



部署BlueXP分类弃用

BlueXP classification

NetApp
June 14, 2024

目录

部署BlueXP分类弃用	1
对于无法访问Internet的大型配置、在多个主机上安装BlueXP分类	1
将扫描程序节点添加到现有部署中	2

部署BlueXP分类弃用

对于无法访问Internet的大型配置、在多个主机上安装BlueXP分类

完成几个步骤、在无法访问Internet的内部站点中的多个主机上安装BlueXP分类、也称为_private mode_。此类安装非常适合您的安全站点。

对于需要扫描站点中数PB的数据而不能访问Internet的超大型配置、您可以包含多个主机以提供额外的处理能力。使用多个主机系统时，主系统称为 *Manager node* ，提供额外处理能力的其他系统称为 扫描 程序 *nodes* 。

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

*注*此信息仅与BlueXP分类的旧版版本1.3及更早版本相关。

您需要的内容

- 验证管理器和扫描程序节点的所有Linux系统是否满足主机要求。
- 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要求。
- 您必须具有计划使用的扫描程序节点主机的 IP 地址。
- 必须在所有主机上启用以下端口和协议：

Port	协议	Description
2377	TCP	集群管理通信
7946	TCP , UDP	节点间通信
4789	UDP	覆盖网络流量
50	电子服务	加密的 IPsec 覆盖网络 (ESP) 流量
111.	TCP , UDP	用于在主机之间共享文件的 NFS 服务器 (需要从每个扫描程序节点到管理器节点)
2049.	TCP , UDP	用于在主机之间共享文件的 NFS 服务器 (需要从每个扫描程序节点到管理器节点)

步骤

1. 按照中的步骤 1 至 8 进行操作 "[单主机安装](#)" 在管理器节点上。
2. 如步骤 9 所示，在安装程序提示时，您可以在一系列提示中输入所需值，也可以将所需参数作为命令行参数提供给安装程序。

除了可用于单主机安装的变量之外，还会使用一个新选项 * -n <node_IP>* 来指定扫描程序节点的 IP 地址。多个节点 IP 以逗号分隔。

例如、此命令将添加3个扫描程序节点：

```
sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host  
<ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no  
-proxy --darksite
```

3. 在管理器节点安装完成之前，将显示一个对话框，其中显示了扫描程序节点所需的安装命令。复制命令(例如：`sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`)并将其保存在文本文件中。
4. 在 * 每个 * 扫描程序节点主机上：
 - a. 将Data sense安装程序文件(* `cc_onprem_installer.tar.gz`*)复制到主机。
 - b. 解压缩安装程序文件。
 - c. 粘贴并运行在步骤 3 中复制的命令。

在所有扫描程序节点上完成安装且这些节点已加入管理器节点后，管理器节点安装也会完成。

结果

BlueXP分类安装程序完成软件包安装并注册安装。安装可能需要 15 到 25 分钟。

下一步行动

在配置页面中，您可以选择本地 **"内部 ONTAP 集群"** 和本地 **"数据库"** 要扫描的。

将扫描程序节点添加到现有部署中

您可以将扫描程序节点添加到可访问Internet的Linux主机上的现有部署中。

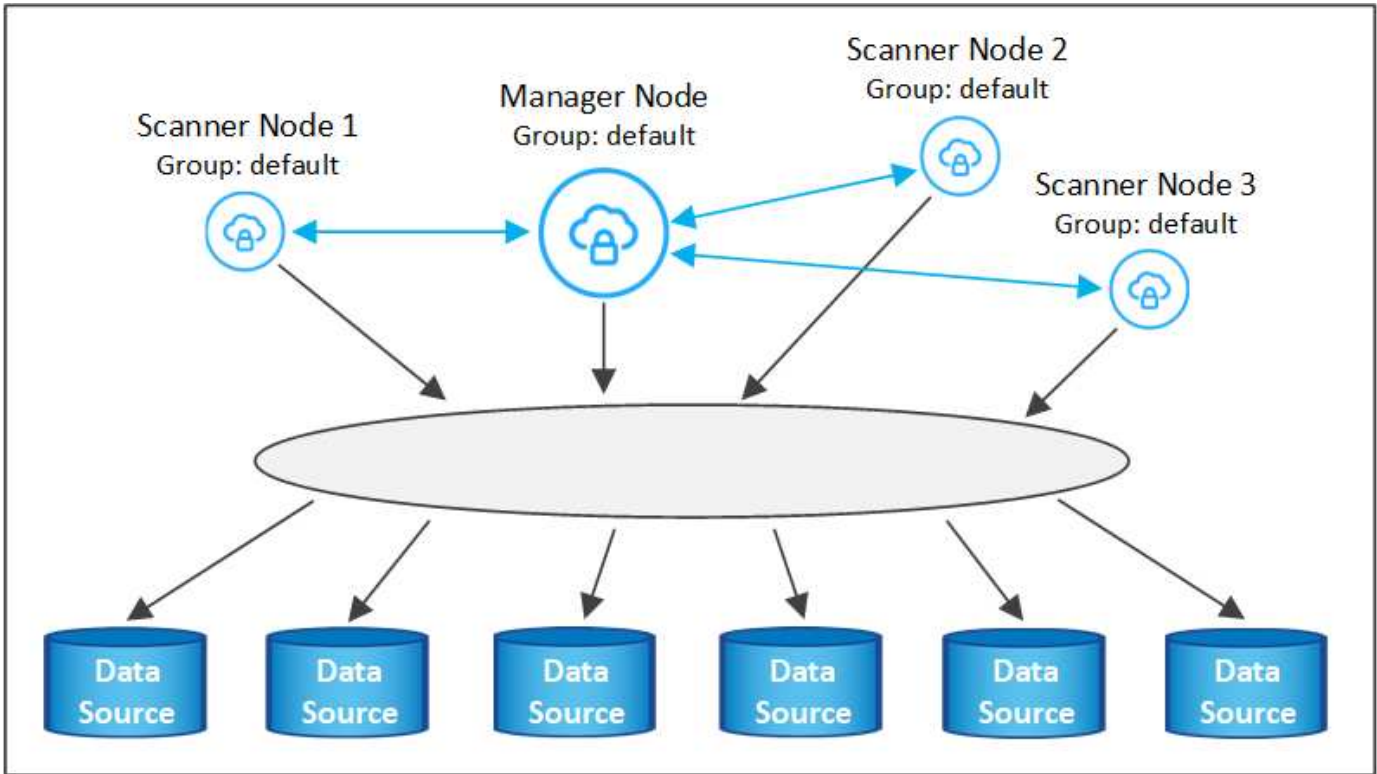
如果您发现扫描数据源需要更多扫描处理能力、则可以添加更多扫描程序节点。您可以在安装管理器节点后立即添加扫描程序节点、也可以稍后添加扫描程序节点。例如、如果您意识到一个数据源中的数据量在6个月后增加了一倍或增加了三倍、则可以添加一个新的扫描程序节点来协助进行数据扫描。

*注*此信息仅与BlueXP分类的旧版版本1.3及更早版本相关。

您可以通过两种方式添加其他扫描程序节点：

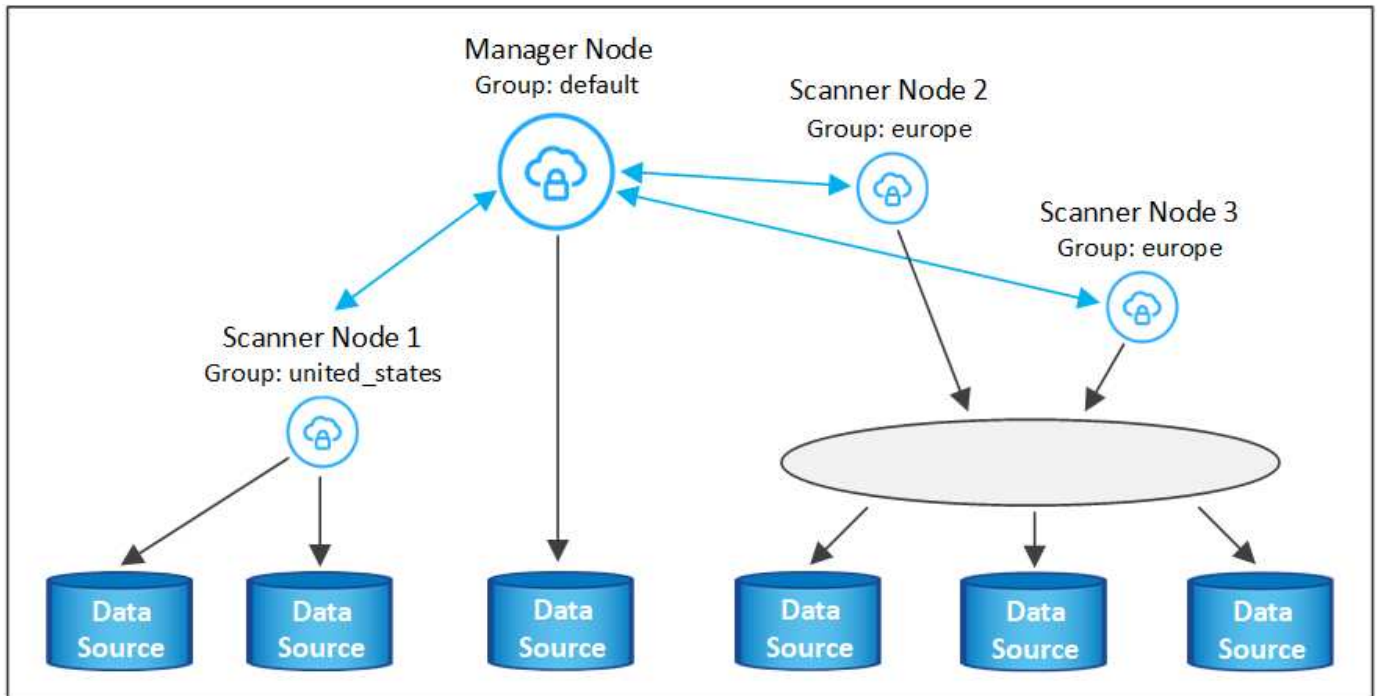
- 添加一个节点以协助扫描所有数据源
- 添加节点以协助扫描特定数据源或特定数据源组(通常基于位置)

默认情况下、您添加的任何新扫描程序节点都会添加到常规扫描资源池中。这称为**"默认扫描程序组"**。在下图中、**"默认"**组中有1个管理器节点和3个扫描程序节点、这些节点均扫描所有6个数据源中的数据。



如果您的某些数据源要由物理上更接近数据源的扫描程序节点扫描，则可以定义一个扫描程序节点或一组扫描程序节点、以扫描特定数据源或一组数据源。在下图中、有1个管理器节点和3个扫描程序节点。

- 管理器节点位于"默认"组中、它正在扫描1个数据源
- 扫描程序节点1位于"United States"组中、它正在扫描2个数据源
- 扫描程序节点2和3属于"欧洲"组、它们共享3个数据源的扫描任务



BlueXP分类扫描程序组可以定义为存储数据的单独地理区域。您可以在全球部署多个BlueXP分类扫描程序节

点、并为每个节点选择一个扫描程序组。这样、每个扫描程序节点都会扫描与其最接近的数据。扫描程序节点与数据的距离越近、越好、因为它可以在扫描数据时尽可能地减少网络延迟。

您可以选择要添加到BlueXP分类的扫描程序组、也可以选择其名称。BlueXP分类不会强制将映射到名为"Euro"的扫描程序组的节点部署在欧洲。

您将按照以下步骤安装其他BlueXP分类扫描程序节点：

1. 准备用作扫描程序节点的Linux主机系统
2. 将Data sense软件下载到这些Linux系统
3. 在管理器节点上运行命令以确定扫描程序节点
4. 按照以下步骤在扫描程序节点上部署软件(也可以为某些扫描程序节点定义"扫描程序组")
5. 如果定义了扫描程序组、请在管理器节点上：
 - a. 打开文件"工作环境_to_scanner_group_config.yml"、并定义每个扫描程序组要扫描的工作环境
 - b. 运行以下脚本、将此映射信息注册到所有扫描程序节点：
`update_we_scanner_group_from_config_file.sh`

您需要的内容

- 验证扫描程序节点的所有Linux系统是否满足主机要求。
- 验证系统是否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。
- 验证您的环境是否满足所需的权限和连接。
- 您必须具有要添加的扫描程序节点主机的IP地址。
- 您必须知道BlueXP分类管理器节点主机系统的IP地址
- 您必须具有连接器系统的IP地址或主机名、NetApp帐户ID、连接器客户端ID和用户访问令牌。如果您计划使用扫描程序组、则需要知道帐户中每个数据源的工作环境ID。要获取此信息、请参见下面的*前提条件步骤_*
- 必须在所有主机上启用以下端口和协议：

Port	协议	Description
2377	TCP	集群管理通信
7946	TCP , UDP	节点间通信
4789	UDP	覆盖网络流量
50	电子服务	加密的 IPsec 覆盖网络 (ESP) 流量
111.	TCP , UDP	用于在主机之间共享文件的 NFS 服务器 (需要从每个扫描程序节点到管理器节点)
2049.	TCP , UDP	用于在主机之间共享文件的 NFS 服务器 (需要从每个扫描程序节点到管理器节点)

- 如果您使用的是 ... firewalld 在BlueXP分类计算机上、我们建议您在安装BlueXP分类之前启用它。运行以下命令进行配置 firewalld 以便与BlueXP分类兼容：

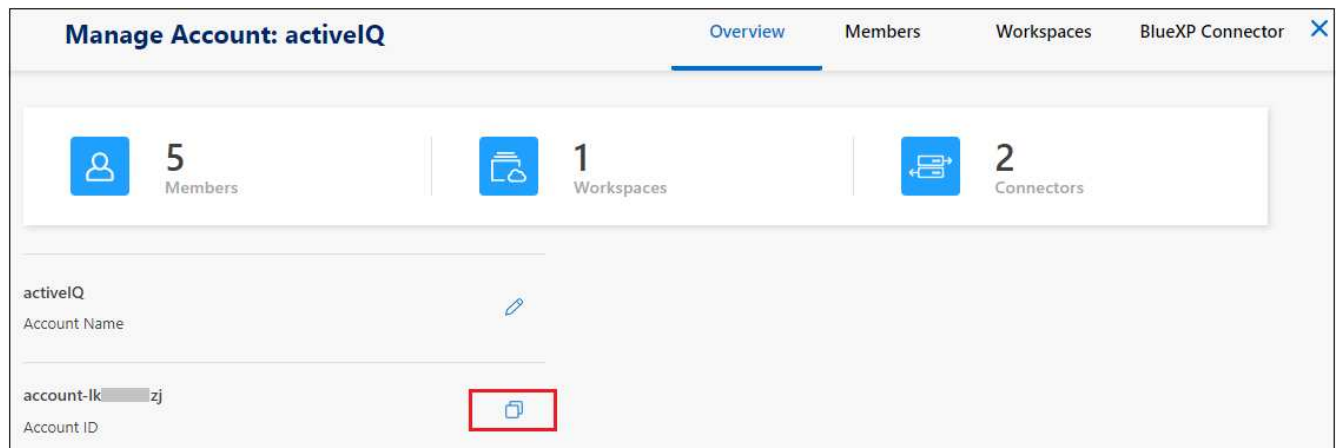
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

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

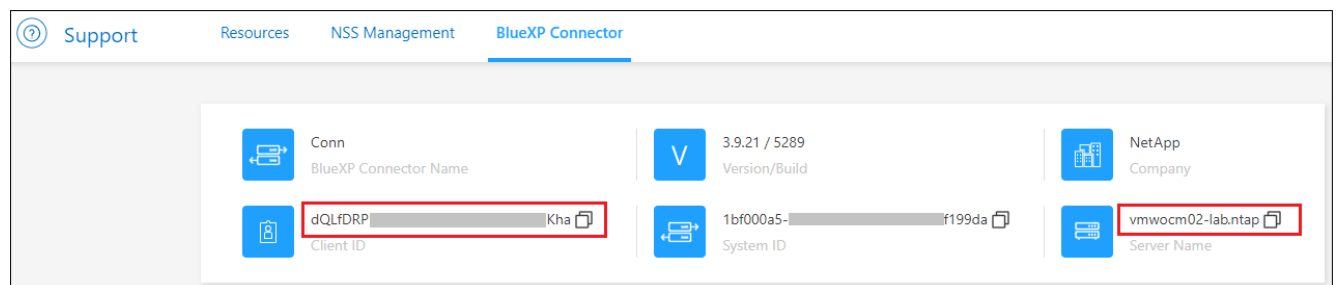
前提条件步骤

按照以下步骤获取添加扫描程序节点所需的NetApp帐户ID、连接器客户端ID、连接器服务器名称和用户访问令牌。

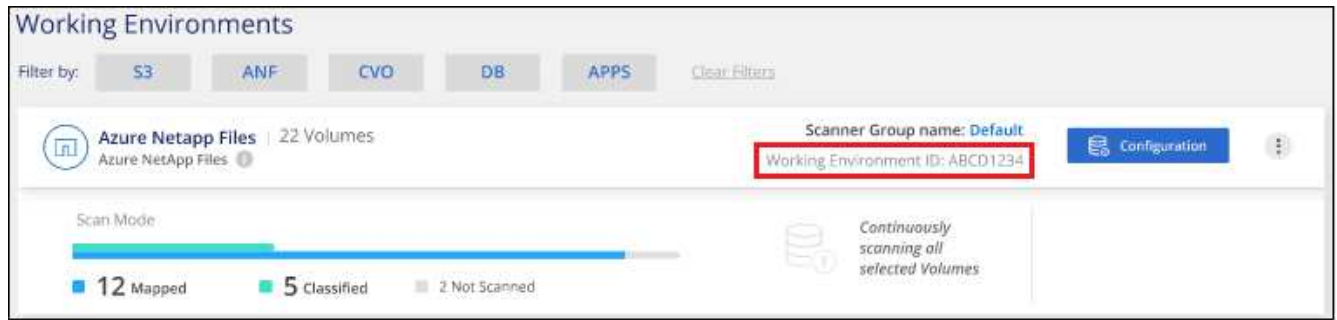
1. 从BlueXP菜单栏中、单击*帐户>管理帐户*。



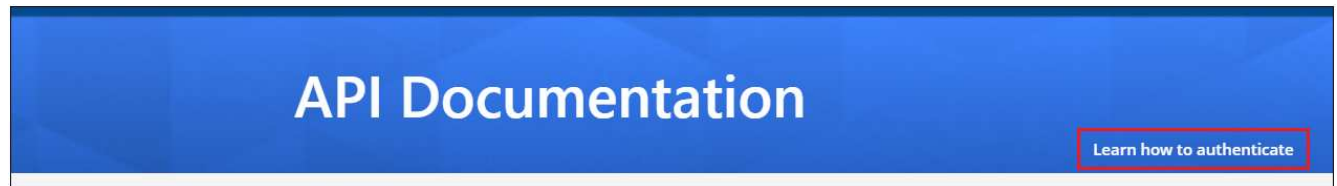
2. 复制_Account ID_。
3. 在BlueXP菜单栏中、单击*帮助>支持> BlueXP连接器*。



4. 复制connector *Client ID*_和_*Server Name*。
5. 如果您计划使用扫描程序组、请从"BlueXP分类配置"选项卡中、复制您计划添加到扫描程序组的每个工作环境的工作环境ID。



6. 转至 "API文档开发人员中心" 然后单击*了解如何进行身份验证*。



7. 按照身份验证说明、在"username"和"password"参数中使用帐户管理员的用户名和密码。

8. 然后、从响应中复制_access token_。

步骤

1. 在BlueXP分类管理器节点上、运行脚本"add_saner_node.sh"。例如、此命令将添加2个扫描程序节点：

```
sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h
<ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
```

变量值：

- *account_id* = NetApp 帐户 ID
 - *_client_id* = 连接器客户端ID (将后缀"clients"添加到在前提条件步骤中复制的客户端ID)
 - *cm_host* = 连接器系统的IP地址或主机名
 - *ds_manager_IP* = BlueXP分类管理器节点系统的专用IP地址
 - *NODE_PRIVIGE_IP* = BlueXP分类扫描程序节点系统的IP地址(多个扫描程序节点IP以逗号分隔)
 - *user_token* = JWT用户访问令牌
2. 在add_scanner_node脚本完成之前、会显示一个对话框、其中显示了扫描程序节点所需的安装命令。复制命令(例如：`sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`)并将其保存在文本文件中。
3. 在 * 每个 * 扫描程序节点主机上：
- a. 将数据感知安装程序文件(* `datasENSE-installer-cp.tar.gz*<version>`)复制到主机(使用`scp`或其他方法)。
 - b. 解压缩安装程序文件。
 - c. 粘贴并执行步骤2中复制的命令。
 - d. 如果要将扫描程序节点添加到"扫描程序组"中、请将参数*`-r <scanner_group_name>`*添加到命令中。否则、扫描程序节点将添加到"默认"组。

在所有扫描程序节点上完成安装且这些节点已加入管理器节点后、"add_scanner_node.sh"脚本也会完成。安装可能需要10到20分钟。

4. 如果将任何扫描程序节点添加到扫描程序组中、请返回到管理器节点并执行以下2项任务：

- a. 打开文件"/opt/NetApp/config/custom_configuration/working_扫描程序_group_config.yml"并输入要扫描特定工作环境的扫描程序组的映射。您需要为每个数据源提供_Working Environment ID_。例如、以下条目会将2个工作环境添加到"欧洲"扫描程序组、并将2个添加到"美国"扫描程序组：

```
scanner_groups:
  europe:
    working_environments:
      - "working_environment_id1"
      - "working_environment_id2"
  united_states:
    working_environments:
      - "working_environment_id3"
      - "working_environment_id4"
```

未添加到列表中的任何工作环境均由"default"组进行扫描-您必须在"default"组中至少有一个管理器或扫描程序节点。

- b. 运行以下脚本、将此映射信息注册到所有扫描程序节点：

```
/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh
```

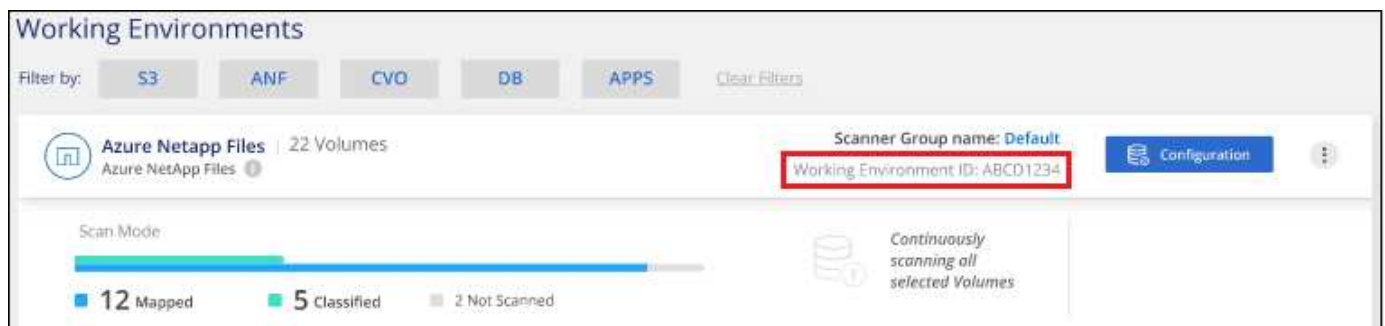
结果

BlueXP分类可通过管理器和扫描程序节点进行设置、以扫描所有数据源。

下一步行动

如果尚未扫描、您可以从配置页面中选择要扫描的数据源。如果创建了扫描程序组、则每个数据源都会由相应组中的扫描程序节点进行扫描。

您可以在配置页面中查看每个工作环境的扫描程序组名称。



The screenshot displays the 'Working Environments' configuration interface. At the top, there are filter buttons for 'S3', 'ANF', 'CVO', 'DB', and 'APPs', along with a 'Clear Filters' option. Below the filters, the main content area shows 'Azure Netapp Files | 22 Volumes'. A 'Scanner Group name: Default' is indicated, and a red box highlights the 'Working Environment ID: ABCD1234' field. A 'Configuration' button is visible to the right. At the bottom, the 'Scan Mode' section shows a progress bar and a status of 'Continuously scanning all selected Volumes'. The progress bar indicates 12 Mapped, 5 Classified, and 2 Not Scanned volumes.

您还可以在配置页面底部查看所有扫描程序组的列表以及组中每个扫描程序节点的IP地址和状态。

Scanner Groups

Scanner Group: Default

Scanner nodes

2 Scanner nodes

Scanner node host name	IP	Last active time	Status	Error
ip-172-████████.us-west-2.compute	172-████████	23/09/2022 14:32	Active	
ip-172-████████.us-west-2.compute	172-████████	23/09/2022 14:32	Active	

Scanner Group: United_States

Scanner nodes

2 Scanner nodes

Scanner node host name	IP	Last active time	Status	Error
ip-172-████████.us-west-2.compute	172-████████	23/09/2022 14:32	Active	
ip-172-████████.us-west-2.compute	172-████████	23/09/2022 14:32	Active	

Scanner Group: Europe

Scanner nodes

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。