



激活对数据源的扫描 Cloud Data Sense

NetApp
July 19, 2022

目录

- 激活对数据源的扫描 1
 - 开始使用适用于 Cloud Volumes ONTAP 和内部 ONTAP 的云数据感知 1
 - 开始使用适用于 Azure NetApp Files 的云数据感知 6
 - 开始使用适用于 Amazon FSX for ONTAP 的 Cloud Data sense 9
 - Amazon S3 云数据感知入门 14
 - 正在扫描数据库架构 20
 - 正在扫描 OneDrive 帐户 24
 - 扫描 SharePoint 帐户 27
 - 扫描Google Drive帐户 31
 - 正在扫描文件共享 33
 - 扫描使用 S3 协议的对象存储 36

激活对数据源的扫描

开始使用适用于 **Cloud Volumes ONTAP** 和内部 **ONTAP** 的云数据感知

完成几个步骤，开始使用 Cloud Data sense 扫描 Cloud Volumes ONTAP 和内部 ONTAP 卷。

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。

在扫描卷之前，必须在 Cloud Manager 中将系统添加为工作环境：

- 对于 Cloud Volumes ONTAP 系统，这些工作环境应已在 Cloud Manager 中可用
- 对于内部 ONTAP 系统，"[Cloud Manager 必须发现 ONTAP 集群](#)"

"[部署 Cloud Data sense](#)" 如果尚未部署实例。

单击 * 数据感知 *，选择 * 配置 * 选项卡，然后为特定工作环境中的卷激活合规性扫描。

启用 Cloud Data sense 后，请确保它可以访问所有卷。

- 云数据感知实例需要与每个 Cloud Volumes ONTAP 子网或内部 ONTAP 系统建立网络连接。
- Cloud Volumes ONTAP 的安全组必须允许来自数据感知实例的入站连接。
- 确保这些端口对 Data sense 实例开放：
 - 对于 NFS — 端口 111 和 2049。
 - 对于 CIFS — 端口 139 和 445。
- NFS 卷导出策略必须允许从 Data sense 实例进行访问。
- Data sense 需要 Active Directory 凭据才能扫描 CIFS 卷。

单击 * 合规性 * > * 配置 * > * 编辑 CIFS 凭据 * 并提供凭据。

选择或取消选择要扫描的卷，Cloud Data sense 将开始或停止扫描这些卷。

发现要扫描的数据源

如果您要扫描的数据源尚未位于 Cloud Manager 环境中，则可以此时将其添加到画布中。

您的 Cloud Volumes ONTAP 系统应已在 Cloud Manager 的 "画布" 中可用。对于内部部署的 ONTAP 系统，您需要拥有 "[Cloud Manager 将发现这些集群](#)"。

部署 **Cloud Data sense** 实例

如果尚未部署实例，请部署 Cloud Data sense。

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 Cloud Data sense"](#) 或 ["位于可访问 Internet 的内部位置"](#)。

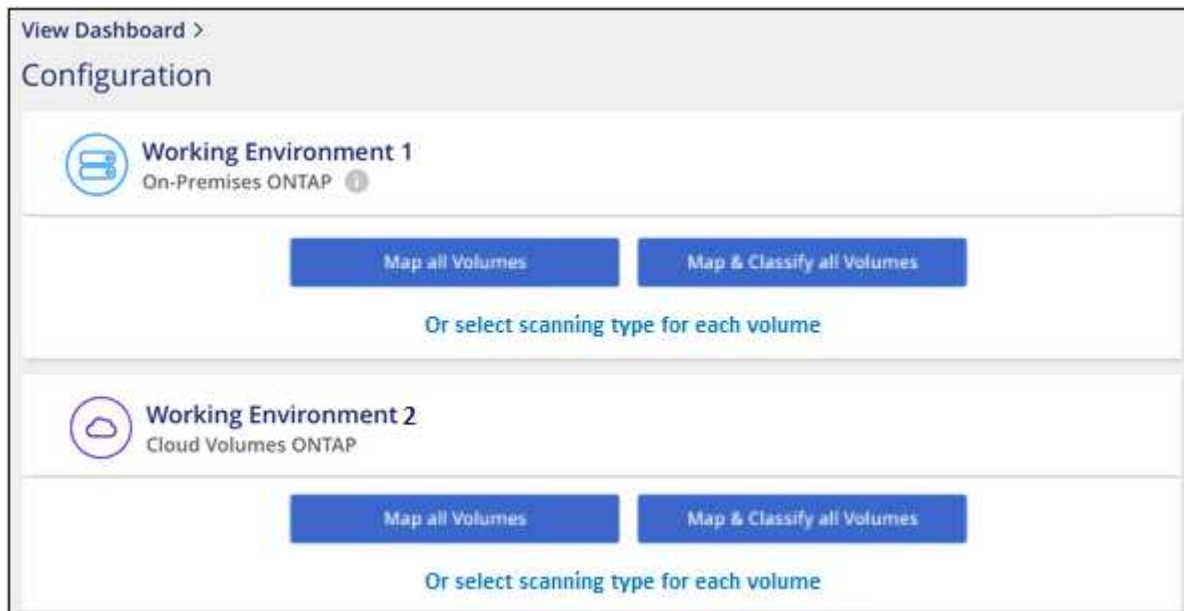
如果要扫描安装在无法访问 Internet 的非公开站点上的内部 ONTAP 系统，则需要执行以下操作 ["在无法访问 Internet 的同一内部位置部署 Cloud Data sense"](#)。这还要求 Cloud Manager Connector 部署在同一内部位置。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

在您的工作环境中实现云数据感知

您可以在任何受支持的云提供商的 Cloud Volumes ONTAP 系统和内部 ONTAP 集群上启用云数据感知。

1. 从 Cloud Manager 左侧导航菜单中、单击*数据感知*、然后选择*配置*选项卡。



2. 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。

请参见 [在卷上启用和禁用合规性扫描](#) 了解详细信息。

3. 在确认对话框中，单击 * 批准 * 以使 Data sense 开始扫描卷。

Cloud Data sense 开始扫描您在工作环境中选择的卷。一旦 Cloud Data sense 完成初始扫描，"合规性"信息板将显示结果。所需时间取决于数据量—可能需要几分钟或几小时。

验证 Cloud Data sense 是否有权访问卷

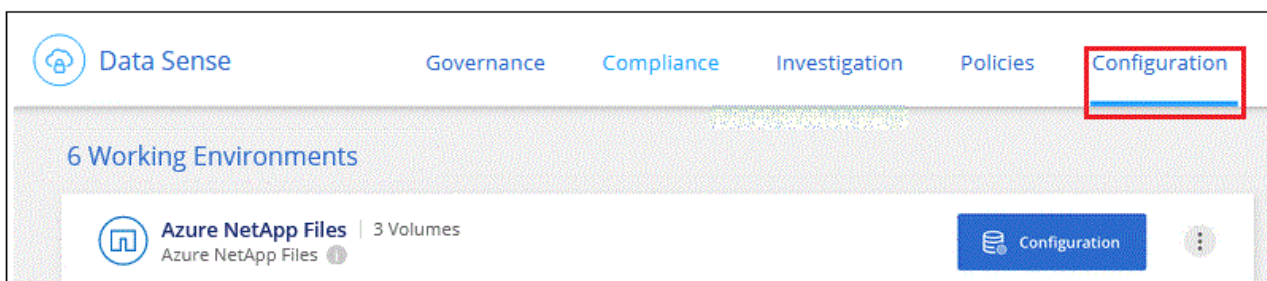
通过检查网络，安全组和导出策略，确保 Cloud Data sense 可以访问卷。您需要为 Data sense 提供 CIFS 凭据，以便它可以访问 CIFS 卷。

步骤

1. 确保云数据感知实例与包含 Cloud Volumes ONTAP 或内部 ONTAP 集群卷的每个网络之间存在网络连接。
2. 确保 Cloud Volumes ONTAP 的安全组允许来自数据感知实例的入站流量。

您可以从 Data sense 实例的 IP 地址打开流量安全组，也可以从虚拟网络内部打开所有流量的安全组。

3. 确保以下端口对 Data sense 实例开放：
 - 对于 NFS —端口 111 和 2049。
 - 对于 CIFS —端口 139 和 445。
4. 确保 NFS 卷导出策略包含 Data sense 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，请为 Data sense 提供 Active Directory 凭据，以便它可以扫描 CIFS 卷。
 - a. 在 Cloud Manager 顶部，单击 * 数据感知 *。
 - b. 单击 * 配置 * 选项卡。

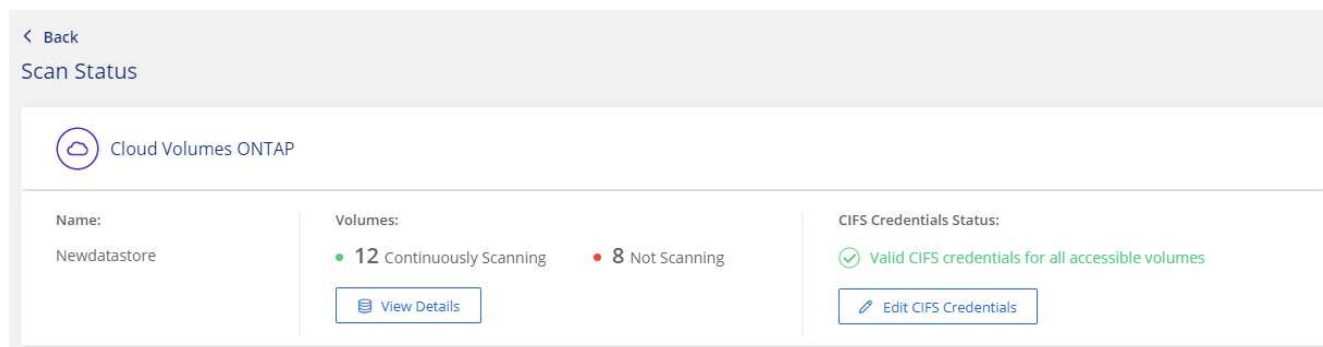


- c. 对于每个工作环境，单击 * 编辑 CIFS 凭据 *，然后输入 Data sense 访问系统上 CIFS 卷所需的用户名和密码。

这些凭据可以是只读的，但提供管理员凭据可确保 Data sense 可以读取任何需要提升权限的数据。这些凭据存储在 Cloud Data sense 实例上。

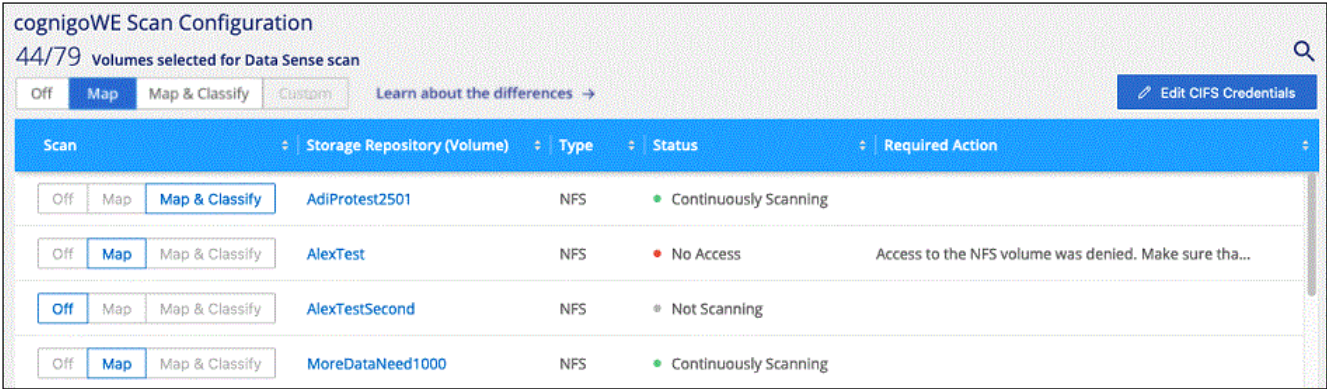
如果要确保数据感知分类扫描不会更改文件的“上次访问时间”、我们建议用户具有“写入属性”权限。如果可能、我们建议将Active Directory配置的用户设置为组织中有权访问所有文件的父组的一部分。

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。



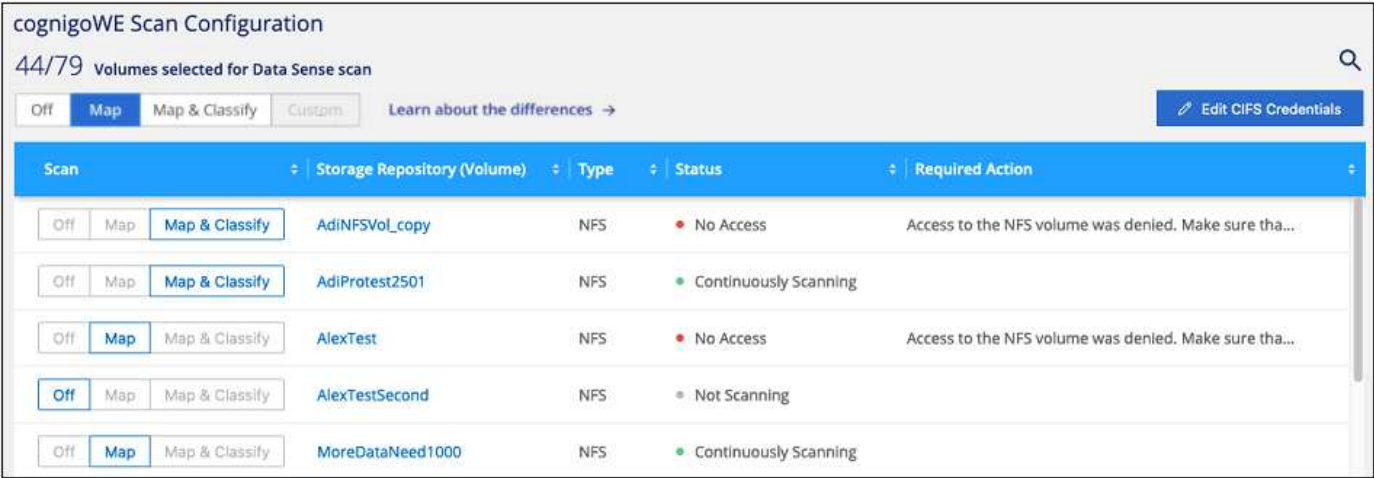
6. 在 *Configuration* 页面上，单击 * 查看详细信息 * 以查看每个 CIFS 和 NFS 卷的状态并更正任何错误。

例如，下图显示了四个卷；其中一个卷由于 Data sense 实例与卷之间的网络连接问题而无法扫描。



在卷上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。



收件人：	执行以下操作：
在卷上启用仅映射扫描	在卷区域中，单击 * 映射 *
对卷启用完全扫描	在卷区域中，单击 * 映射和分类 *
禁用对卷的扫描	在卷区域中，单击 * 关闭 *
在所有卷上启用仅映射扫描	在标题区域中，单击 * 映射 *
对所有卷启用完全扫描	在标题区域中，单击 * 映射和分类 *
禁用对所有卷的扫描	在标题区域中，单击 * 关闭 *



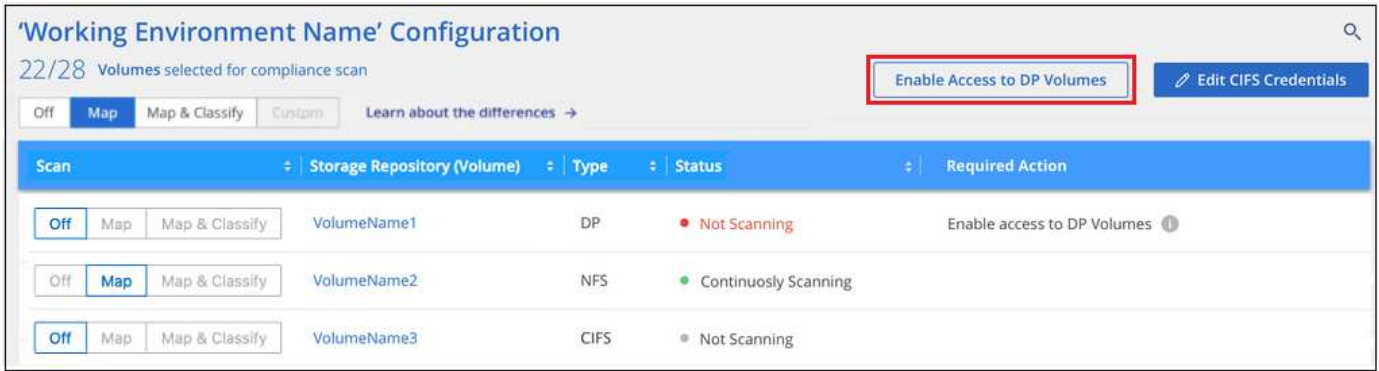
只有在标题区域中设置了 * 映射 * 或 * 映射和分类 * 设置后，才会自动扫描添加到工作环境中的新卷。如果在标题区域中设置为 * 自定义 * 或 * 关闭 *，则需要在工作环境中添加的每个新卷上激活映射和 / 或完全扫描。

扫描数据保护卷

默认情况下，不会扫描数据保护（DP）卷，因为它们不会公开在外部，并且 Cloud Data sense 无法访问它

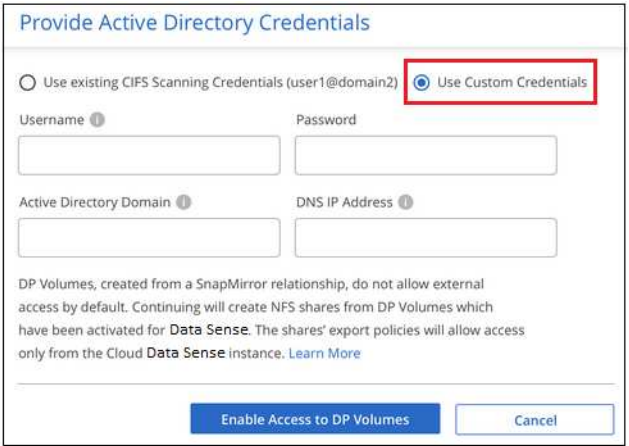
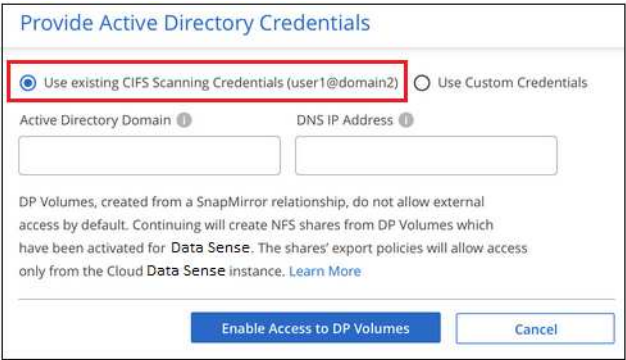
们。这些卷是从内部 ONTAP 系统或 Cloud Volumes ONTAP 系统执行 SnapMirror 操作的目标卷。

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* 。



如果要扫描这些数据保护卷：

1. 单击页面顶部的 * 启用对 DP 卷的访问 * 。
2. 查看确认消息，然后再次单击 * 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 Cloud Data sense 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。



3. 激活要扫描的每个 DP 卷 与启用其他卷的方式相同。

启用后， Cloud Data sense 会从已激活进行扫描的每个 DP 卷创建一个 NFS 共享。共享导出策略仅允许从 Data sense 实例进行访问。

- 注意： * 如果在最初启用对 DP 卷的访问时没有 CIFS 数据保护卷，稍后再添加一些，则配置页面顶部会显示 * 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 凭据仅在第一个 CIFS DP 卷的 Storage VM 中注册，因此将扫描该 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。

开始使用适用于 **Azure NetApp Files** 的云数据感知

完成几个步骤，开始使用适用于 Azure NetApp Files 的云数据感知。

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。

扫描 Azure NetApp Files 卷之前，"[必须设置 Cloud Manager 才能发现配置](#)"。

"[在 Cloud Manager 中部署 Cloud Data sense](#)" 如果尚未部署实例。

单击 * 合规性 *，选择 * 配置 * 选项卡，然后为特定工作环境中的卷激活合规性扫描。

启用 Cloud Data sense 后，请确保它可以访问所有卷。

- 云数据感知实例需要与每个 Azure NetApp Files 子网建立网络连接。
- 确保这些端口对 Data sense 实例开放：
 - 对于 NFS — 端口 111 和 2049。
 - 对于 CIFS — 端口 139 和 445。
- NFS 卷导出策略必须允许从 Data sense 实例进行访问。
- Data sense 需要 Active Directory 凭据才能扫描 CIFS 卷。

单击 * 合规性 * > * 配置 * > * 编辑 CIFS 凭据 * 并提供凭据。

选择或取消选择要扫描的卷，Cloud Data sense 将开始或停止扫描这些卷。

正在发现要扫描的 **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 Cloud Manager 中，您可以此时将其添加到画布中。

"[了解如何在 Cloud Manager 中发现 Azure NetApp Files 系统](#)"。

部署 **Cloud Data sense** 实例

"[部署 Cloud Data sense](#)" 如果尚未部署实例。

扫描 Azure NetApp Files 卷时，必须在云中部署数据感知，并且数据感知必须与要扫描的卷部署在同一区域。

- 注意：* 扫描 Azure NetApp Files 卷时，当前不支持在内部位置部署云数据感知。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

在您的工作环境中实现云数据感知

您可以在 Azure NetApp Files 卷上启用云数据感知。

1. 从Cloud Manager左侧导航菜单中、单击*数据感知*、然后选择*配置*选项卡。



2. 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。

请参见 [在卷上启用和禁用合规性扫描](#) 了解详细信息。

3. 在确认对话框中，单击 * 批准 * 以使 Data sense 开始扫描卷。

Cloud Data sense 开始扫描您在工作环境中选择的卷。一旦 Cloud Data sense 完成初始扫描，" 合规性 " 信息板将显示结果。所需时间取决于数据量—可能需要几分钟或几小时。

验证 **Cloud Data sense** 是否有权访问卷

通过检查网络，安全组和导出策略，确保 Cloud Data sense 可以访问卷。您需要为 Data sense 提供 CIFS 凭据，以便它可以访问 CIFS 卷。

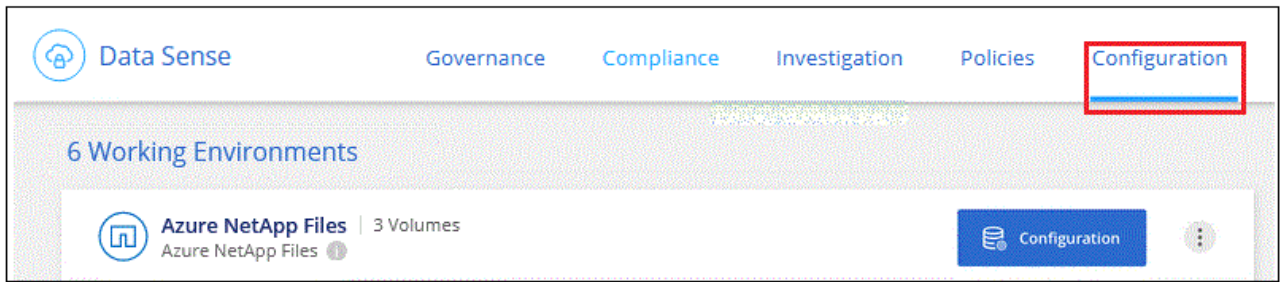
步骤

1. 确保云数据感知实例与包含 Azure NetApp Files 卷的每个网络之间存在网络连接。



对于 Azure NetApp Files，Cloud Data sense 只能扫描与 Cloud Manager 位于同一区域的卷。

2. 确保以下端口对 Data sense 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 Data sense 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，请为 Data sense 提供 Active Directory 凭据，以便它可以扫描 CIFS 卷。
 - a. 在 Cloud Manager 顶部，单击 * 数据感知 *。
 - b. 单击 * 配置 * 选项卡。

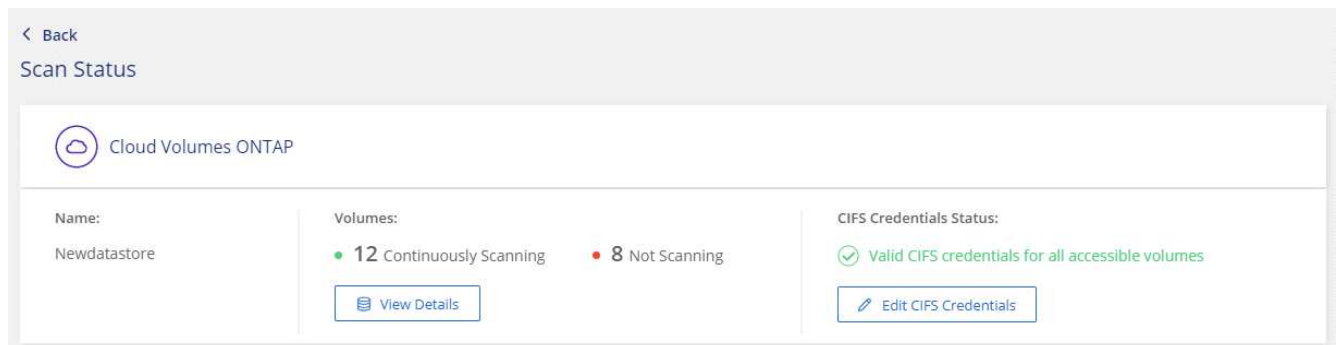


- c. 对于每个工作环境，单击 * 编辑 CIFS 凭据 *，然后输入 Data sense 访问系统上 CIFS 卷所需的用户名和密码。

这些凭据可以是只读的，但提供管理员凭据可确保 Data sense 可以读取任何需要提升权限的数据。这些凭据存储在 Cloud Data sense 实例上。

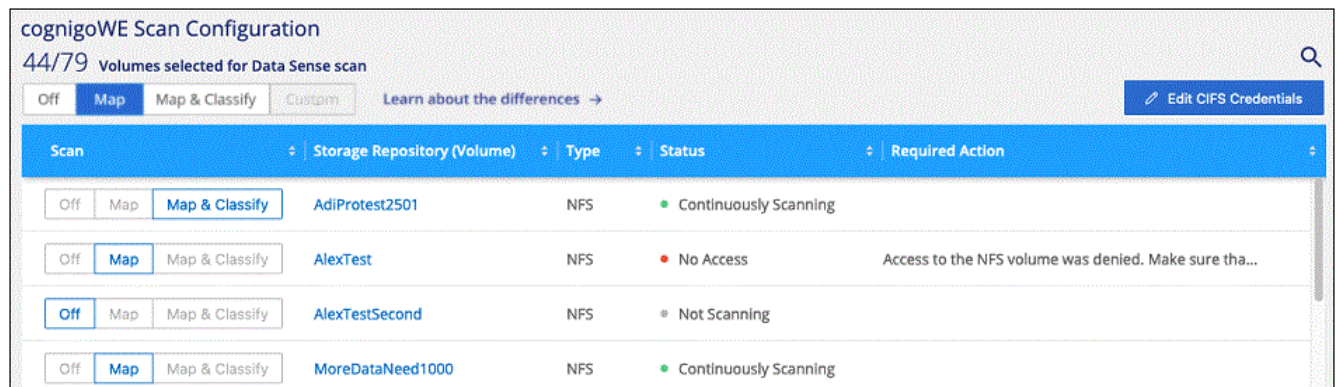
如果要确保数据感知分类扫描不会更改文件的"上次访问时间"、我们建议用户具有"写入属性"权限。如果可能、我们建议将Active Directory配置的用户设置为组织中有权访问所有文件的父组的一部分。

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。



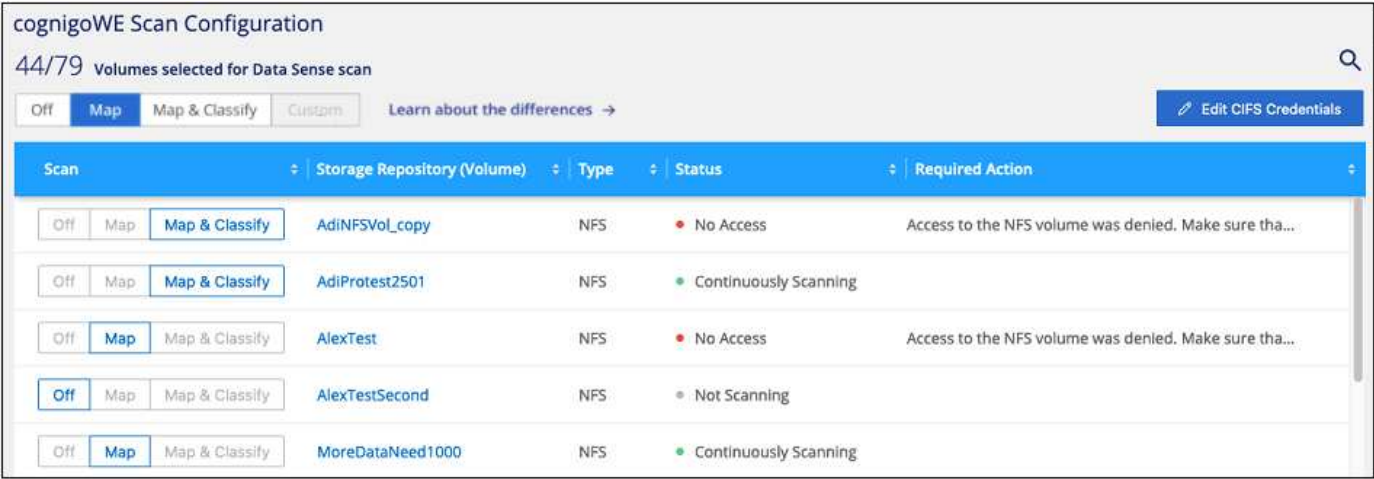
5. 在 *Configuration* 页面上，单击 * 查看详细信息 * 以查看每个 CIFS 和 NFS 卷的状态并更正任何错误。

例如，下图显示了四个卷；其中一个卷由于 Data sense 实例与卷之间的网络连接问题而无法扫描。



在卷上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。



收件人：	执行以下操作：
在卷上启用仅映射扫描	在卷区域中，单击 * 映射 *
对卷启用完全扫描	在卷区域中，单击 * 映射和分类 *
禁用对卷的扫描	在卷区域中，单击 * 关闭 *
在所有卷上启用仅映射扫描	在标题区域中，单击 * 映射 *
对所有卷启用完全扫描	在标题区域中，单击 * 映射和分类 *
禁用对所有卷的扫描	在标题区域中，单击 * 关闭 *



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。

开始使用适用于 Amazon FSX for ONTAP 的 Cloud Data sense

请完成几个步骤，开始使用 Cloud Data sense 扫描 Amazon FSX for ONTAP 卷。

开始之前

- 您需要在 AWS 中使用主动连接器来部署和管理 Data sense。
- 您在创建工作环境时选择的安全组必须允许来自云数据感知实例的流量。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）"](#)

快速入门

按照以下步骤快速入门，或者向下滚动以查看完整详细信息。

在扫描 ONTAP 卷的 FSX 之前，["您必须具有配置了卷的 FSX 工作环境"](#)。

["在 Cloud Manager 中部署 Cloud Data sense"](#) 如果尚未部署实例。

单击 * 数据感知 *，选择 * 配置 * 选项卡，然后为特定工作环境中的卷激活合规性扫描。

启用 Cloud Data sense 后，请确保它可以访问所有卷。

- 云数据感知实例需要与 ONTAP 子网的每个 FSX 建立网络连接。
- 确保以下端口已对 Data sense 实例开放。
 - 对于 NFS — 端口 111 和 2049。
 - 对于 CIFS — 端口 139 和 445。
- NFS 卷导出策略必须允许从 Data sense 实例进行访问。
- Data sense 需要 Active Directory 凭据才能扫描 CIFS 卷。+ 单击 * 合规性 * > * 配置 * > * 编辑 CIFS 凭据 * 并提供凭据。

选择或取消选择要扫描的卷，Cloud Data sense 将开始或停止扫描这些卷。

正在发现要扫描的 **FSX for ONTAP** 文件系统

如果您要扫描的适用于 ONTAP 的 FSX 文件系统尚未作为工作环境在 Cloud Manager 中，则可以此时将其添加到画布中。

["了解如何在 Cloud Manager 中发现或创建适用于 ONTAP 的 FSX 文件系统"](#)。

部署 **Cloud Data sense** 实例

["部署 Cloud Data sense"](#) 如果尚未部署实例。

您应将 Data sense 部署在与 Connector for AWS 和要扫描的 FSX 卷相同的 AWS 网络中。

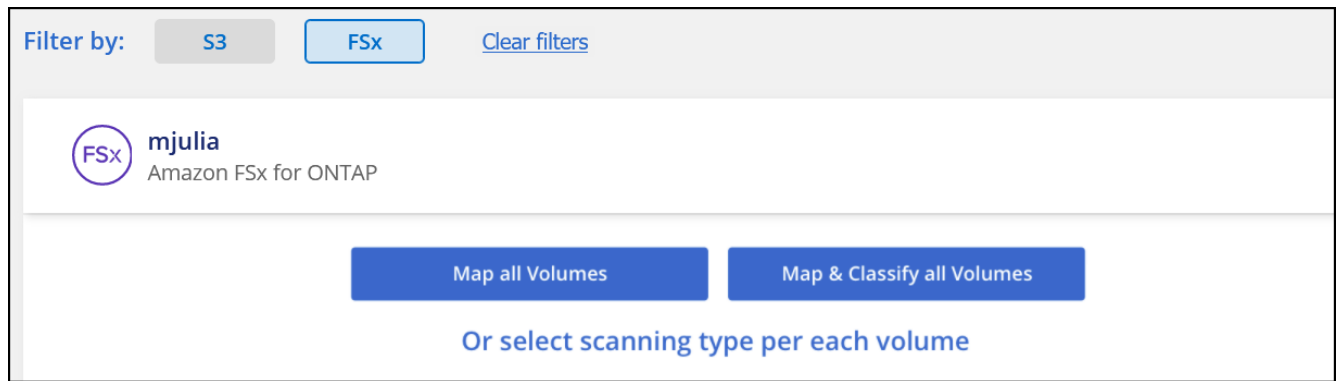
- 注意：* 扫描 FSX 卷时，当前不支持在内部位置部署 Cloud Data sense。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

在您的工作环境中实现云数据感知

您可以为 ONTAP 卷的 FSX 启用云数据感知。

1. 从 Cloud Manager 左侧导航菜单中、单击 * 数据感知 *、然后选择 * 配置 * 选项卡。



2. 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。

请参见 [在卷上启用和禁用合规性扫描](#) 了解详细信息。

3. 在确认对话框中，单击 * 批准 * 以使 Data sense 开始扫描卷。

Cloud Data sense 开始扫描您在工作环境中选择的卷。一旦 Cloud Data sense 完成初始扫描，" 合规性 " 信息板将显示结果。所需时间取决于数据量—可能需要几分钟或几小时。

验证 Cloud Data sense 是否有权访问卷

通过检查网络，安全组和导出策略，确保 Cloud Data sense 可以访问卷。

您需要为 Data sense 提供 CIFS 凭据，以便它可以访问 CIFS 卷。

步骤

1. 在 *Configuration* 页面上，单击 * 查看详细信息 * 以查看状态并更正任何错误。

例如，下图显示了由于 Data sense 实例与卷之间的网络连接问题，卷 Cloud Data sense 无法扫描。

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...

2. 确保云数据感知实例与包含适用于 ONTAP 的 FSX 卷的每个网络之间存在网络连接。



对于适用于 ONTAP 的 FSX，Cloud Data sense 只能扫描与 Cloud Manager 位于同一区域的卷。

3. 确保以下端口对 Data sense 实例开放：

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

4. 确保 NFS 卷导出策略包含 Data sense 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 ， 请为 Data sense 提供 Active Directory 凭据，以便它可以扫描 CIFS 卷。
- a. 在 Cloud Manager 顶部，单击 * 数据感知 * 。
 - b. 单击 * 配置 * 选项卡。
 - c. 对于每个工作环境，单击 * 编辑 CIFS 凭据 * ，然后输入 Data sense 访问系统上 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 Data sense 可以读取任何需要提升权限的数据。这些凭据存储在 Cloud Data sense 实例上。

如果要确保数据感知分类扫描不会更改文件的"上次访问时间"、我们建议用户具有"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。

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。

在卷上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。

cognigoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

OffMapMap & ClassifyCustom

Learn about the differences →

Edit CIFS Credentials

Scan	Storage Repository (Volume)	Type	Status	Required Action
<div>OffMapMap & Classify</div>	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap & Classify</div>	AdiProtest2501	NFS	Continuously Scanning	
<div>OffMapMap & Classify</div>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap & Classify</div>	AlexTestSecond	NFS	Not Scanning	
<div>OffMapMap & Classify</div>	MoreDataNeed1000	NFS	Continuously Scanning	

收件人：	执行以下操作：
在卷上启用仅映射扫描	在卷区域中，单击 * 映射 *
对卷启用完全扫描	在卷区域中，单击 * 映射和分类 *
禁用对卷的扫描	在卷区域中，单击 * 关闭 *
在所有卷上启用仅映射扫描	在标题区域中，单击 * 映射 *
对所有卷启用完全扫描	在标题区域中，单击 * 映射和分类 *
禁用对所有卷的扫描	在标题区域中，单击 * 关闭 *

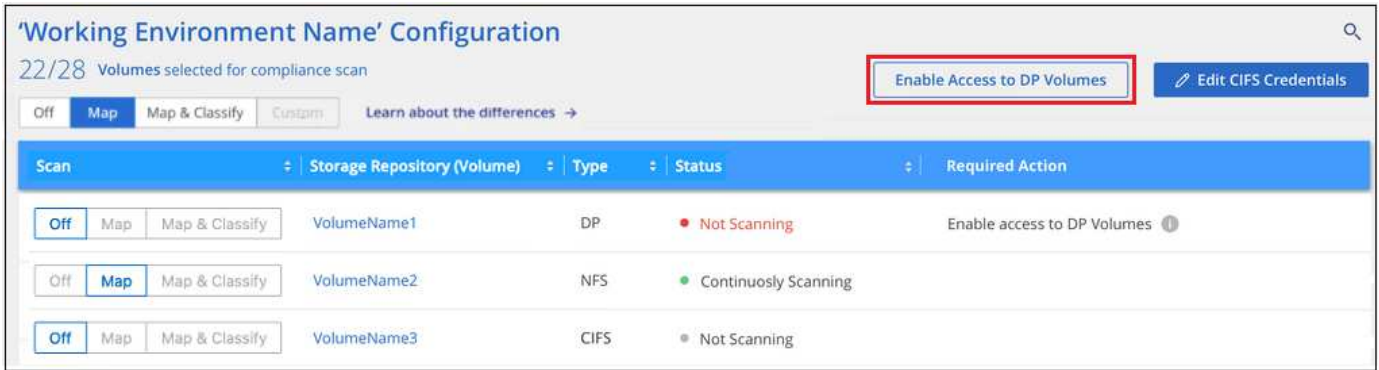


只有在标题区域中设置了 * 映射 * 或 * 映射和分类 * 设置后，才会自动扫描添加到工作环境中的新卷。如果在标题区域中设置为 * 自定义 * 或 * 关闭 * ，则需要在工作环境中添加的每个新卷上激活映射和 / 或完全扫描。

扫描数据保护卷

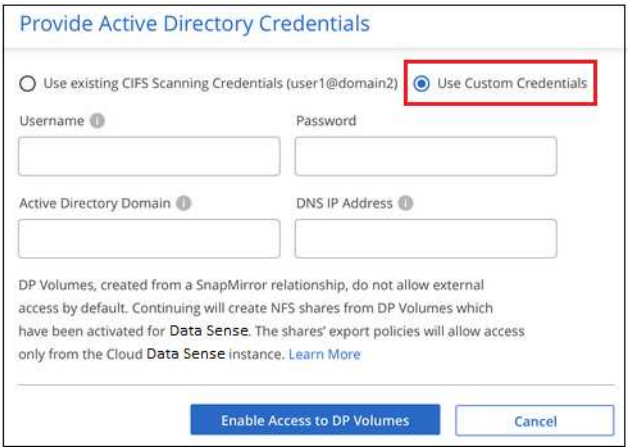
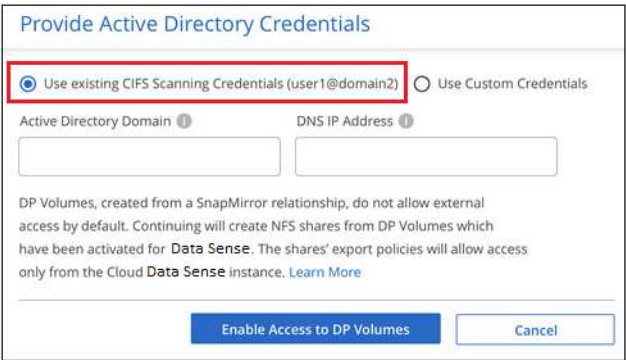
默认情况下，不会扫描数据保护（DP）卷，因为它们不会公开在外部，并且 Cloud Data sense 无法访问它们。这些卷是从适用于 ONTAP 的 FSX 文件系统执行 SnapMirror 操作的目标卷。

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* 。



如果要扫描这些数据保护卷：

1. 单击页面顶部的 * 启用对 DP 卷的访问 * 。
2. 查看确认消息，然后再次单击 * 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 Cloud Data sense 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。



3. 激活要扫描的每个 DP 卷 与启用其他卷的方式相同。

启用后， Cloud Data sense 会从已激活进行扫描的每个 DP 卷创建一个 NFS 共享。共享导出策略仅允许从 Data sense 实例进行访问。

- 注意： * 如果在最初启用对 DP 卷的访问时没有 CIFS 数据保护卷，稍后再添加一些，则配置页面顶部会显示 * 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 凭据仅在第一个 CIFS DP 卷的 Storage VM 中注册，因此将扫描该 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。

Amazon S3 云数据感知入门

Cloud Data sense 可以扫描 Amazon S3 存储分段，以确定 S3 对象存储中的个人和敏感数据。Cloud Data sense 可以扫描帐户中的任何存储分段，而不管它是否是为 NetApp 解决方案创建的。

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。

确保您的云环境能够满足 Cloud Data sense 的要求，包括准备 IAM 角色以及设置从 Data sense 到 S3 的连接。 [请参见完整列表](#)。

"部署 Cloud Data sense" 如果尚未部署实例。

选择 Amazon S3 工作环境，单击 * 启用 *，然后选择包含所需权限的 IAM 角色。

选择要扫描的存储分段，Cloud Data sense 将开始扫描这些存储分段。

查看 S3 前提条件

以下要求特定于扫描 S3 存储分段。

为云数据感知实例设置 IAM 角色

Cloud Data sense 需要获得连接到您帐户中的 S3 存储分段并对其进行扫描的权限。设置一个包含以下权限的 IAM 角色。在 Amazon S3 工作环境中启用 Data sense 时，Cloud Manager 会提示您选择 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

提供从 **Cloud Data sense** 到 **Amazon S3** 的连接

Cloud Data sense 需要连接到 Amazon S3。提供此连接的最佳方式是通过 VPC 端点连接到 S3 服务。有关说明，请参见 ["AWS 文档：创建网关端点"](#)。

创建 VPC 端点时，请务必选择与云数据感知实例对应的区域，VPC 和路由表。您还必须修改安全组才能添加出站 HTTPS 规则、该规则允许通信到 S3 端点。否则，Data sense 将无法连接到 S3 服务。

如果遇到任何问题，请参见 ["AWS 支持知识中心：为什么我无法使用网关 VPC 端点连接到 S3 存储分段？"](#)

另一种方法是使用 NAT 网关提供连接。



您无法使用代理通过 Internet 访问 S3。

部署 **Cloud Data sense** 实例

["在 Cloud Manager 中部署 Cloud Data sense"](#) 如果尚未部署实例。

您需要使用部署在 AWS 中的 Connector 部署此实例，以便 Cloud Manager 自动发现此 AWS 帐户中的 S3 存储分段并将其显示在 Amazon S3 工作环境中。

- 注意：* 扫描 S3 存储分段时，当前不支持在内部位置部署 Cloud Data sense 。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

在 S3 工作环境中激活 Data sense

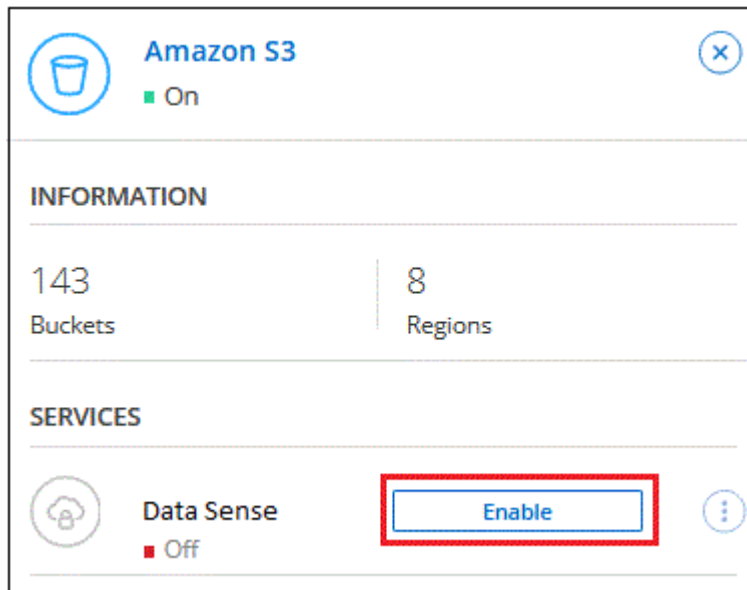
验证前提条件后，在 Amazon S3 上启用 Cloud Data sense 。

步骤

1. 从Cloud Manager左侧导航菜单中、单击*画布*。
2. 选择 Amazon S3 工作环境。



3. 在右侧的数据感知窗格中，单击 * 启用 * 。



4. 出现提示时，将 IAM 角色分配给具有的 Cloud Data sense 实例 [所需权限](#)。

Assign an AWS IAM Role for Cloud Data Sense

To enable **Cloud Data Sense** on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

occm

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so **Data Sense** can securely scan the data.

Alternatively, ensure that the **Data Sense** instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB


Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable

Cancel

5. 单击 * 启用 *。



您也可以通过单击在配置页面中为工作环境启用合规性扫描  按钮并选择 * 激活数据感知 *。

Cloud Manager 将 IAM 角色分配给实例。

在 S3 存储分段上启用和禁用合规性扫描

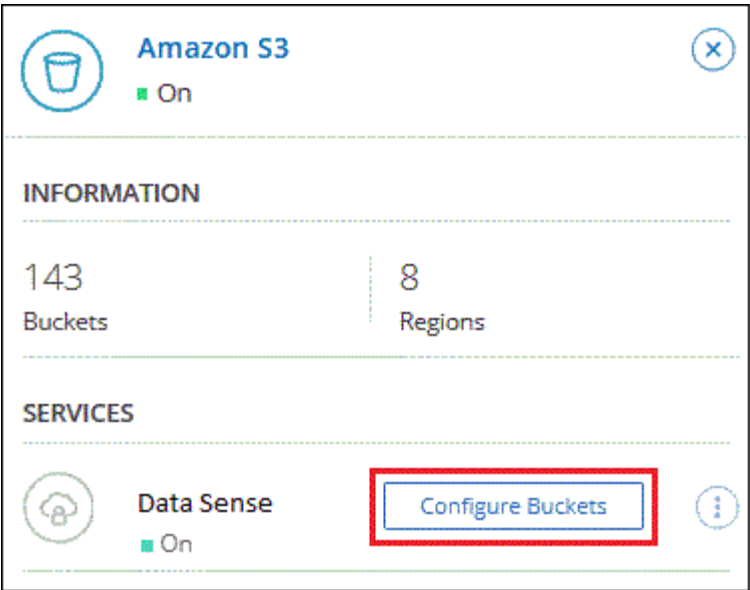
在 Cloud Manager 在 Amazon S3 上启用 Cloud Data sense 后，下一步是配置要扫描的分段。

如果 Cloud Manager 运行在包含要扫描的 S3 存储分段的 AWS 帐户中，则它会发现这些存储分段并将其显示在 Amazon S3 工作环境中。

云数据感知也可以 [扫描位于不同 AWS 帐户中的 S3 存储分段](#)。

步骤

1. 选择 Amazon S3 工作环境。
2. 在右侧窗格中，单击 * 配置分段 *。



3. 在存储分段上启用仅映射扫描或映射和分类扫描。

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
<div>OffMapMap & Classify</div>	BucketName1	● Not Scanning	Add Credentials
<div>OffMapMap & Classify</div>	BucketName2	● Continuously Scanning	
<div>OffMapMap & Classify</div>	BucketName3	● Not Scanning	

收件人：	执行以下操作：
在存储分段上启用仅映射扫描	单击 * 映射 *
对存储分段启用完全扫描	单击 * 映射和分类 *
禁用对存储分段的扫描	单击 * 关闭 *

Cloud Data sense 开始扫描您启用的 S3 存储分段。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。

从其他 AWS 帐户扫描存储分段

您可以通过从其他 AWS 帐户中分配角色来扫描此帐户下的 S3 存储分段，以访问现有 Cloud Data sense 实例。

步骤

1. 转到要扫描 S3 存储分段的目标 AWS 帐户，然后选择 * 其他 AWS 帐户 * 来创建 IAM 角色。

Create role





1

2

3

4


Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
 - ☐ Require MFA 

请务必执行以下操作：

- 输入 Cloud Data sense 实例所在帐户的 ID 。
- 将 * 最大 CLI/API 会话持续时间 * 从 1 小时更改为 12 小时，然后保存此更改。
- 附加云数据感知 IAM 策略。确保它具有所需的权限。

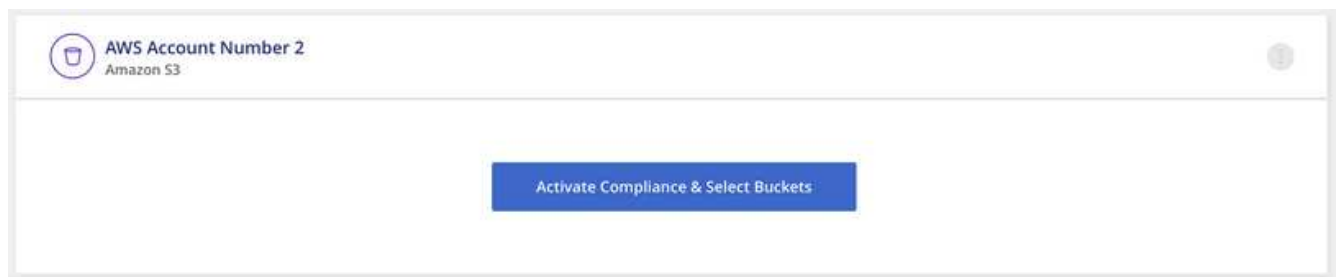
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

2. 转到 Data sense 实例所在的源 AWS 帐户，然后选择附加到该实例的 IAM 角色。
 - a. 将 * 最大 CLI/API 会话持续时间 * 从 1 小时更改为 12 小时，然后保存此更改。
 - b. 单击 * 附加策略 *，然后单击 * 创建策略 *。
 - c. 创建一个包含 "STS : AssumeRole" 操作的策略，并指定您在目标帐户中创建的角色 ARN 。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Cloud Data sense 实例配置文件帐户现在可以访问其他 AWS 帐户。

3. 转到 * Amazon S3 Configuration* 页面，此时将显示新的 AWS 帐户。请注意， Cloud Data sense 可能需要几分钟时间来同步新帐户的工作环境并显示此信息。



4. 单击 * 激活数据感知并选择分段 *，然后选择要扫描的分段。

Cloud Data sense 将开始扫描您启用的新 S3 存储分段。

正在扫描数据库架构

完成几个步骤，开始使用 Cloud Data sense 扫描数据库架构。

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。

确保您的数据库受支持，并且您具有连接到数据库所需的信息。

"部署 Cloud Data sense" 如果尚未部署实例。

添加要访问的数据库服务器。

选择要扫描的模式。

查看前提条件

在启用 Cloud Data sense 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

Cloud Data sense 可以从以下数据库扫描架构：

- 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。

数据库要求

可以扫描连接到云数据感知实例的任何数据库，而不管其托管在何处。要连接到数据库，您只需提供以下信息：

- IP 地址或主机名
- Port
- 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。建议您为 Cloud Data sense 系统创建一个具有所有所需权限的专用用户。

- 注： * 对于 MongoDB ，需要只读管理员角色。

部署 Cloud Data sense 实例

如果尚未部署实例，请部署 Cloud Data sense 。

如果要扫描可通过 Internet 访问的数据库架构，则可以 ["在云中部署 Cloud Data sense"](#) 或 ["在可访问 Internet 的内部位置部署 Data sense"](#)。

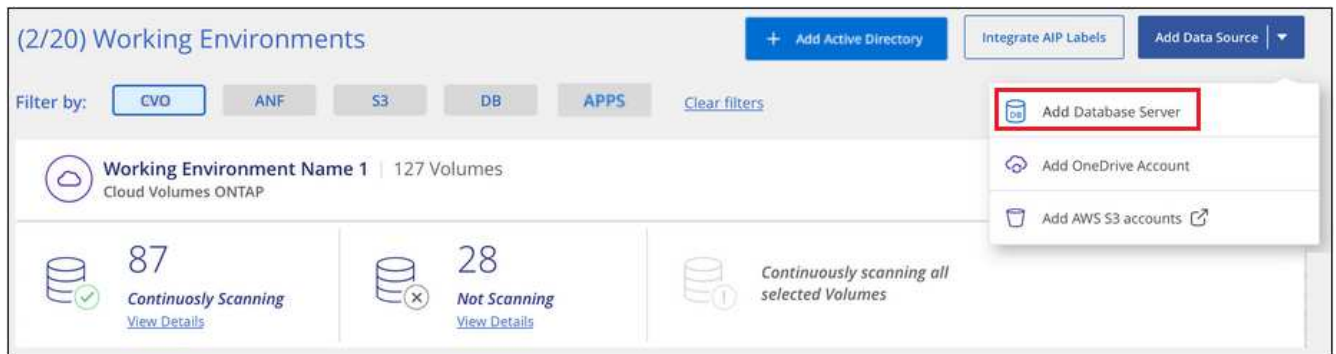
如果要扫描的数据库架构安装在无法访问 Internet 的非公开站点中，则需要执行 ["在无法访问 Internet 的同一内部位置部署 Cloud Data sense"](#)。这还要求 Cloud Manager Connector 部署在同一内部位置。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

正在添加数据库服务器

添加架构所在的数据库服务器。

1. 在工作环境配置页面中，单击 * 添加数据源 * > * 添加数据库服务器 *。



2. 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 Cloud Data sense 可以访问服务器。
 - e. 单击 * 添加数据库服务器 *。

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type	Host Name or IP Address
<input type="text"/>	<input type="text"/>
Port	Service Name
<input type="text"/>	<input type="text"/>

Credentials

Username	Password
<input type="text"/>	<input type="text"/>

Add DB ServerCancel

数据库将添加到工作环境列表中。

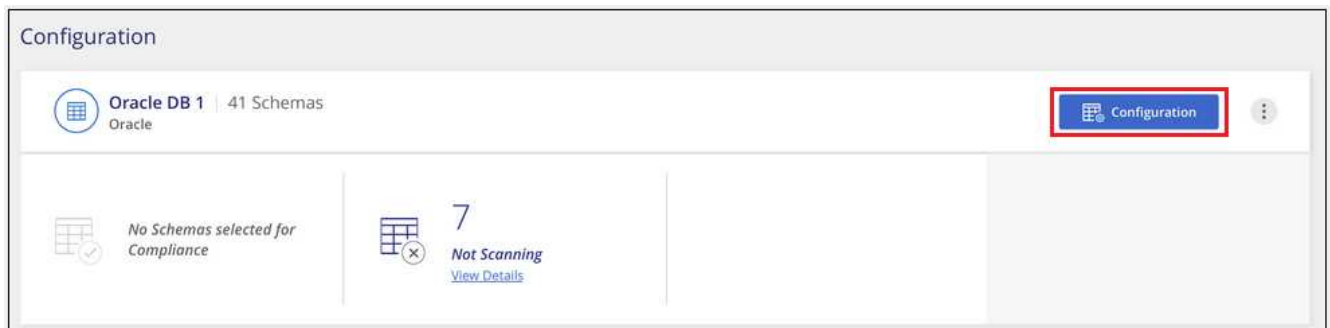
对数据库架构启用和禁用合规性扫描

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. 在 *Configuration* 页面中，单击要配置的数据库的 * 配置 * 按钮。



2. 向右移动滑块以选择要扫描的架构。

'Working Environment Name' Configuration			
28/28 Schemas selected for compliance scan		Edit Credentials	
Scan	Schema Name	Status	Required Action
<input type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

Cloud Data sense 将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。

正在扫描 OneDrive 帐户

完成几个步骤，使用 Cloud Data sense 扫描用户的 OneDrive 文件夹中的文件。

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。

确保您拥有登录到 OneDrive 帐户所需的管理员凭据。

"部署 Cloud Data sense" 如果尚未部署实例。

使用管理员用户凭据登录到要访问的 OneDrive 帐户，以便将其添加为新的工作环境。

从 OneDrive 帐户中添加要扫描的用户列表，然后选择扫描类型。一次最多可以添加 100 个用户。

查看 OneDrive 要求

在启用 Cloud Data sense 之前，请查看以下前提条件以确保您的配置受支持。

- 您必须具有 OneDrive for Business 帐户的管理员登录凭据、该帐户可提供对用户文件的读取访问权限。
- 您需要列出要扫描其 OneDrive 文件夹的所有用户的电子邮件地址、并以行分隔。

部署 Cloud Data sense 实例

如果尚未部署实例，请部署 Cloud Data sense。

数据感知可以是 "部署在云中" 或 "位于可访问 Internet 的内部位置"。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

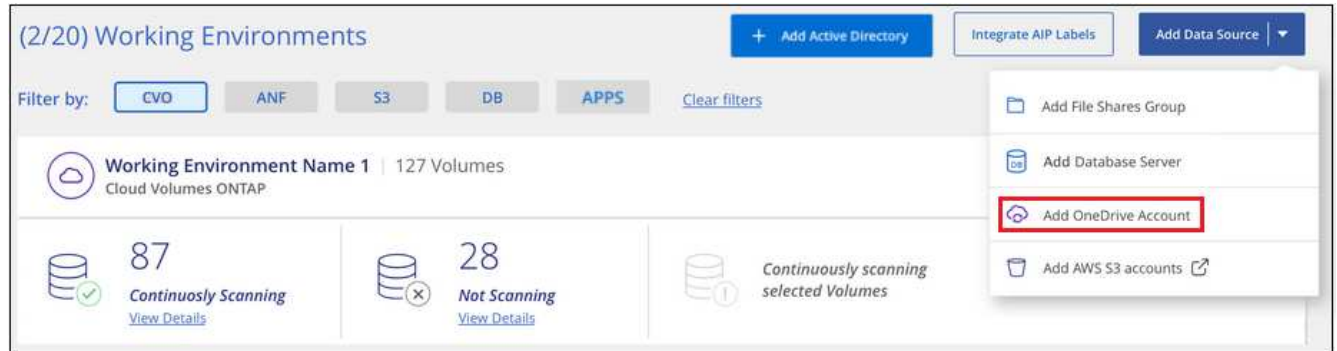
数据感知也可以是 "部署在无法访问 Internet 的内部位置"。但是，要扫描本地 OneDrive 文件，您需要为一些选定端点提供 Internet 访问。"请在此处查看所需端点的列表"。

正在添加 OneDrive 帐户

添加用户文件所在的 OneDrive 帐户。

步骤

1. 在工作环境配置页面中，单击 * 添加数据源 * > * 添加 OneDrive 帐户 *。



2. 在添加 OneDrive 帐户对话框中，单击 * 登录到 OneDrive*。
3. 在显示的 Microsoft 页面中，选择 OneDrive 帐户并输入所需的管理员用户和密码，然后单击 * 接受 * 以允许 Cloud Data sense 从此帐户读取数据。

OneDrive 帐户将添加到工作环境列表中。

将 OneDrive 用户添加到合规性扫描

您可以添加单个 OneDrive 用户或所有 OneDrive 用户，以便 Cloud Data sense 对其文件进行扫描。

步骤

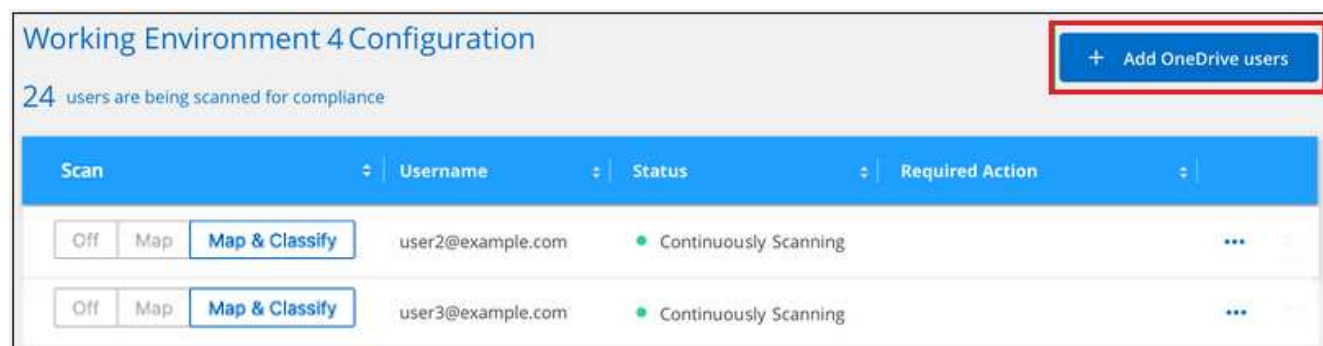
1. 在 *Configuration* 页面中，单击 OneDrive 帐户的 * 配置 * 按钮。



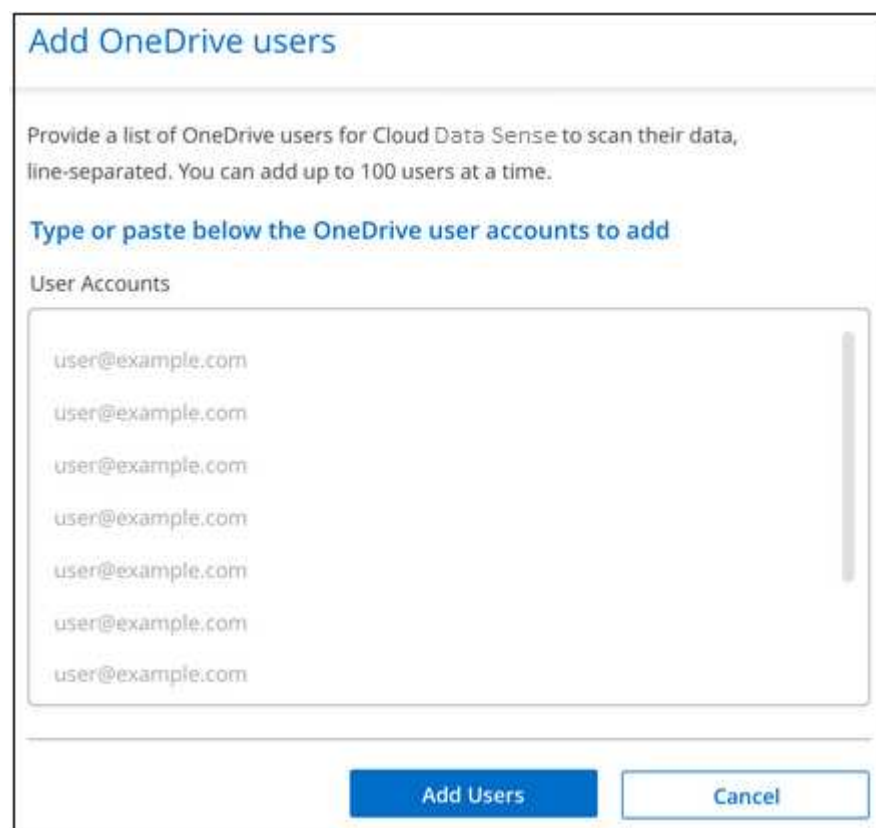
2. 如果这是首次为此 OneDrive 帐户添加用户，请单击 * 添加您的首个 OneDrive 用户 *。



如果要从 OneDrive 帐户添加其他用户，请单击 * 添加 OneDrive 用户 *。



3. 为要扫描其文件的用户添加电子邮件地址 - 每行一个电子邮件地址（每个会话最多 100 个） - 然后单击 * 添加用户 *。



确认对话框将显示已添加的用户数。

如果此对话框列出了任何无法添加的用户，请捕获此信息，以便解析问题描述。在某些情况下，您可以使用更正后的电子邮件地址重新添加用户。

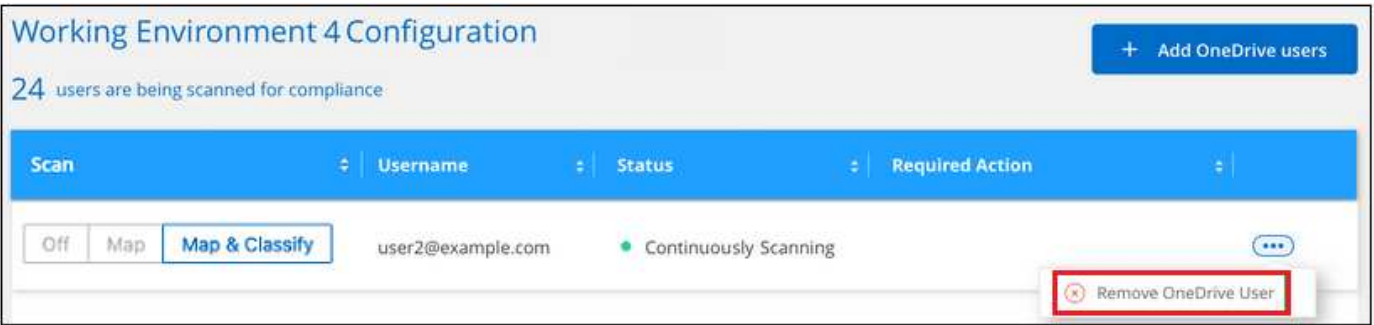
4. 对用户文件启用仅映射扫描或映射和分类扫描。

收件人：	执行以下操作：
对用户文件启用仅映射扫描	单击 * 映射 *
对用户文件启用完全扫描	单击 * 映射和分类 *
禁用对用户文件的扫描	单击 * 关闭 *

Cloud Data sense 开始扫描您添加的用户文件，结果将显示在信息板和其他位置。

从合规性扫描中删除 OneDrive 用户

如果用户离开公司或其电子邮件地址发生变化，您可以随时删除单个 OneDrive 用户的文件扫描功能。只需从配置页面中单击 * 删除 OneDrive 用户 * 即可。



请注意，您可以 "从Data sense中删除整个OneDrive帐户" 如果您不想再扫描OneDrive帐户中的任何用户数据。

扫描 SharePoint 帐户

完成几个步骤，使用 Cloud Data sense 扫描 SharePoint 帐户中的文件。

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。

请确保您拥有用于登录到 SharePoint 帐户的管理员凭据，并且拥有要扫描的 SharePoint 站点的 URL 。

"部署 Cloud Data sense" 如果尚未部署实例。

使用管理员用户凭据登录到要访问的 SharePoint 帐户，以便将其添加为新的数据源 / 工作环境。

在 SharePoint 帐户中添加要扫描的 SharePoint 站点 URL 列表，然后选择扫描类型。一次最多可以添加 100 个 URL 。

查看 SharePoint 要求

请查看以下前提条件，以确保您已准备好在 SharePoint 帐户上启用 Cloud Data sense。

- 您必须具有可对所有 SharePoint 站点进行读取访问的 SharePoint 帐户的管理员登录凭据。
- 对于要扫描的所有数据，您需要一个以行分隔的 SharePoint 站点 URL 列表。

部署 Cloud Data sense 实例

如果尚未部署实例，请部署 Cloud Data sense。

数据感知可以是 "部署在云中" 或 "位于可访问 Internet 的内部位置"。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

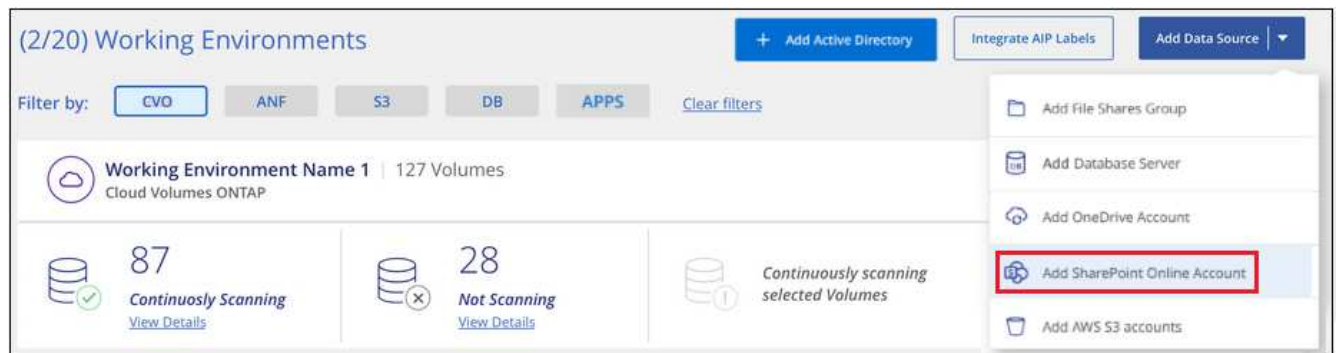
数据感知也可以是 "部署在无法访问 Internet 的内部位置"。但是，要扫描本地 SharePoint 文件，您需要为一些选定端点提供 Internet 访问。"请在此处查看所需端点的列表"。

正在添加 SharePoint 帐户

添加用户文件所在的 SharePoint 帐户。

步骤

1. 在工作环境配置页面中，单击 * 添加数据源 * > * 添加 SharePoint Online 帐户 *。



2. 在添加 SharePoint Online 帐户对话框中，单击 * 登录到 SharePoint*。
3. 在显示的 Microsoft 页面中，选择 SharePoint 帐户并输入所需的管理人员用户和密码，然后单击 * 接受 * 以允许 Cloud Data sense 从此帐户读取数据。

SharePoint 帐户将添加到工作环境列表中。

将 SharePoint 站点添加到合规性扫描

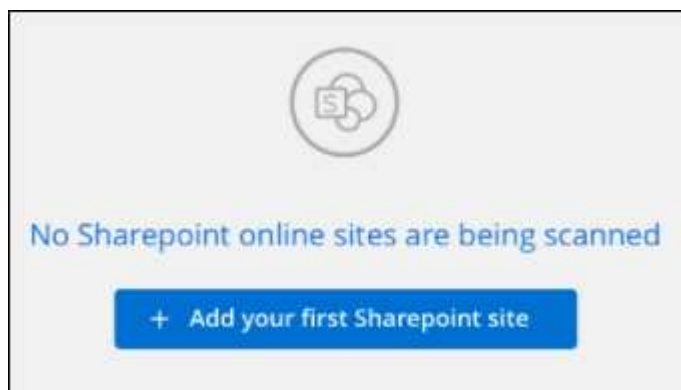
您可以在帐户中添加单个 SharePoint 站点或所有 SharePoint 站点，以便 Cloud Data sense 扫描关联的文件。

步骤

1. 在 *Configuration* 页面中，单击 SharePoint 帐户的 * 配置 * 按钮。



2. 如果这是首次为此 SharePoint 帐户添加站点，请单击 * 添加您的第一个 SharePoint 站点 *。



如果要从 SharePoint 帐户添加其他用户，请单击 * 添加 SharePoint 站点 *。



3. 为要扫描其文件的站点添加 URL - 每行一个 URL（每个会话最多 100 个 URL） - 然后单击 * 添加站点 *。

Add Sharepoint Online Sites

Provide a list of Sharepoint sites for Cloud Data Sense to scan their data, line-separated. You can add up to 100 sites at a time.

Type or paste below the Sharepoint Site URL to add

Site URL

https://netapp.sharepoint.com/sites/ComplianceUserStories

https://netapp.sharepoint.com/sites/ComplianceUserStories

https://netapp.sharepoint.com/sites/ComplianceUserStories

https://netapp.sharepoint.com/sites/ComplianceUserStories

https://netapp.sharepoint.com/sites/ComplianceUserStories

https://netapp.sharepoint.com/sites/ComplianceUserStories

Add Sites

Cancel

确认对话框将显示已添加的站点数量。

如果此对话框列出了任何无法添加的站点，请捕获此信息，以便您可以解析问题描述。在某些情况下，您可以使用更正后的 URL 重新添加此站点。

4. 对 SharePoint 站点中的文件启用仅映射扫描或映射和分类扫描。

收件人：	执行以下操作：
对文件启用仅映射扫描	单击 * 映射 *
对文件启用完全扫描	单击 * 映射和分类 *
禁用文件扫描	单击 * 关闭 *

Cloud Data sense 开始扫描您添加的 SharePoint 站点中的文件，结果将显示在信息板和其他位置。

从合规性扫描中删除 **SharePoint** 站点

如果您将来删除某个 SharePoint 站点，或者决定不扫描 SharePoint 站点中的文件，则可以随时删除各个 SharePoint 站点，使其无法扫描其文件。只需从配置页面中单击 * 删除 SharePoint 站点 * 即可。

ScanSite URLStatusRequired Action

OffMapMap & Classify

Site URL

Continuously Scanning

Remove SharePoint Site

OffMapMap & Classify

Site URL

Continuously Scanning

请注意，您可以 ["从Data sense中删除整个SharePoint帐户"](#) 如果您不想再扫描SharePoint帐户中的任何用户数据。

扫描Google Drive帐户

请完成几个步骤、开始使用Cloud Data sense扫描Google Drive帐户中的用户文件。

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。

确保您拥有登录到Google Drive帐户所需的管理员凭据。

["部署 Cloud Data sense"](#) 如果尚未部署实例。

使用管理员用户凭据登录到要访问的Google Drive帐户、以便将其添加为新的数据源。

选择要对用户文件执行的扫描类型；映射或映射和分类。

查看Google Drive要求

请查看以下前提条件、以确保您已准备好在Google Drive帐户上启用Cloud Data sense。

- 您必须拥有Google Drive帐户的管理员登录凭据、该帐户可提供对用户文件的读取访问权限

当前限制

Google Drive文件当前不支持以下Data sense功能：

- 在"数据调查"页面中查看文件时、按钮栏中的操作未处于活动状态。您不能复制、移动、删除等任何文件。
- 无法在Google Drive中的文件中标识权限、因此调查页面中不会显示任何权限信息。

部署 Cloud Data sense

如果尚未部署实例，请部署 Cloud Data sense 。

数据感知可以是 ["部署在云中"](#) 或 ["位于可访问 Internet 的内部位置"](#)。

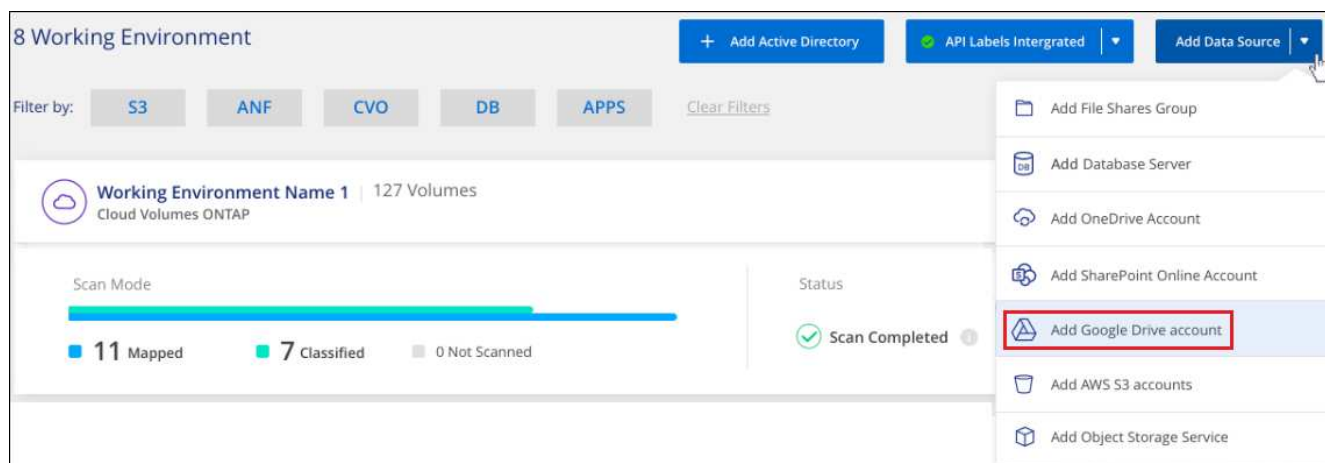
只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

正在添加Google Drive帐户

添加用户文件所在的Google Drive帐户。如果要扫描多个用户的文件、则需要对每个用户运行此步骤。

步骤

1. 在工作环境配置页面中、单击*添加数据源*>*添加Google Drive帐户*。



2. 在添加Google Drive帐户对话框中、单击*登录到Google Drive*。
3. 在显示的Google页面中、选择Google Drive帐户并输入所需的管理员用户和密码、然后单击*接受*以允许Cloud Data sense从此帐户读取数据。

Google Drive帐户将添加到工作环境列表中。

选择扫描用户数据的类型

选择Cloud Data sense将对用户数据执行的扫描类型。

步骤

1. 在_Configuration_页面中、单击Google Drive帐户的*配置*按钮。



2. 对Google Drive帐户中的文件启用仅映射扫描或映射和分类扫描。



收件人：	执行以下操作：
对文件启用仅映射扫描	单击 * 映射 *
对文件启用完全扫描	单击 * 映射和分类 *
禁用文件扫描	单击 * 关闭 *

Cloud Data sense开始扫描您添加的Google Drive帐户中的文件、结果将显示在信息板和其他位置。

从合规性扫描中删除Google Drive帐户

由于只有一个用户的Google Drive文件属于一个Google Drive帐户、因此、如果要停止扫描用户的Google Drive帐户中的文件、则应执行此操作 "[从Data sense中删除Google Drive帐户](#)"。

正在扫描文件共享

完成几个步骤，直接使用 Cloud Data sense 扫描非 NetApp NFS 或 CIFS 文件共享。这些文件共享可以驻留在内部或云中。

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。

对于 CIFS （ SMB ） 共享，请确保您具有访问这些共享的凭据。

["部署 Cloud Data sense"](#) 如果尚未部署实例。

组是要扫描的文件共享的容器，它用作这些文件共享的工作环境名称。

添加要扫描的文件共享列表并选择扫描类型。一次最多可以添加 100 个文件共享。

查看文件共享要求

在启用 Cloud Data sense 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。这些文件共享驻留在非 NetApp 存储系统上。
- Data sense 实例和共享之间需要有网络连接。
- 确保这些端口对 Data sense 实例开放：
 - 对于 NFS —端口 111 和 2049 。
 - 对于 CIFS —端口 139 和 445 。
- 您需要采用格式 ``<host_name> : /<share_path>`` 添加的共享列表。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。
- 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 Cloud Data sense 需要扫描任何需要提升权限的数据，则最好使用管理员凭据。

如果要确保数据感知分类扫描不会更改文件的"上次访问时间"、我们建议用户具有"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。

部署 Cloud Data sense 实例

如果尚未部署实例，请部署 Cloud Data sense 。

如果要扫描可通过 Internet 访问的非 NetApp NFS 或 CIFS 文件共享，则可以 "[在云中部署 Cloud Data sense](#)" 或 "[在可访问 Internet 的内部位置部署 Data sense](#)"。

如果要扫描的非 NetApp NFS 或 CIFS 文件共享安装在无法访问 Internet 的非公开站点中，则需要执行以下操作

"在无法访问 Internet 的同一内部位置部署 Cloud Data sense"。这还要求 Cloud Manager Connector 部署在 同一内部位置。

只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

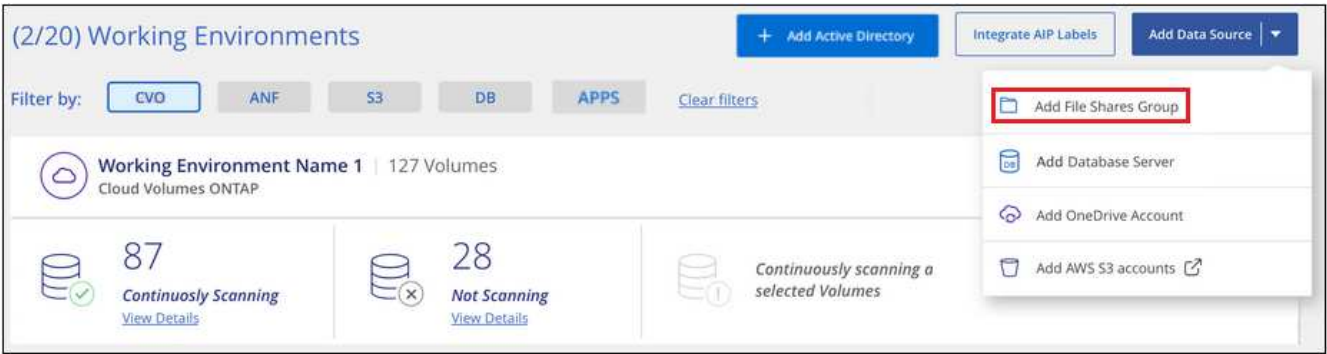
为文件共享创建组

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. 在工作环境配置页面中，单击 * 添加数据源 * > * 添加文件共享组 *。



- 2. 在添加文件共享组对话框中，输入共享组的名称，然后单击 * 继续 *。

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 Cloud Data sense 扫描这些共享中的文件。添加的共享格式为 `<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. 在 Working Environments 页面中，单击文件共享组的 * 配置 * 按钮。



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

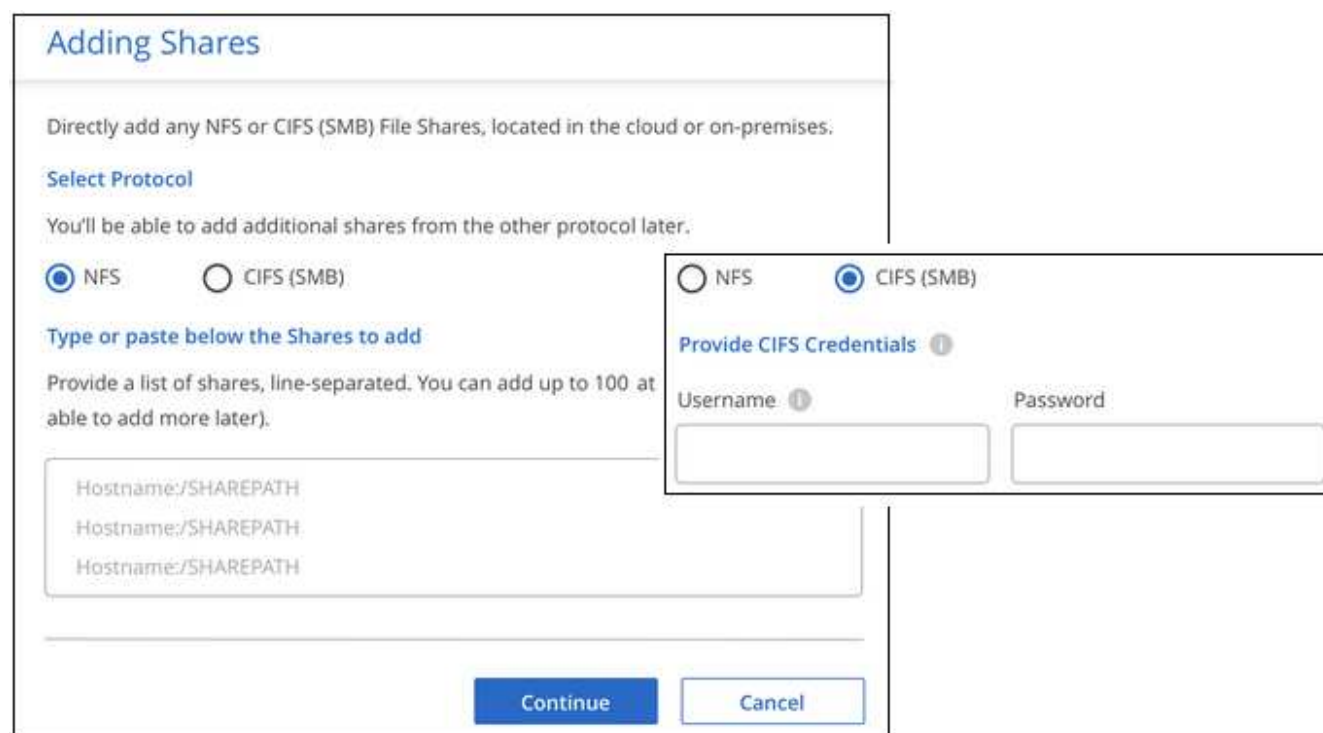


如果要向现有组添加文件共享，请单击 * 添加共享 *。



3. 选择要添加的文件共享的协议，添加要扫描的文件共享 - 每行一个文件共享 - 然后单击 * 继续 *。

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。

4. 在每个文件共享上启用仅映射扫描或映射和分类扫描。

收件人：	执行以下操作：
对文件共享启用仅映射扫描	单击 * 映射 *
对文件共享启用完全扫描	单击 * 映射和分类 *
禁用对文件共享的扫描	单击 * 关闭 *

Cloud Data sense 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。只需单击配置页面中的 * 删除共享 * 即可。



扫描使用 S3 协议的对象存储

完成几个步骤，直接使用 Cloud Data sense 扫描对象存储中的数据。数据感知功能可以扫描使用简单存储服务（ Simple Storage Service ， S3 ）协议的任何对象存储服务中的数据。其中包括 NetApp StorageGRID ， IBM 云对象存储， Azure Blob （使用 MinIO ）， Linode ， B2 云存储， Amazon S3 等。

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。

您需要具有端点 URL 才能连接到对象存储服务。

您需要从对象存储提供程序获取访问密钥和机密密钥，以便 Cloud Data sense 可以访问存储分段。

"部署 Cloud Data sense" 如果尚未部署实例。

将对象存储服务添加到 Cloud Data sense 。

选择要扫描的存储分段， Cloud Data sense 将开始扫描这些存储分段。

查看对象存储要求

在启用 Cloud Data sense 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。
- 您需要从对象存储提供程序获取访问密钥和机密密钥，以便 Data sense 可以访问存储分段。
- 要支持 Azure Blob ， 您需要使用 "MinIO 服务"。

部署 Cloud Data sense 实例

如果尚未部署实例，请部署 Cloud Data sense 。

如果要从可通过 Internet 访问的 S3 对象存储扫描数据，则可以 ["在云中部署 Cloud Data sense"](#) 或 ["在可访问 Internet 的内部位置部署 Data sense"](#)。

如果要从安装在无法访问 Internet 的非公开站点中的 S3 对象存储扫描数据，则需要执行以下操作 ["在无法访问 Internet 的同一内部位置部署 Cloud Data sense"](#)。这还要求 Cloud Manager Connector 部署在同一内部位置。

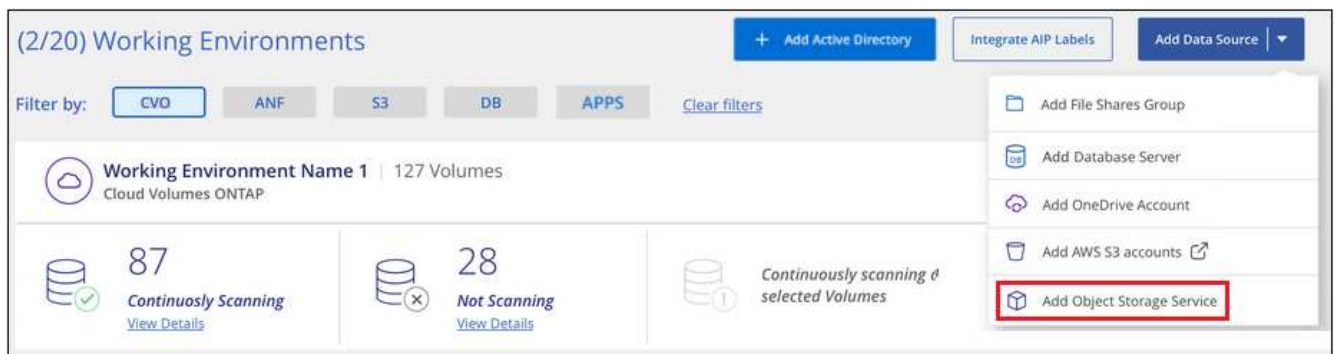
只要实例具有 Internet 连接，就会自动升级到 Data sense 软件。

将对象存储服务添加到 Cloud Data sense

添加对象存储服务。

步骤

1. 在工作环境配置页面中，单击 * 添加数据源 * > * 添加对象存储服务 * 。



2. 在添加对象存储服务对话框中，输入对象存储服务的详细信息，然后单击 * 继续 * 。
 - a. 输入要用于工作环境的名称。此名称应反映要连接到的对象存储服务的名称。
 - 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 Cloud Data sense 可以访问对象存储中的存储分段。

Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKD0574NDJG86795"/>	<input type="text" value="....."/>

新的对象存储服务将添加到工作环境列表中。

启用和禁用对象存储分段上的合规性扫描

在对象存储服务上启用 Cloud Data sense 后，下一步是配置要扫描的分段。Data sense 会发现这些分段并将其显示在您创建的工作环境中。

步骤

1. 在配置页面中，单击对象存储服务工作环境中的 * 配置 *。

(1/20) Working Environments

+ Add Active Directory

Integrate AIP Labels

Add Data Source

Filter by:

CVO

ANF

S3

DB

APPS

OB.STG

Clear filters

Rstor Integrated

Object Storage Service

41 Buckets

Configuration

23

Continuously Scanning

View Details

All Buckets selected for Compliance

Continuously scanning all selected Buckets

2. 在存储分段上启用仅映射扫描或映射和分类扫描。

38

Rstor Integrated Configuration			
3/55 Buckets selected for Compliance scan			
Scan	Storage Repository (Bucket) ↓↑	Status ↓↑	Required Action ↓↑
Off Map Map & Classify	logs-759995470648-us-east-1	● Not Scanning	
Off Map Map & Classify	logs-759995470648-us-west-2	● Not Scanning	
Off Map Map & Classify	carstock	● Continuously Scanning	

收件人：	执行以下操作：
在存储分段上启用仅映射扫描	单击 * 映射 *
对存储分段启用完全扫描	单击 * 映射和分类 *
禁用对存储分段的扫描	单击 * 关闭 *

Cloud Data sense 开始扫描您启用的存储分段。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。

版权信息

版权所有©2022 NetApp、Inc.。保留所有权利。Printed in the U.S.版权所涵盖的本文档的任何部分不得以任何形式或任何手段复制、包括影印、录制、磁带或存储在电子检索系统中—未经版权所有者事先书面许可。

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

本软件由NetApp按"原样"提供、不含任何明示或默示担保、包括但不限于适销性和特定用途适用性的默示担保、特此声明不承担任何任何责任。IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

商标信息

NetApp、NetApp标识和中列出的标记 <http://www.netapp.com/TM> 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。