为文件共享创建组

您必须先添加文件共享 "group" ，然后才能添加文件共享。组是要扫描的文件共享的容器，组名称用作这些文件共享的工作环境名称。

您可以在同一个组中混用 NFS 和 CIFS 共享，但是，一个组中的所有 CIFS 文件共享都需要使用相同的 Active Directory 凭据。如果您计划添加使用不同凭据的 CIFS 共享，则必须为每组唯一的凭据创建一个单独的组。

步骤

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 从配置页中，选择*添加工作环境*>*添加文件共享组*。
3. 在"Add Files Shares"(添加文件共享组)对话框中，输入共享组的名称，然后选择*Continue*(继续)。

结果

新的文件共享组将添加到工作环境列表中。

将文件共享添加到组

您可以将文件共享添加到文件共享组、以便按照BlueXP分类扫描这些共享中的文件。您可以按格式添加共享 `<host_name>:/<share_path>`。

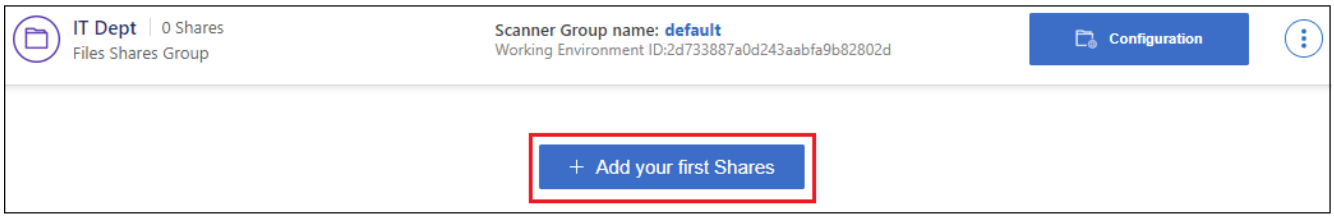
您可以添加单个文件共享，也可以提供要扫描的文件共享的行分隔列表。一次最多可以添加 100 个共享。

在一个组中同时添加 NFS 和 CIFS 共享时，您需要运行此过程两次，一次是添加 NFS 共享，然后再次添加 CIFS 共享。

步骤

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 从"配置"页面上的"工作环境"磁贴中、选择文件共享组的*配置*按钮。

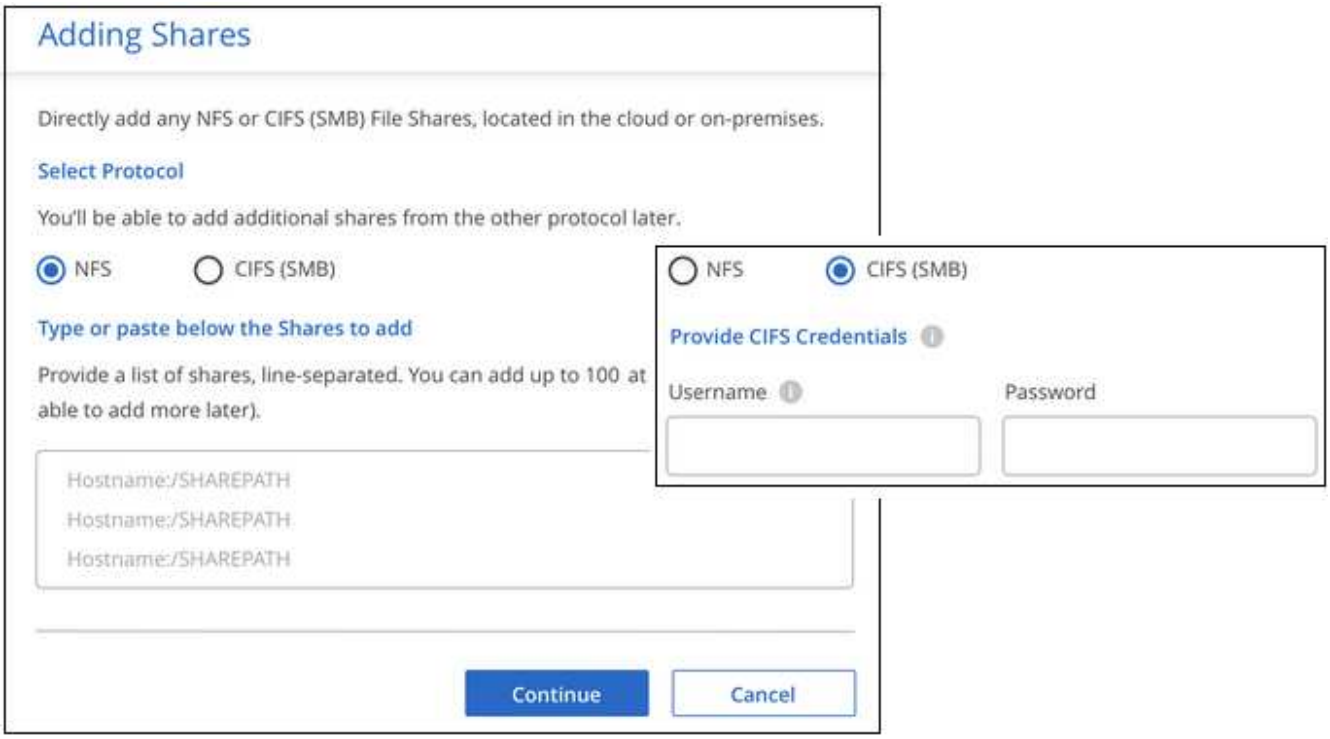
3. 如果这是首次为此文件共享组添加文件共享，请选择*添加您的第一个共享*。



如果要向现有组添加文件共享，请选择*Add Shares*。

4. 为要添加的文件共享选择协议，添加要扫描的文件共享(每行一个文件共享)，然后选择*CONTINUOD*。

   添加 CIFS （ SMB ）共享时，您需要输入 Active Directory 凭据，以提供对共享的读取访问权限。首选管理员凭据。



   确认对话框将显示已添加的共享数量。

   如果此对话框列出了任何无法添加的共享，请捕获此信息，以便解析此问题描述。在某些情况下，您可以使用更正后的主机名或共享名称重新添加共享。

5. 在每个文件共享上启用仅映射扫描或映射和分类扫描。

6. 执行以下操作之一以启用或禁用扫描：
   - 要对文件共享启用仅映射扫描，请选择*Map*。
   - 要对文件共享启用完全扫描，请选择*映射和分类*。
   - 要禁用对文件共享的扫描，请选择*off*。

默认情况下、页面顶部的*缺少"写入属性"权限时扫描*开关处于禁用状态。这意味着、如果BlueXP分类在CIFS中没有写入属性权限、或者在NFS中没有写入权限、则系统将不会扫描文件、因为BlueXP分类无法将"上次访问时间"还原为原始时间戳。如果您不关心上次访问时间是否已重置、请打开此开关、无论权限如何、所有文件都将被扫描。"了解更多信息。"(英文)

结果

BlueXP分类开始扫描您添加的文件共享中的文件、结果将显示在信息板和其他位置。

从合规性扫描中删除文件共享

如果您不再需要扫描某些文件共享，则可以随时从扫描其文件中删除各个文件共享。

步骤

1. 从BlueXP 分类菜单中，选择*Configuration*。
2. 在配置页中，选择*Remove Share*。

使用**BlueXP** 分类扫描**StorageGRID**数据

完成几个步骤、即可开始使用BlueXP 分类直接扫描StorageGRID中的数据。

查看**StorageGRID**要求

在启用BlueXP分类之前、请查看以下前提条件、以确保您的配置受支持。

- 您需要具有端点 URL 才能连接到对象存储服务。
- 您需要具有StorageGRID中的访问密钥和机密密钥、以便BlueXP 分类可以访问存储分段。

部署**BlueXP**分类实例

如果尚未部署实例、请部署BlueXP分类。

如果要从可通过Internet访问的StorageGRID扫描数据，则可以"在云中部署BlueXP分类"或"在可访问Internet的

内部位置部署BlueXP分类"。

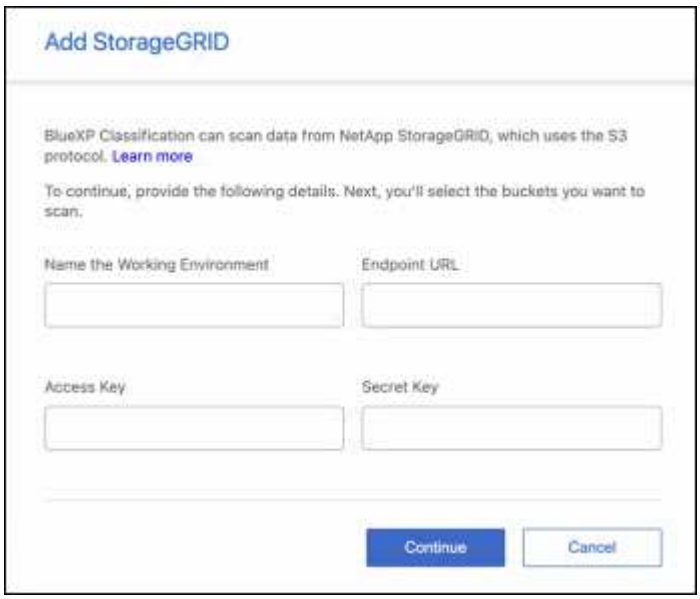
如果要从安装在无法访问Internet的非公开站点上的StorageGRID扫描数据，则需要"在无法访问Internet的同一内部位置部署BlueXP分类"。这还要求在同一内部位置部署BlueXP Connector。

将**StorageGRID**服务添加到**BlueXP** 分类

添加StorageGRID服务。

步骤

1. 从BlueXP 分类菜单中，选择*Configuration*选项。
2. 从“配置”页中，选择*Add Working Environment *>*Add StorageGRID *。
3. 在添加StorageGRID服务对话框中，输入StorageGRID服务的详细信息，然后单击*Continue*。
   a. 输入要用于工作环境的名称。此名称应反映要连接到的StorageGRID服务的名称。
   b. 输入端点 URL 以访问对象存储服务。
   c. 输入访问密钥和机密密钥、以便BlueXP 分类可以访问StorageGRID中的分段。



结果

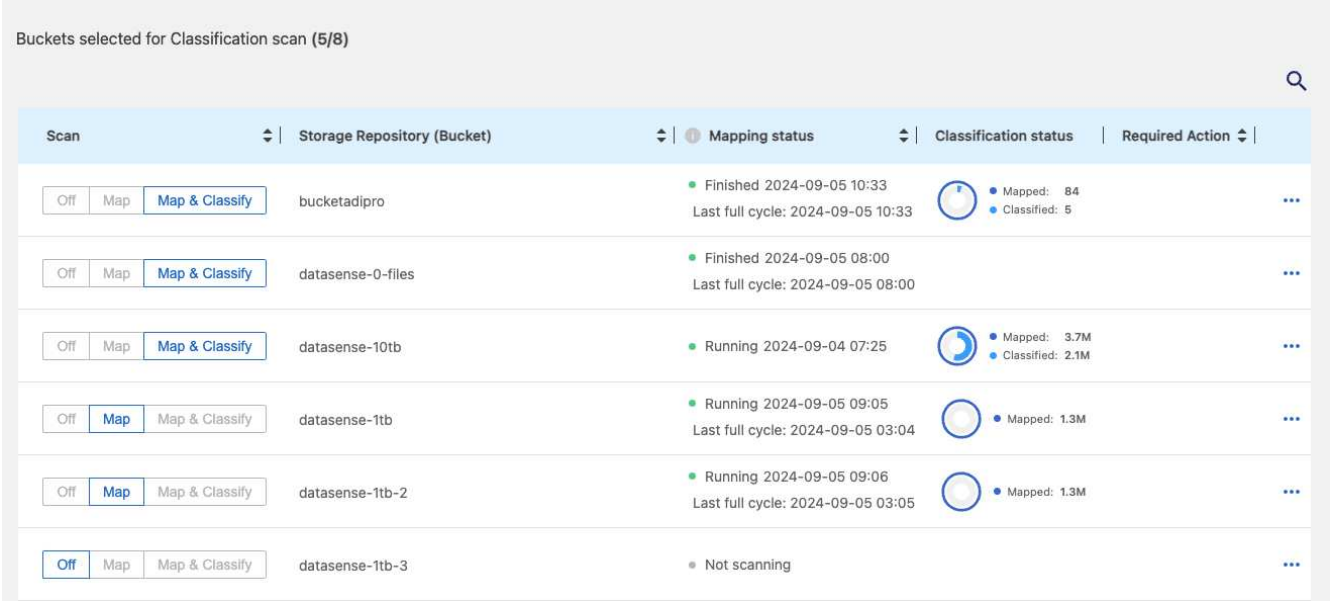
StorageGRID已添加到工作环境列表中。

对**StorageGRID**存储分段启用和禁用合规性扫描

在StorageGRID上启用BlueXP 分类后、下一步是配置要扫描的存储分段。BlueXP分类可发现这些分段、并在您创建的工作环境中显示它们。

步骤

1. 在配置页面中、找到StorageGRID工作环境。
2. 在StorageGRID工作环境磁贴中，选择*Configuration*。



3. 完成以下步骤之一以启用或禁用扫描：
   - 要对存储分段启用仅映射扫描，请选择*Map*。
   - 要对存储分段启用完整扫描，请选择*映射和分类*。
   - 要禁用存储分段上的扫描，请选择*off*。

结果

BlueXP分类开始扫描您启用的分段。如果存在任何错误，它们将显示在状态列中，并显示修复此错误所需的操作。

将Active Directory与BlueXP分类集成

您可以将全局Active Directory与BlueXP分类相集成、以增强BlueXP分类报告的有关文件所有者以及哪些用户和组有权访问您的文件的结果。

在设置某些数据源(如下所列)时、您需要输入Active Directory凭据、以便BlueXP分类扫描CIFS卷。这种集成提供了BlueXP分类、其中包含驻留在这些数据源中的数据的文件所有者和权限详细信息。为这些数据源输入的Active Directory可能与您在此处输入的全局Active Directory凭据不同。BlueXP分类将在所有集成的Active Directory中查找用户和权限详细信息。

此集成在BlueXP分类的以下位置提供追加信息：

- 您可以使用"文件所有者""筛选器"、并在"调查"窗格中查看文件元数据中的结果。此文件所有者不包含 SID （安全标识符），而是使用实际用户名进行填充。
- 单击"查看所有权限"按钮时、您可以查看"完整文件权限"每个文件和目录的。
- 在中"监管信息板"，“打开权限”面板将显示有关数据的更多详细信息。

本地用户 SID 和未知域中的 SID 不会转换为实际用户名。

支持的数据源

与BlueXP分类的Active Directory集成可以标识以下数据源中的数据：

- 内部部署 ONTAP 系统
- Cloud Volumes ONTAP
- Azure NetApp Files
- 适用于 ONTAP 的 FSX
- OneDrive帐户和SharePoint帐户(适用于旧版1.3及更早版本)

不支持从使用简单存储服务(Simple Storage Service、S3)协议的数据库架构、Google Drive帐户、Amazon S3帐户或对象存储中识别用户和权限信息。

连接到**Active Directory**服务器

在部署BlueXP分类并对数据源激活扫描后、您可以将BlueXP分类与Active Directory集成。可以使用 DNS 服务器 IP 地址或 LDAP 服务器 IP 地址访问 Active Directory 。

Active Directory凭据可以是只读的、但提供管理员凭据可确保BlueXP分类可以读取需要提升权限的任何数据。这些凭据存储在BlueXP分类实例上。

对于CIFS卷/文件共享、如果要确保文件"上次访问时间"在BlueXP分类扫描中保持不变、建议用户具有写入属性权限。如果可能、我们建议将Active Directory配置的用户设置为组织中有权访问所有文件的父组的一部分。

要求

- 您必须已为公司中的用户设置 Active Directory 。
- 您必须具有 Active Directory 的信息：
  - DNS 服务器 IP 地址或多个 IP 地址

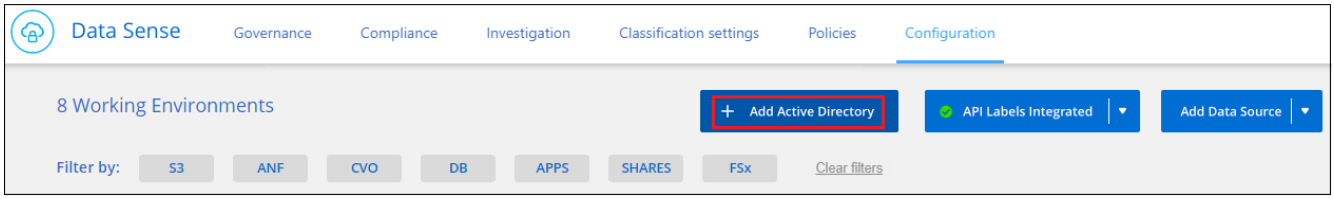
    或

  LDAP 服务器 IP 地址或多个 IP 地址
  - 用于访问服务器的用户名和密码
  - 域名（ Active Directory 名称）
  - 是否使用安全 LDAP （ LDAPS ）
  - LDAP 服务器端口（对于 LDAP ，通常为 389 ；对于安全 LDAP ，通常为 636 ）
- 必须通过BlueXP分类实例为出站通信打开以下端口：

协议	端口	目标	目的
TCP 和 UDP	389	Active Directory	LDAP
TCP	636	Active Directory	基于 SSL 的 LDAP
TCP	3268	Active Directory	全局目录
TCP	3269	Active Directory	基于 SSL 的全局目录

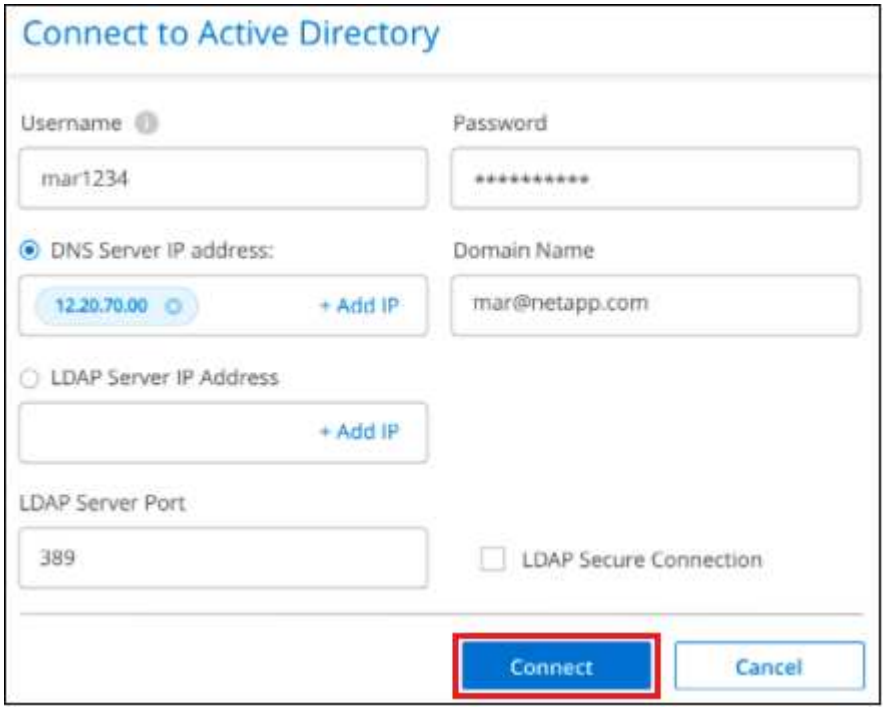
步骤

1. 从"BlueXP分类配置"页面中，单击*Add Active Directory*。

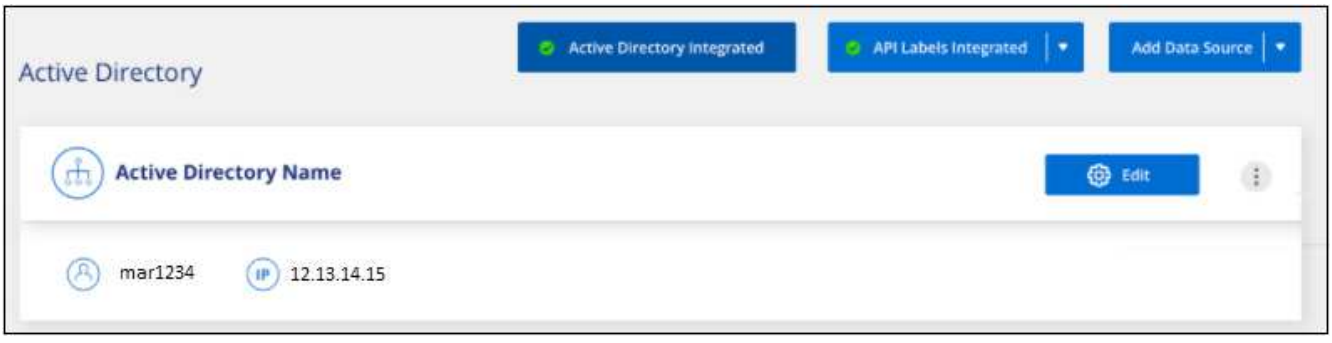


2. 在连接到 Active Directory 对话框中，输入 Active Directory 详细信息，然后单击 * 连接 * 。

   如果需要，可以单击 * 添加 IP* 来添加多个 IP 地址。



   BlueXP分类集成到Active Directory中、并在"配置"页面中添加了一个新部分。



管理Active Directory集成

如果需要修改 Active Directory 集成中的任何值，请单击 * 编辑 * 按钮并进行更改。

如果不再需要集成，也可以单击按钮，然后单击*Remove Active Directory*来删除它。

有关BlueXP分类的常见问题

如果您只是想快速了解问题解答，此常见问题解答会很有帮助。

BlueXP分类服务

以下问题概括说明了BlueXP分类。

什么是BlueXP分类?

BlueXP分类是一种云产品、它使用人工智能(AI)驱动的技术帮助您了解数据环境并识别存储系统中的敏感数据。这些系统可以是您已添加到BlueXP Canvas中的工作环境、也可以是BlueXP分类可通过网络访问的多种类型的数据源。"请参见下面的完整列表"(英文)

BlueXP分类提供了预定义的参数(例如敏感信息类型和类别)、以满足有关数据隐私和敏感性的新数据合规性法规、例如GDPR、CCPA、HIPAA等。

BlueXP分类的工作原理是什么?

BlueXP分类可在BlueXP系统和存储系统的旁边部署另一层人工智能。然后、它会扫描卷、分段、数据库和其他存储帐户上的数据、并为找到的数据洞察力编制索引。BlueXP分类利用人工智能和自然语言处理、而不是通常围绕正则表达式和模式匹配构建的替代解决方案。

BlueXP分类使用AI提供对数据的上下文了解、以实现准确的检测和分类。它由AI驱动、因为它专为现代数据类型和规模而设计。它还了解数据环境、以便提供强大、准确的发现和分类。

"详细了解BlueXP分类的工作原理"(英文)

"详细了解BlueXP分类的用例"(英文)

BlueXP分类的架构如何?

BlueXP分类可在云端或内部部署一个服务器或集群、无论您选择在何处。这些服务器通过标准协议连接到数据源、并为Elasticsearch集群中的结果编制索引、该集群也部署在相同的服务器上。这样可以支持多云、跨云、私有云和内部环境。

支持哪些云提供商?

BlueXP分类作为BlueXP的一部分运行、并支持AWS、Azure和GCP。这样，您的组织就可以在不同的云提供商之间实现统一的隐私可见性。

BlueXP分类是否具有REST API？是否可与第三方工具配合使用?

否、BlueXP分类没有REST API。

BlueXP分类是否可通过商城获得?

是的、BlueXP和BlueXP分类可从AWS、Azure和GCP市场获得。

BlueXP分类扫描和分析

以下问题与用户可用的BlueXP分类扫描性能和分析相关。

BlueXP分类多久扫描一次我的数据?

虽然初始数据扫描可能需要一点时间、但后续扫描只会检查增量更改、从而缩短系统扫描时间。BlueXP分类功能会以循环方式持续扫描数据、一次扫描六个存储库、以便快速对所有更改过的数据进行分类。

"了解扫描的工作原理"(英文)

请注意、BlueXP分类每天只扫描一次数据库-数据库不会像其他数据源一样连续扫描。

数据扫描对存储系统和数据的影响可以忽略不计。但是、如果您担心的影响非常小、则可以将BlueXP分类配置为执行"慢速"扫描。"请参见如何降低扫描速度"(英文)

是否可以使用BlueXP分类搜索数据?

BlueXP分类提供了广泛的搜索功能、使您可以轻松搜索所有连接源中的特定文件或数据片段。BlueXP分类使用户能够更深入地搜索元数据所反映的内容。它是一种不受语言限制的服务、还可以读取文件并分析多种敏感数据类型、例如名称和ID。例如、用户可以在结构化数据存储和非结构化数据存储之间进行搜索、以查找可能违反公司策略从数据库泄漏到用户文件的数据。可以保存搜索以供日后使用、也可以创建策略以按设置的频率搜索结果并对结果执行操作。

找到感兴趣的文件后、可以列出相关特征、包括标记、工作环境帐户、存储分段、文件路径、 类别(来自分类)、文件大小、上次修改、权限状态、重复、 敏感度级别、个人数据、文件中的敏感数据类型、所有者、文件类型、文件大小、创建时间、 文件哈希、数据是否已分配给需要关注的人员等。筛选器可用于筛选与此无关的特征。BlueXP分类还具有RBAC控件、允许在具有适当权限的情况下移动或删除文件。如果不存在适当的权限、则可以将任务分配给组织中拥有适当权限的人员。

BlueXP分类是否提供报告?

是。BlueXP分类提供的信息可能与组织中的其他利益相关方相关、因此我们可以帮助您生成报告以分享见解。以下报告可用于BlueXP分类:

隐私风险评估报告
: 根据您的数据提供隐私洞察力并获得隐私风险得分。"了解更多信息。"(英文)

数据主体访问请求报告
: 用于提取包含数据主体的特定名称或个人标识符相关信息的所有文件的报告。"了解更多信息。"(英文)

PCI DSS 报告
: 帮助您确定信用卡信息在整个文件中的分布情况。"了解更多信息。"(英文)

HIPAA 报告
: 帮助您确定运行状况信息在文件中的分布情况。"了解更多信息。"(英文)

数据映射报告
: 提供有关工作环境中文件大小和数量的信息。其中包括使用容量，数据期限，数据大小和文件类型。"了解更多信息。"(英文)

数据发现评估报告

对扫描的环境进行高级别分析、以突出显示系统的发现结果、并显示关注领域和可能的修复步骤。"学习模式"(英文)

报告特定信息类型

我们提供的报告包含有关包含个人数据和敏感个人数据的已识别文件的详细信息。您还可以查看按类别和文件类型细分的文件。"了解更多信息。"(英文)

扫描性能是否有所不同?

扫描性能可能因网络带宽和环境中的平均文件大小而异。它还可能取决于主机系统（在云端或内部）的大小特征。有关详细信息、请参见 "BlueXP分类实例" 和 "正在部署BlueXP分类" 。

在首次添加新数据源时，您还可以选择仅执行 " 映射 " 扫描，而不是执行完整的 " 分类 " 扫描。由于无法访问文件以查看数据源中的数据，因此可以非常快速地对数据源进行映射。"查看映射扫描与分类扫描之间的区别"(英文)

BlueXP分类管理和隐私

以下问题提供了有关如何管理BlueXP分类和隐私设置的信息。

如何启用**BlueXP**分类?

首先、您需要在BlueXP中或内部系统上部署BlueXP分类实例。实例运行后，您可以从*Configuration*选项卡或通过选择特定的工作环境在现有工作环境、数据库和其他数据源上启用该服务。

"了解如何开始使用"(英文)

在数据源上激活BlueXP分类会立即执行初始扫描。扫描结果会在之后不久显示。

如何禁用**BlueXP**分类?

您可以从"BlueXP分类配置"页面中禁用BlueXP分类、使其无法扫描单个工作环境、数据库或文件共享组。

"了解更多信息。"(英文)

要完全删除BlueXP分类实例、您可以从云提供商的门户或内部位置手动删除BlueXP分类实例。

我是否可以根据组织的需求自定义服务?

BlueXP分类可帮助您深入了解数据。您可以根据组织的需求提取和利用这些洞察信息。

此外、BlueXP分类还提供了多种方法来添加BlueXP分类将在扫描中识别的自定义"个人数据"列表、从而为您提供有关组织的_all_文件中潜在敏感数据所在位置的完整信息。

- 您可以根据要扫描的数据库中的特定列添加唯一标识符—我们称之为*数据Fusion *。
- 您可以从文本文件添加自定义关键字。
- 您可以使用正则表达式(regex)添加自定义模式。

"了解更多信息。"(英文)

是否可以指示服务排除某些目录中的扫描数据?

是。如果希望BlueXP分类排除驻留在特定数据源目录中的扫描数据、则可以将该列表提供给分类引擎。应用此更改后、BlueXP分类将排除指定目录中的扫描数据。

"了解更多信息。"(英文)

是否已扫描驻留在**ONTAP**卷上的快照?

不会。BlueXP 分类不会扫描快照、因为其内容与卷中的内容相同。

如果在 **ONTAP** 卷上启用了数据分层，会发生什么情况?

当BlueXP分类扫描冷数据分层到对象存储的卷时、它会扫描所有数据—本地磁盘上的数据以及分层到对象存储的冷数据。实施分层的非NetApp产品也是如此。

扫描不会加热冷数据—它会保持冷状态并保留在对象存储中。

源系统的类型和数据类型

以下问题与可扫描的存储类型以及所扫描的数据类型有关。

可以使用**BlueXP**分类扫描哪些数据源?

BlueXP分类可以扫描您添加到BlueXP Canvas中的工作环境中的数据、以及BlueXP分类可以通过网络访问的多种结构化和非结构化数据源中的数据。

请参阅。 "支持的工作环境和数据源"

在政府区域部署时是否存在任何限制?

如果Connector部署在政府区域(AWS GovCloud、Azure Gov或Azure DoD)中、则支持BlueXP分类、也称为"受限模式"。以这种方式部署时、BlueXP分类具有以下限制：

*注*此信息仅与BlueXP 分类旧版1.3及更早版本相关。

- 无法扫描OneDrive帐户、SharePoint帐户和Google Drive帐户。
- 无法集成Microsoft Azure信息保护(AIP)标签功能。

如果在无法访问**Internet**的站点上安装**BlueXP**分类、则可以扫描哪些数据源?

BlueXP分类只能扫描内部站点本地数据源中的数据。此时、BlueXP分类可以在"专用模式"(也称为"非公开"站点)下扫描以下本地数据源：

- 内部部署 ONTAP 系统
- 数据库架构

- 使用简单存储服务（ S3 ）协议的对象存储

请参阅。 "支持的工作环境和数据源"

支持哪些文件类型?

BlueXP分类会扫描所有文件以查看类别和元数据洞察力、并在信息板的文件类型部分中显示所有文件类型。

当BlueXP分类检测到个人身份信息(PII)或执行DSAR搜索时、仅支持以下文件格式：

```
.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX,
Docs, Sheets, and Slides
```

BlueXP分类可捕获哪些类型的数据和元数据?

通过BlueXP分类、您可以对数据源运行常规"映射"扫描或完整的"分类"扫描。映射仅提供数据的概览，而 " 分类 " 则提供数据的深度扫描。由于无法访问文件以查看数据源中的数据，因此可以非常快速地对数据源进行映射。

- 数据映射扫描：BlueXP 分类仅扫描元数据。这对于整体数据管理和监管、快速的项目范围界定、非常大的资产和优先级排序非常有用。数据映射基于元数据、被视为*快速*扫描。

  快速扫描后、您可以生成数据映射报告。本报告概述了存储在企业数据源中的数据、可帮助您确定资源利用率、迁移、备份、安全性和合规性流程。

- 数据分类(深度)扫描：在整个环境中使用标准协议和只读权限进行BlueXP 分类扫描。系统会打开并扫描选定文件、以查看与业务相关的敏感数据、私有信息以及与勒索软件相关的问题。

  完成完整扫描后、您可以对数据应用许多其他BlueXP分类功能、例如在"数据调查"页面中查看和细化数据、在文件中搜索名称、复制、移动和删除源文件等。

BlueXP分类可捕获元数据、例如：文件名、权限、创建时间、上次访问和上次修改。这包括"数据调查详细信息"页面和"数据调查报告"中显示的所有元数据。

BlueXP 分类可以识别多种类型的私有数据、例如个人信息(Pii)和敏感个人信息(SPii)。有关私有数据的详细信息，请参见 "BlueXP分类扫描的私有数据的类别"。

是否可以将**BlueXP**分类信息限制为特定用户?

是的、BlueXP分类与BlueXP完全集成。BlueXP 用户只能查看其根据权限有资格查看的工作环境的信息。

此外，如果要允许某些用户只查看BlueXP 分类扫描结果而不管理BlueXP 分类设置，则可以为这些用户分配*Classification viewer*角色(在标准模式下使用BlueXP 时)或*Compliance Viewer*角色(在受限模式下使用BlueXP 时)。

"了解更多信息。"(英文)

任何人都可以访问在我的浏览器和**BlueXP**分类之间发送的私有数据吗?

不可以。您的浏览器和BlueXP 分类实例之间发送的私有数据会通过TLS 1.2进行端到端加密来保护、这意味着NetApp和非NetApp方无法读取这些数据。除非您申请并批准访问权限、否则BlueXP分类不会与NetApp共享任何数据或结果。

扫描的数据会保留在您的环境中。

如何处理敏感数据?

NetApp无法访问敏感数据、也不会在UI中显示这些数据。敏感数据会被屏蔽、例如、信用卡信息会显示最后四个数字。

数据存储在何处?

扫描结果存储在BlueXP分类实例中的ElancSearch中。

如何访问数据?

BlueXP分类可通过API调用访问存储在EI路径 搜索中的数据、API调用需要进行身份验证、并使用AES-128进行加密。要访问EI路径 搜索、直接需要root访问权限。

许可证和成本

以下问题与使用BlueXP分类的许可和成本有关。

BlueXP分类的成本是多少?

BlueXP分类是BlueXP的核心功能、不收费。

连接器部署

以下问题与BlueXP Connector相关。

什么是连接器?

Connector是在您的云帐户或内部环境中的计算实例上运行的软件、可使BlueXP安全地管理云资源。要使用BlueXP分类、您必须部署Connector。

连接器需要安装在何处?

- 在AWS中的Cloud Volumes ONTAP或Amazon FSx for ONTAP中扫描数据时、您需要使用AWS中的连接器。
- 在 Azure 或 Azure NetApp Files 中的 Cloud Volumes ONTAP 中扫描数据时，您可以使用 Azure 中的连接器。
- 在 GCP 的 Cloud Volumes ONTAP 中扫描数据时，您可以在 GCP 中使用连接器。
- 在扫描内部ONTAP系统、NetApp文件共享或数据库中的数据时、您可以使用这些云位置中任何位置的连接器。

因此，如果您在其中许多位置都有数据，则可能需要使用 "多个连接器"。

BlueXP分类是否需要访问凭据?

BlueXP分类本身不会检索存储凭据。而是存储在BlueXP Connector中。

BlueXP分类使用数据平面凭据、例如CIFS凭据在扫描前挂载共享。

是否可以在自己的主机上部署此连接器?

是。您可以在网络中的Linux主机上、也可以 "在内部部署 Connector"在云中的主机上。如果您计划在内部部署BlueXP分类、则可能还需要在内部安装Connector、但这不是必需的。

服务和连接器之间的通信是否使用**HTTP**?

是的、BlueXP分类使用HTTP与BlueXP Connector进行通信。

没有**Internet**访问的安全站点如何?

是的、这一点也受支持。您可以 "在无法访问Internet的内部Linux主机上部署Connector"。 "这也称为"专用模式""(英文)。然后、您可以发现内部ONTAP 集群和其他本地数据源、并使用BlueXP分类扫描数据。

BlueXP分类部署

以下问题与单独的BlueXP分类实例相关。

BlueXP分类支持哪些部署模式?

借助BlueXP、用户几乎可以在任何位置扫描和报告系统、包括内部环境、云和混合环境。BlueXP分类通常使用SaaS模式进行部署、在该模式中、服务通过BlueXP界面启用、无需安装硬件或软件。即使在这种即点即用的部署模式下、无论数据存储是在内部还是在公有 云中、都可以进行数据管理。

BlueXP分类需要哪种类型的实例或**VM**?

时间"部署在云中":

- 在AWS中、BlueXP分类在具有500 GiB GP2磁盘的m6i.4x大型 实例上运行。您可以在部署期间选择较小的实例类型。
- 在Azure中、BlueXP分类在具有500 GiB磁盘的Standard" D16s_v3虚拟机上运行。
- 在GCP中、BlueXP分类在具有500 GiB标准永久性磁盘的n2-standard-16虚拟机上运行。

"详细了解BlueXP分类的工作原理"(英文)

是否可以在自己的主机上部署**BlueXP**分类?

是。您可以在可通过网络或云访问Internet的Linux主机上安装BlueXP分类软件。一切都运行正常、您可以继续通过BlueXP管理扫描配置和结果。有关系统要求和安装详细信息、请参见"在内部部署BlueXP分类"。

没有**Internet**访问的安全站点如何?

是的、这一点也受支持。您可以"在无法访问Internet的内部站点中部署BlueXP分类"访问完全安全的站点。