设置和配置Keystone

Keystone

NetApp
January 15, 2026

目录

设置和配置Keystone 1
要求 1
Keystone Collector 的虚拟基础设施要求 1
Keystone Collector 的 Linux 系统要求 2
Keystone对ONTAP和StorageGRID 的要求 4
安装Keystone Collector 6
在 VMware vSphere 系统上部署Keystone Collector 6
在 Linux 系统上安装Keystone Collector 9
Keystone软件的自动验证 10
配置Keystone收集器 11
在Keystone Collector 上配置 HTTP 代理 12
限制收集私人数据 13
信任自定义根 CA 14
创建性能服务级别 15
安装 ITOM Collector 18
Keystone ITOM Collector 的安装要求 19
在 Linux 系统上安装Keystone ITOM Collector 20
在 Windows 系统上安装Keystone ITOM Collector 21
为Keystone配置AutoSupport 21
监控和升级 23
监控Keystone Collector 的健康状况 23
手动升级Keystone Collector 28
Keystone Collector 安全性 30
安全强化 30
Keystone收集的用户数据类型 31
ONTAP数据收集 31
StorageGRID数据收集 39
遥测数据收集 39
Keystone处于私人模式 41
了解Keystone （私人模式） 41
准备以私有模式安装Keystone Collector 42
以私人模式安装Keystone Collector 43
以私有模式配置Keystone Collector 44
以私人模式监控Keystone Collector 的健康状况 49

设置和配置Keystone

要求

Keystone Collector 的虚拟基础设施要求

在安装Keystone Collector 之前，您的 VMware vSphere 系统必须满足几个要求。

Keystone Collector 服务器虚拟机的先决条件：

- 操作系统：VMware vCenter 服务器和 ESXi 8.0 或更高版本
- 核心：1 个 CPU
- 内存：2 GB
- 磁盘空间：20 GB vDisk

其他要求

确保满足以下通用要求：

组网需求

Keystone Collector 的组网要求如下表所示。

Keystone Collector 需要互联网连接。您可以通过默认网关（通过 NAT）直接路由或通过 HTTP 代理提供互联网连接。这里描述了这两种变体。

源	目标	服务	协议和端口	类别	目的
Keystone Collector（适用于Keystone ONTAP）	Active IQ Unified Manager（统一管理器）	HTTPS	TCP 443	强制（如果使用Keystone ONTAP）	ONTAP的Keystone Collector 使用情况指标收集
Keystone Collector（用于Keystone StorageGRID）	StorageGRID管理节点	HTTPS	TCP 443	强制（如果使用Keystone StorageGRID）	StorageGRID的Keystone Collector 使用情况指标收集
Keystone收集器（通用）	互联网（根据稍后给出的 URL 要求）	HTTPS	TCP 443	强制性（互联网连接）	Keystone Collector 软件、操作系统更新和指标上传
Keystone收集器（通用）	客户 HTTP 代理	HTTP 代理	客户代理端口	强制性（互联网连接）	Keystone Collector 软件、操作系统更新和指标上传

Keystone收集器（通用）	客户 DNS 服务器	DNS	TCP/UDP 53	强制的	DNS解析
Keystone收集器（通用）	客户 NTP 服务器	NTP	UDP 123	强制的	时间同步
Keystone Collector（适用于Keystone ONTAP）	Unified Manager	MYSQL	TCP 3306	可选功能	Keystone Collector 的性能指标收集
Keystone收集器（通用）	客户监控系统	HTTPS	TCP 7777	可选功能	Keystone Collector 健康报告
客户的操作工作站	Keystone收集器	SSH	TCP 22	管理	访问Keystone Collector Management
NetApp ONTAP 集群和节点管理地址	Keystone收集器	HTTP_8000，PING	TCP 8000，ICMP 回显请求/答复	可选功能	用于ONTAP固件更新的 Web 服务器

在全新安装 Unified Manager 期间，MySQL 的默认端口 3306 仅限于本地主机，这会阻止收集Keystone Collector 的性能指标。有关更多信息，请参阅"ONTAP要求" 。

URL 访问

Keystone Collector 需要访问以下互联网主机：

地址	原因
https://keystone.netapp.com	Keystone Collector 软件更新和使用情况报告
https://support.netapp.com	NetApp HQ 用于账单信息和AutoSupport交付

Keystone Collector 的 Linux 系统要求

使用所需的软件准备您的 Linux 系统可确保Keystone Collector 进行精确安装和数据收集。

确保您的 Linux 和Keystone Collector 服务器 VM 具有这些配置。

Linux 服务器：

- 操作系统：以下任一种：
  - Debian 12
  - Red Hat Enterprise Linux 8.6 或更高版本 8.x

- Red Hat Enterprise Linux 9.0 或更高版本
- CentOS 7（仅适用于现有环境）

- Chronyd时间同步
- 访问标准 Linux 软件存储库

同一服务器还应该具有以下第三方包：

- podman（POD管理器）
- 求救
- 慢性
- Python 3（3.9.14 至 3.11.8）

Keystone Collector 服务器虚拟机：

- 核心：2 个 CPU
- 内存：4 GB
- 磁盘空间：50 GB vDisk

其他要求

确保满足以下通用要求：

组网需求

Keystone Collector 的组网要求如下表所示。

Keystone Collector 需要互联网连接。您可以通过默认网关（通过 NAT）直接路由或通过 HTTP 代理提供互联网连接。这里描述了这两种变体。

源	目标	服务	协议和端口	类别	目的
Keystone Collector（适用于Keystone ONTAP）	Active IQ Unified Manager（统一管理器）	HTTPS	TCP 443	强制（如果使用Keystone ONTAP）	ONTAP的Keystone Collector 使用情况指标收集
Keystone Collector（用于Keystone StorageGRID）	StorageGRID管理节点	HTTPS	TCP 443	强制（如果使用Keystone StorageGRID）	StorageGRID的Keystone Collector 使用情况指标收集
Keystone收集器（通用）	互联网（根据稍后给出的 URL 要求）	HTTPS	TCP 443	强制性（互联网连接）	Keystone Collector 软件、操作系统更新和指标上传

Keystone收集器（通用）	客户 HTTP 代理	HTTP 代理	客户代理端口	强制性（互联网连接）	Keystone Collector 软件、操作系统更新和指标上传
Keystone收集器（通用）	客户 DNS 服务器	DNS	TCP/UDP 53	强制的	DNS解析
Keystone收集器（通用）	客户 NTP 服务器	NTP	UDP 123	强制的	时间同步
Keystone Collector（适用于Keystone ONTAP）	Unified Manager	MYSQL	TCP 3306	可选功能	Keystone Collector 的性能指标收集
Keystone收集器（通用）	客户监控系统	HTTPS	TCP 7777	可选功能	Keystone Collector 健康报告
客户的操作工作站	Keystone收集器	SSH	TCP 22	管理	访问Keystone Collector Management
NetApp ONTAP 集群和节点管理地址	Keystone收集器	HTTP_8000，PING	TCP 8000，ICMP 回显请求/答复	可选功能	用于ONTAP固件更新的 Web 服务器

在全新安装 Unified Manager 期间，MySQL 的默认端口 3306 仅限于本地主机，这会阻止收集Keystone Collector 的性能指标。有关更多信息，请参阅"ONTAP要求" 。

URL 访问

Keystone Collector 需要访问以下互联网主机：

地址	原因
https://keystone.netapp.com	Keystone Collector 软件更新和使用情况报告
https://support.netapp.com	NetApp HQ 用于账单信息和AutoSupport交付

Keystone对ONTAP和StorageGRID 的要求

在开始使用Keystone之前，您需要确保ONTAP集群和StorageGRID系统满足一些要求。

ONTAP

软件版本

1. ONTAP 9.8 或更高版本
2. Active IQ Unified Manager （Unified Manager）9.10 或更高版本

开始之前

如果您打算仅通过ONTAP收集使用情况数据，请满足以下要求：

1. 确保已配置ONTAP 9.8 或更高版本。有关配置新集群的信息，请参阅以下链接：
   - "使用 System Manager 在新集群上配置ONTAP"
   - "使用 CLI 设置集群"
2. 创建具有特定角色的ONTAP登录帐户。要了解更多信息，请参阅 "了解如何创建ONTAP登录帐户"。
   - 网页用户界面
     i. 使用您的默认凭据登录ONTAP系统管理器。要了解更多信息，请参阅 "使用系统管理器进行集群管理"。
     ii. 创建具有“readonly”角色和“http”应用程序类型的ONTAP用户，并通过导航到 **Cluster > Settings > Security > Users** 启用密码验证。
   - 命令行界面
     i. 使用您的默认凭据登录ONTAP CLI。要了解更多信息，请参阅 "使用 CLI 进行集群管理"。
     ii. 创建具有“readonly”角色和“http”应用程序类型的ONTAP用户，并启用密码验证。要了解有关身份验证的更多信息，请参阅 "启用ONTAP帐户密码访问"。

如果您打算通过Active IQ Unified Manager收集使用情况数据，请满足以下要求：

1. 确保已配置 Unified Manager 9.10 或更高版本。有关安装 Unified Manager 的信息，请参阅以下链接：
   - "在 VMware vSphere 系统上安装 Unified Manager"
   - "在 Linux 系统上安装 Unified Manager"
2. 确保ONTAP集群已添加到 Unified Manager。有关添加集群的信息，请参阅 "添加集群"。
3. 创建具有特定角色的 Unified Manager 用户以收集使用情况和性能数据。执行以下步骤。有关用户角色的信息，请参阅 "用户角色的定义"。
   a. 使用安装期间生成的默认应用程序管理员用户凭据登录 Unified Manager Web UI。看 "访问 Unified Manager Web UI"。
   b. 使用以下方式为Keystone Collector 创建服务帐户 `Operator`用户角色。 Keystone Collector 服务 API 使用此服务帐户与 Unified Manager 通信并收集使用情况数据。看 "添加用户"。
   c. 创建一个 `Database`用户帐户， `Report Schema`角色。性能数据收集需要此用户。看 "创建数据库用户"。

> 在全新安装 Unified Manager 期间，MySQL 的默认端口 3306 仅限于本地主机，这会阻止收集Keystone ONTAP的性能数据。可以修改此配置，并且可以使用 `Control access to MySQL port 3306`Unified Manager 维护控制台上的选项。有关信息，请参阅"附加菜单选项"。

4. 在 Unified Manager 中启用 API 网关。 Keystone Collector 利用 API 网关功能与ONTAP集群进行通信。您可以从 Web UI 启用 API 网关，也可以通过 Unified Manager CLI 运行一些命令来启用 API 网关。

   Web 用户界面

   要从 Unified Manager Web UI 启用 API 网关，请登录 Unified Manager Web UI 并启用 API 网关。有关信息，请参阅 "启用 API 网关"。

   命令行界面

   要通过 Unified Manager CLI 启用 API Gateway，请按照以下步骤操作：

   a. 在 Unified Manager 服务器上，开始 SSH 会话并登录 Unified Manager CLI。
   `um cli login -u <*umadmin*>`有关 CLI 命令的信息，请参阅 "支持的 Unified Manager CLI 命令"。

   b. 验证 API 网关是否已启用。
   `um option list api.gateway.enabled`一个 `true`值表示API网关已启用。

   c. 如果返回的值是 `false`，运行此命令：
   `um option set api.gateway.enabled=true`

   d. 重新启动 Unified Manager 服务器：

      - Linux： "重新启动 Unified Manager" 。
      - VMware vSphere： "重新启动 Unified Manager 虚拟机" 。

StorageGRID

在StorageGRID上安装Keystone Collector 需要以下配置。

- StorageGRID `11.6.0`或更高版本应安装。有关升级StorageGRID 的信息，请参阅"升级StorageGRID 软件：概述"。
- 应创建一个StorageGRID本地管理员用户帐户来收集使用情况数据。 Keystone Collector 服务使用此服务帐户通过管理员节点 API 与StorageGRID通信。

  步骤

  a. 登录网格管理器。看 "Sign in网格管理器"。

  b. 使用以下方式创建本地管理员组 `Access mode: Read-only`。看 "创建管理员组"。

  c. 添加以下权限：

     - 租户账户
     - 维护
     - 指标查询

  d. 创建Keystone服务帐户用户并将其与管理员组关联。看 "管理用户"。

安装Keystone Collector

在 **VMware vSphere** 系统上部署**Keystone Collector**

在 VMware vSphere 系统上部署Keystone Collector 包括下载 OVA 模板、使用 部署 **OVF**

模板 向导部署模板、验证证书的完整性以及验证 VM 的准备情况。

部署 **OVA** 模板

按照下面的步骤进行操作：

步骤

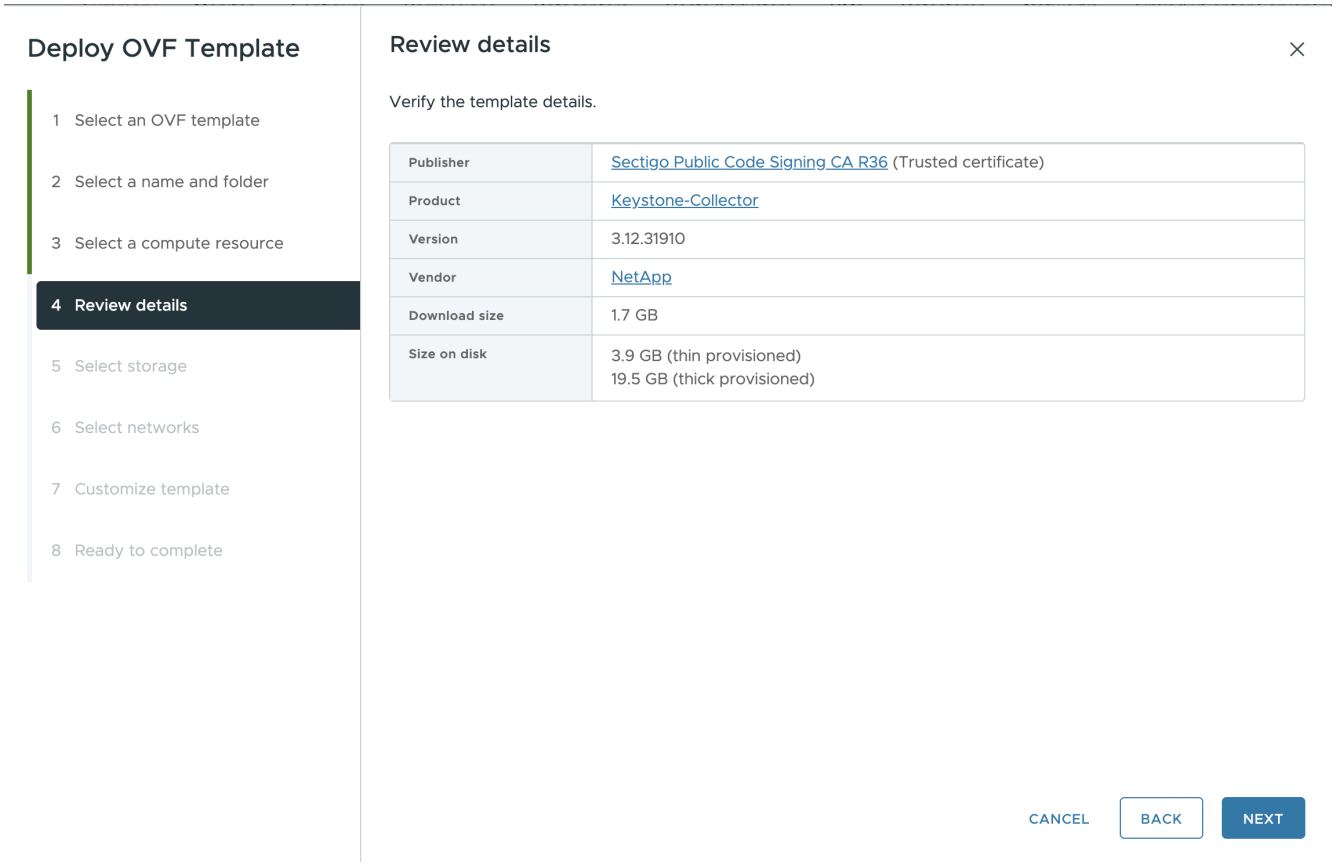
1. 从以下位置下载 OVA 文件 "此链接"并将其存储在您的 VMware vSphere 系统上。
2. 在 VMware vSphere 系统上，导航到 **VMs and Templates** 视图。
3. 右键单击虚拟机 (VM)（或数据中心，如果不使用 VM 文件夹）所需的文件夹，然后选择 部署 **OVF** 模板。
4. 在“部署 OVF 模板”向导的“步骤 1”中，单击“选择 OVF 模板”以选择已下载的 `KeystoneCollector-latest.ova` 文件。
5. 在_步骤 2_中，指定 VM 名称并选择 VM 文件夹。
6. 在_步骤 3_中，指定运行虚拟机所需的计算资源。
7. 在步骤 4：检查细节中，验证 OVA 文件的正确性和真实性。

   vCenter 根信任库仅包含 VMware 证书。NetApp使用 Entrust 作为认证机构，这些证书需要添加到 vCenter 信任库中。

   a. 从 Sectigo 下载代码签名 CA 证书 "此处"。
   b. 按照 `Resolution`此知识库 (KB) 文章的部分内容： https://kb.vmware.com/s/article/84240 。

   > 对于 vCenter 7.x 及更早版本，您必须将 vCenter 和 ESXi 更新到 8.0 或更高版本。早期版本已不再受支持。

   当Keystone Collector OVA 的完整性和真实性得到验证后，您就可以看到文本了。 `(Trusted certificate)` 与出版商合作。



8. 在部署 OVF 模板向导的第 5 步中，指定存储虚拟机的位置。
9. 在步骤 6 中，选择虚拟机要使用的目标网络。
10. 在_步骤 7 自定义模板_中，指定管理员用户帐户的初始网络地址和密码。

> 管理员密码以可逆格式存储在 vCenter 中，应用作引导凭据来获取对 VMware vSphere 系统的初始访问权限。在初始软件配置期间，应更改此管理员密码。 IPv4 地址的子网掩码应以 CIDR 表示法提供。例如，子网掩码 255.255.255.0 使用值 24。

11. 在部署 OVF 模板*向导的_步骤 8 准备完成_中，检查配置并验证您是否正确设置了 OVA 部署的参数。

从模板部署虚拟机并启动后，打开到虚拟机的 SSH 会话并使用临时管理员凭据登录以验证虚拟机是否已准备好进行配置。

初始系统配置

在 VMware vSphere 系统上执行以下步骤，对通过 OVA 部署的Keystone Collector 服务器进行初始配置：

> 完成部署后，您可以使用Keystone Collector 管理终端用户界面 (TUI) 实用程序执行配置和监控活动。您可以使用各种键盘控制（例如 Enter 和箭头键）来选择选项并浏览此 TUI。

1. 打开与Keystone Collector 服务器的 SSH 会话。当您连接时，系统将提示您更新管理员密码。按要求完成管理员密码更新。
2. 使用新密码登录以访问 TUI。登录后，TUI 就会出现。

   或者，您可以通过运行 `keystone-collector-tui`CLI 命令。

3. 如果需要，请在 TUI 上的 配置 **>** 网络部分 中配置代理详细信息。
4. 在*配置 > 系统*部分配置系统主机名、位置和 NTP 服务器。
5. 使用“维护”>“更新收集器”选项更新Keystone收集器。更新后，重新启动Keystone Collector 管理 TUI 实用程序以应用更改。

在 **Linux** 系统上安装**Keystone Collector**

您可以使用 RPM 或 Debian 包在 Linux 服务器上安装Keystone Collector 软件。根据您的 Linux 发行版执行安装步骤。

使用 **RPM**

1. 通过 SSH 连接到Keystone Collector 服务器并提升至 `root`特权。
2. 导入Keystone公共签名：
   `# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020`
3. 请通过检查 RPM 数据库中Keystone Billing Platform 的指纹，确保已导入正确的公共证书：
   `# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint` 正确的指纹如下所示：
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. 下载 `keystonerepo.rpm` 文件：
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. 验证文件的真实性：
   `rpm --checksig -v keystonerepo.rpm` 正版文件的签名如下所示：
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK`
6. 安装 YUM 软件存储库文件：
   `# yum install keystonerepo.rpm`
7. 安装Keystone repo 后，通过 YUM 包管理器安装 keystone-collector 包：

   `# yum install keystone-collector`

   对于 Red Hat Enterprise Linux 9，运行以下命令安装 keystone-collector 包：
   `# yum install keystone-collector-rhel9`

使用 **Debian**

1. 通过 SSH 连接到Keystone Collector 服务器并提升至 `root`特权。
   `` `sudo su ``
2. 下载 `keystone-sw-repo.deb`文件：
   `` `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb ``
3. 安装Keystone软件存储库文件：
   `# dpkg -i keystone-sw-repo.deb`
4. 更新软件包列表：
   `# apt-get update`
5. 安装Keystone repo 后，安装 keystone-collector 包：
   `# apt-get install keystone-collector`

完成安装后，您可以使用Keystone Collector 管理终端用户界面 (TUI) 实用程序执行配置和监控活动。您可以使用各种键盘控制（例如 Enter 和箭头键）来选择选项并浏览此 TUI。看"配置Keystone收集器"和"监控系统健康状况"了解详情。

Keystone软件的自动验证

Keystone存储库配置为自动验证Keystone软件的完整性，以便您的站点只安装有效且真实

的软件。

Keystone YUM 存储库客户端配置 `keystonerepo.rpm`使用强制 `GPG 检查(`gpgcheck=1`)` 适用于通过此存储库下载的所有软件。通过Keystone存储库下载的任何未通过签名验证的 RPM 都将被阻止安装。此功能用于Keystone Collector 的预定自动更新功能，以确保在您的站点上仅安装有效且真实的软件。

配置Keystone收集器

您需要完成一些配置任务才能使Keystone Collector 能够收集存储环境中的使用数据。这是一次性活动，用于激活所需组件并将其与您的存储环境关联起来。

- Keystone Collector 为您提供了Keystone Collector 管理终端用户界面 (TUI) 实用程序来执行配置和监控活动。您可以使用各种键盘控制（例如 Enter 和箭头键）来选择选项并浏览此 TUI。
- Keystone Collector 可以为无法访问互联网的组织进行配置，也称为_暗站_或_私人模式_。要了解更多信息，请参阅"Keystone处于私人模式"。

步骤

1. 启动Keystone Collector 管理 TUI 实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 转到配置**> KS-Collector**打开Keystone Collector 配置屏幕，查看可用的更新选项。
3. 更新所需的选项。

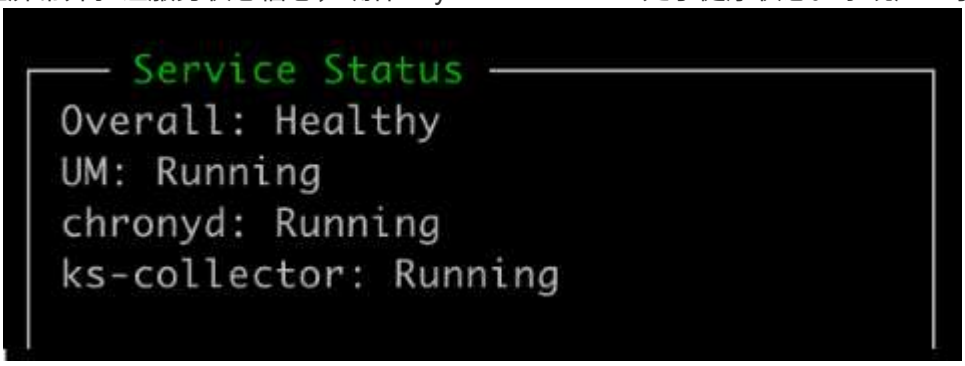
   适用于ONTAP

   - 收集**ONTAP**使用情况：此选项可收集ONTAP的使用情况数据。添加Active IQ Unified Manager（Unified Manager）服务器和服务帐户的详细信息。
   - 收集**ONTAP**性能数据：此选项可收集ONTAP的性能数据。默认情况下，此功能是禁用的。如果您的环境需要出于 SLA 目的进行性能监控，请启用此选项。提供 Unified Manager 数据库用户帐户详细信息。有关创建数据库用户的信息，请参阅"创建 Unified Manager 用户"。
   - 删除私人数据：此选项删除客户的特定私人数据，默认启用。有关启用此选项后哪些数据将从指标中排除的信息，请参阅"限制收集私人数据"。

   对于**StorageGRID**

   - 收集**StorageGRID**使用情况：此选项可以收集节点使用情况的详细信息。添加StorageGRID节点地址和用户详细信息。
   - 删除私人数据：此选项删除客户的特定私人数据，默认启用。有关启用此选项后哪些数据将从指标中排除的信息，请参阅"限制收集私人数据"。
4. 切换使用系统启动 **KS-Collector**字段。
5. 单击保存
   。

6. 通过返回 TUI 主屏幕并验证服务状态信息，确保Keystone Collector 处于健康状态。系统应显示服务处于总体：健康状态。



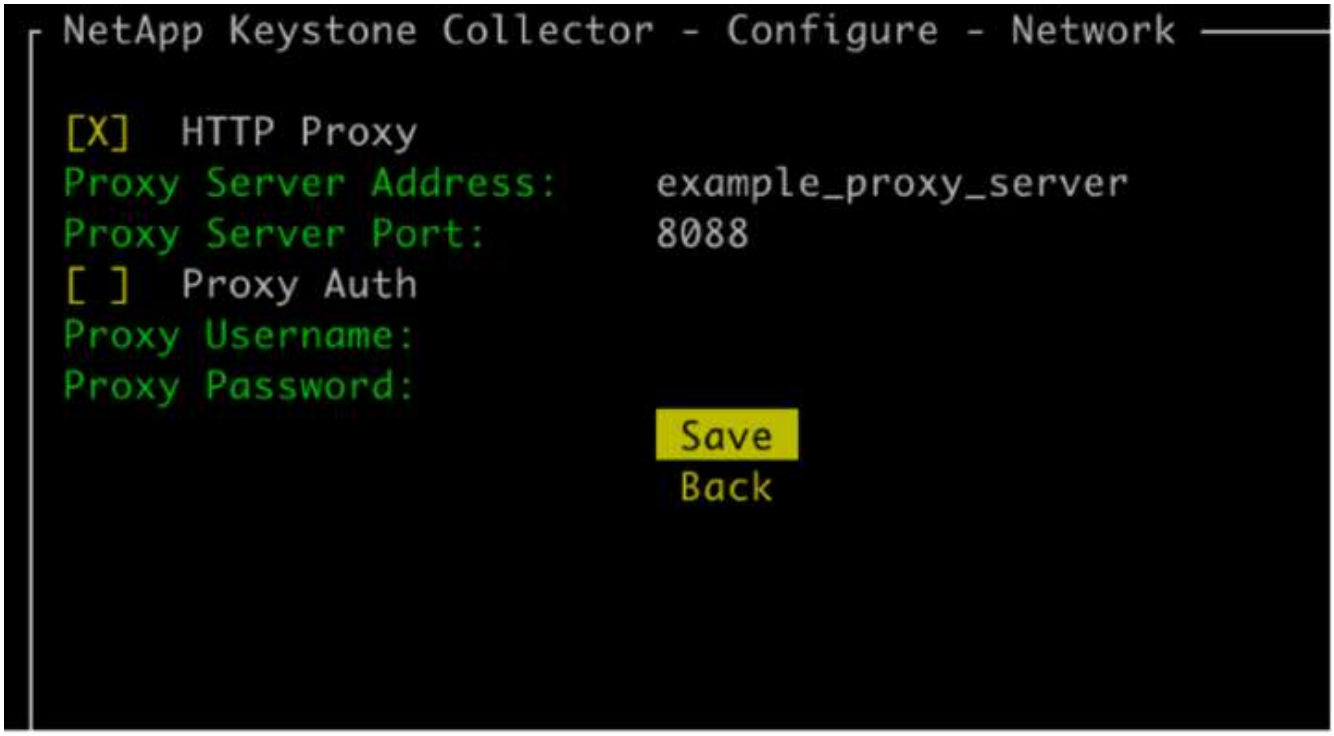
7. 通过选择主屏幕上的“退出到 Shell”选项退出Keystone Collector 管理 TUI。

在Keystone Collector 上配置 HTTP 代理

收集器软件支持使用 HTTP 代理与互联网通信。这可以在 TUI 中进行配置。

步骤

1. 如果已关闭，请重新启动Keystone Collector 管理 TUI 实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 切换到**HTTP** 代理字段，并添加 HTTP 代理服务器、端口和凭据的详细信息（如果需要身份验证）。
3. 单击保存
   。



限制收集私人数据

Keystone Collector 收集执行订阅计量所需的有限配置、状态和性能信息。有一个选项可以通过屏蔽上传内容中的敏感信息来进一步限制收集的信息。这不会影响账单计算。但是，限制信息可能会影响报告信息的可用性，因为一些用户可以轻松识别的元素（例如卷名）被 UUID 取代。

限制特定客户数据的收集是Keystone Collector TUI 屏幕上的可配置选项。此选项“删除私人数据”默认启用。

有关在ONTAP和StorageGRID中限制私有数据访问而删除的项目的信息，请参阅"限制私人数据访问而删除的项目列表"。

信任自定义根 CA

根据公共根证书颁发机构 (CA) 验证证书是Keystone Collector 安全功能的一部分。但是，如果需要，您可以将Keystone Collector 配置为信任自定义根 CA。

如果您在系统防火墙中使用 SSL/TLS 检查，则会导致基于互联网的流量使用您的自定义 CA 证书重新加密。在接受根证书并允许连接之前，需要配置设置以验证源是否为受信任的 CA。按照下面的步骤进行操作：

步骤

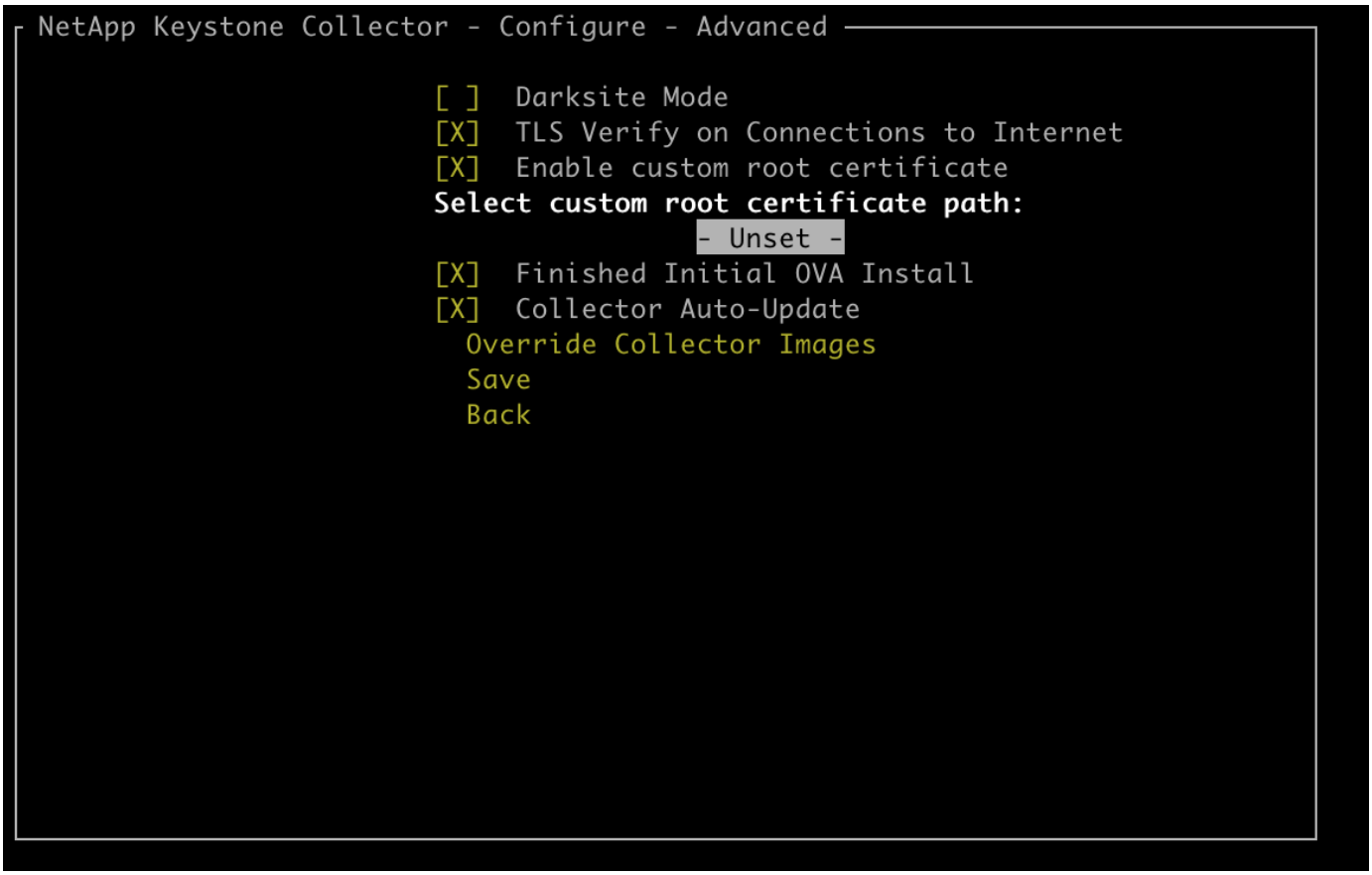
1. 准备CA证书。它应该是_base64 编码的 X.509_ 文件格式。

   支持的文件扩展名是 `.pem`， `.crt` ， `.cert` 。确保证书采用以下格式之一。

2. 将证书复制到Keystone Collector 服务器。记下文件复制的位置。
3. 在服务器上打开终端并运行管理 TUI 实用程序。
   ```
   $ keystone-collector-tui
   ```
4. 转到*配置>高级*。
5. 启用选项*启用自定义根证书*。
6. 对于 选择自定义根证书路径：，选择 `- Unset -`
7. 按 Enter。弹出选择证书路径的对话框。

8. 从文件系统浏览器中选择根证书或输入精确的路径。
9. 按 Enter。您将返回到*高级*屏幕。
10. 选择*保存*。配置已应用。

CA证书被复制到 `/opt/netapp/ks-collector/ca.pem` 在Keystone Collector 服务器上。



创建性能服务级别

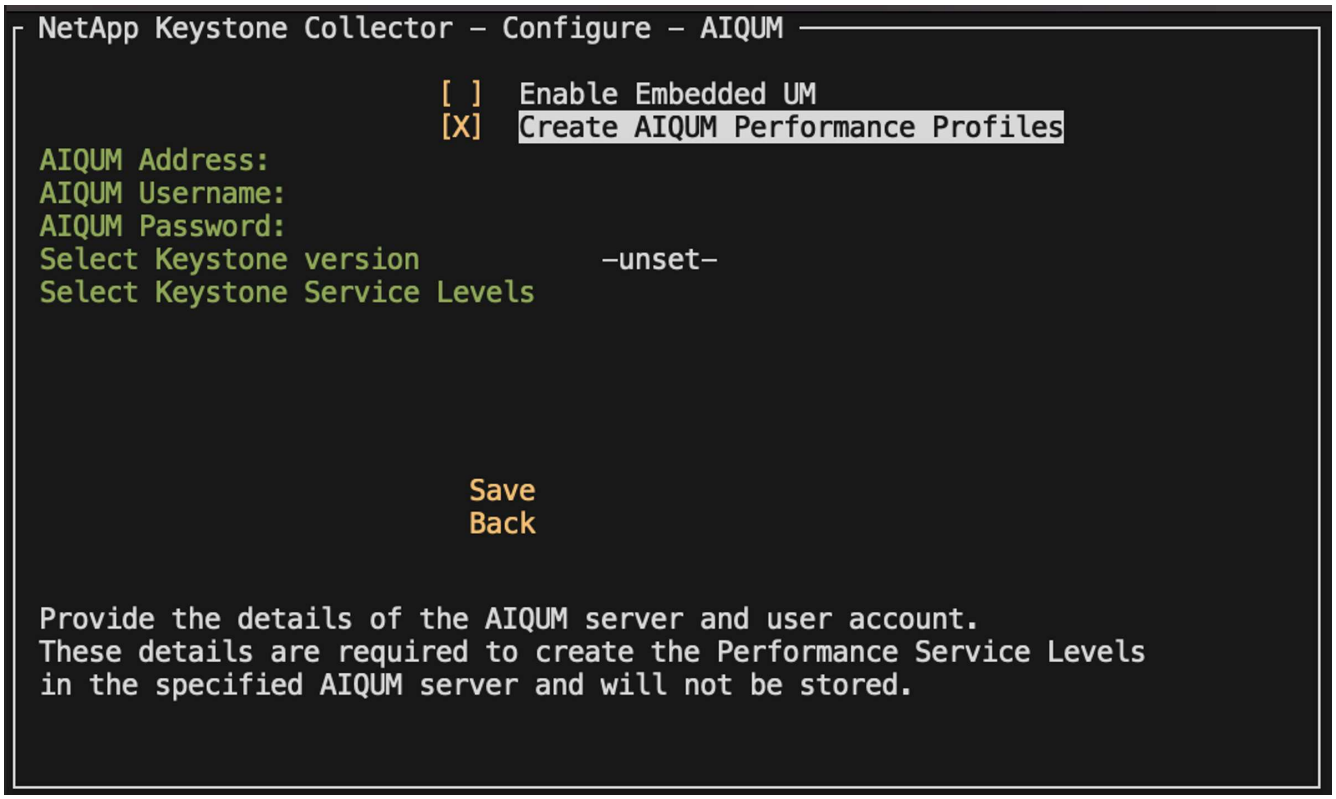
您可以使用Keystone Collector 管理 TUI 实用程序创建性能服务级别 (PSL)。通过 TUI 创建 PSL 会自动选择为每个性能服务级别设置的默认值，从而减少通过Active IQ Unified Manager创建 PSL 时手动设置这些值时可能发生的错误的可能性。

要了解有关 PSL 的更多信息，请参阅"性能服务级别"。

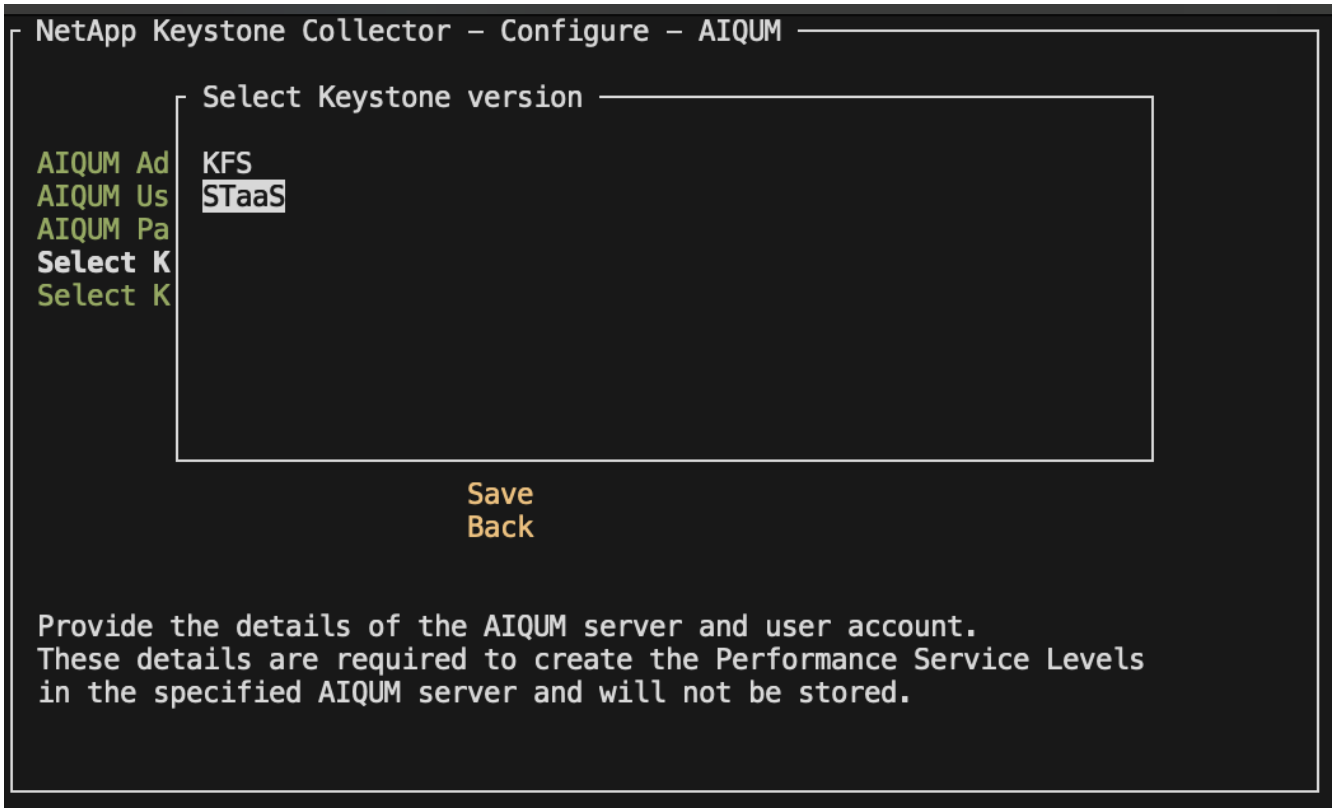
要了解有关服务级别的更多信息，请参阅"Keystone的服务级别"。

步骤

1. 启动Keystone Collector 管理 TUI 实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 转到*配置>AIQUM*以打开 AIQUM 屏幕。
3. 启用选项*创建 AIQUM 性能配置文件*。
4. 输入Active IQ Unified Manager服务器和用户帐户的详细信息。这些详细信息是创建 PSL 所必需的，并且不会被存储。

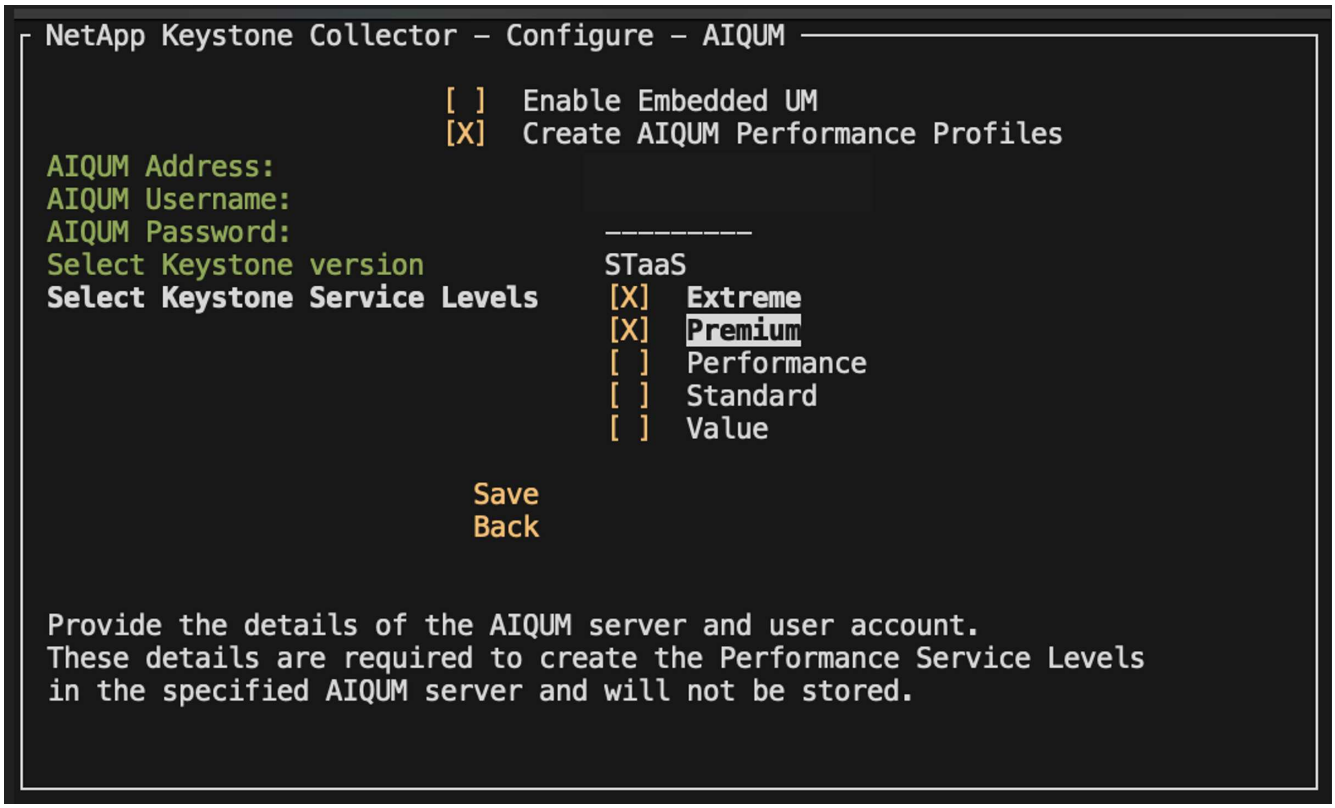


5. 对于“选择Keystone版本”，选择 `-unset-`。
6. 按 Enter。弹出选择Keystone版本的对话框。
7. 突出显示 **STaaS** 以指定Keystone STaaS 的Keystone版本，然后按 Enter。



您可以突出显示Keystone订阅服务版本 1 的 **KFS** 选项。Keystone订阅服务与Keystone STaaS 在组成性能服务级别、服务产品和计费原则方面有所不同。要了解更多信息，请参阅"Keystone订阅服务 | 版本 1"。

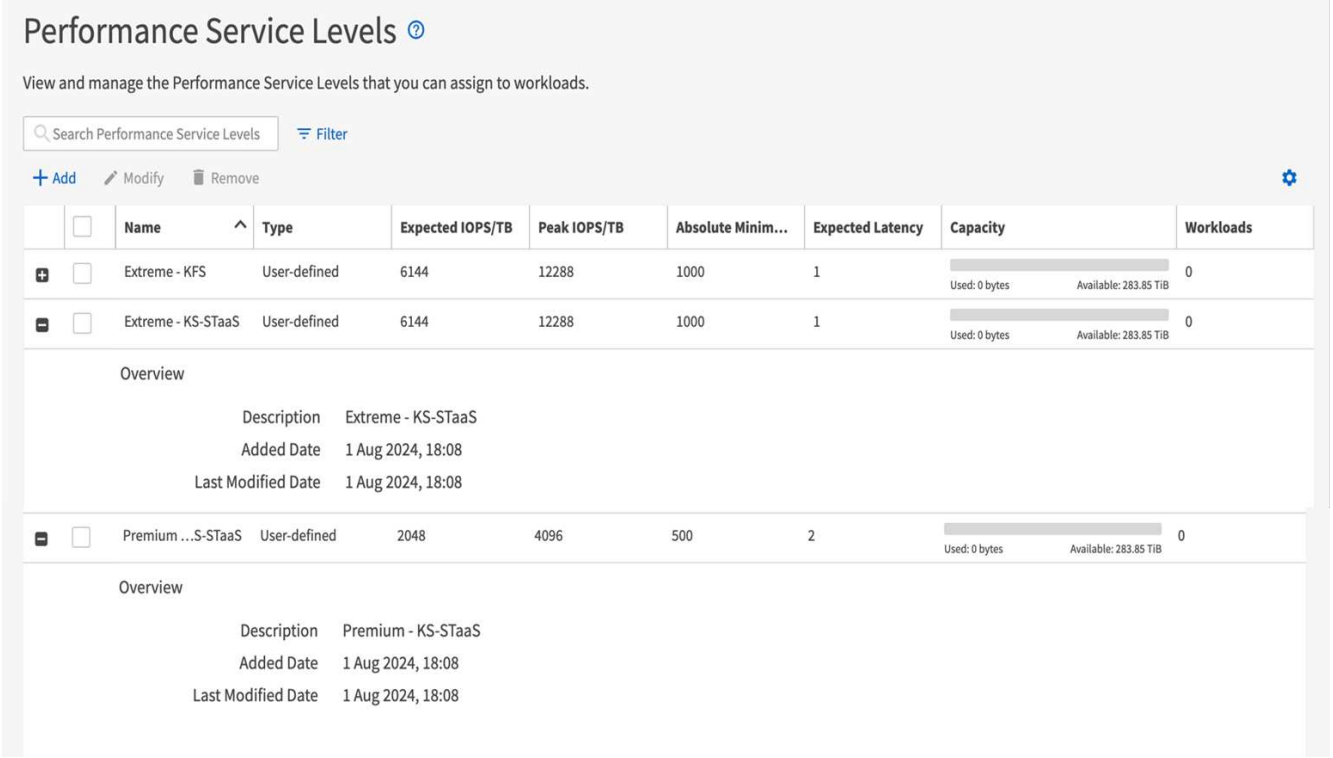
8. 所有受支持的Keystone性能服务级别将显示在指定Keystone版本的 选择**Keystone**服务级别 选项中。从列表中启用所需的性能服务级别。



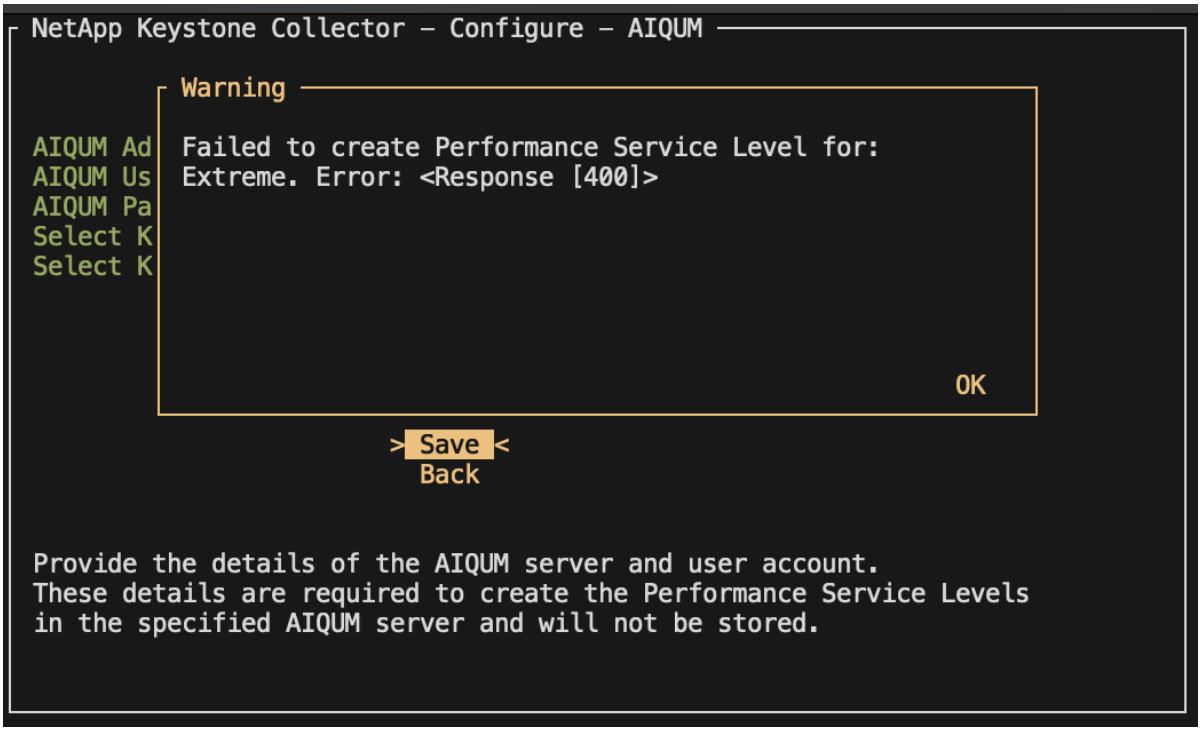
您可以同时选择多个性能服务级别来创建 PSL。

9. 选择“保存”并按 Enter。将创建性能服务级别。

   您可以在Active IQ Unified Manager中的 性能服务级别 页面上查看已创建的 PSL，例如 STaaS 的 Premium-KS-STaaS 或 KFS 的 Extreme KFS。如果创建的 PSL 不能满足您的要求，那么您可以修改 PSL 以满足您的需求。要了解更多信息，请参阅"创建和编辑性能服务级别"。



如果所选性能服务级别的 PSL 已存在于指定的Active IQ Unified Manger 服务器上，则无法再次创建它。如果您尝试这样做，您将收到一条错误消
息。



安装 ITOM Collector

Keystone ITOM Collector 的安装要求

在安装 ITOM Collector 之前，请确保您的系统已准备好必要的软件并满足所有必需的先决条件。

ITOM Collector 服务器 **VM** 的先决条件：

- 支持的操作系统：
  - Debian 12 或更高版本
  - Windows Server 2016 或更高版本
  - Ubuntu 20.04 LTS 或更高版本
  - 红帽企业 Linux (RHEL) 8.x
  - Red Hat Enterprise Linux 9.0 或更高版本
  - Amazon Linux 2023 或更高版本

  推荐的操作系统是 Debian 12、Windows Server 2016 或更新版本。

- 资源需求：根据监控的NetApp节点数量，虚拟机资源需求如下：
  - 2-10 个节点：4 个 CPU、8 GB RAM、40 GB 磁盘
  - 12-20 个节点：8 个 CPU、16 GB RAM、40 GB 磁盘
- 配置要求：确保被监控的设备上配置了只读账户和SNMP。如果适用，ITOM Collector 服务器 VM 还需要配置为NetApp集群和集群交换机上的 SNMP 陷阱主机和 Syslog 服务器。

网络要求

ITOM Collector 的组网要求如下表所示。

源	目标	协议	端口	描述
ITOM 收集器	NetApp ONTAP集群管理 IP	HTTPS、SNMP	TCP 443，UDP 161	ONTAP控制器监控
NetApp ONTAP集群和节点管理 IP	ITOM 收集器	SNMP、系统日志	UDP 162，UDP 514	来自控制器的 SNMP 陷阱和 Syslog
ITOM 收集器	集群交换机	SNMP	UDP 161	开关监控
集群交换机	ITOM 收集器	SNMP、系统日志	UDP 162，UDP 514	来自交换机的 SNMP 陷阱和 Syslog
ITOM 收集器	StorageGRID节点 IP	HTTPS、SNMP	TCP 443，UDP 161	StorageGRID的 SNMP 监控
StorageGRID节点 IP	ITOM 收集器	SNMP、系统日志	UDP 162，UDP 514	来自StorageGRID的 SNMP 陷阱
ITOM 收集器	Keystone收集器	SSH、HTTPS、SNMP	TCP 22、TCP 443、UDP 161	Keystone Collector 监控和远程管理
ITOM 收集器	本地 DNS	DNS	UDP 53	公共或私有 DNS 服务

ITOM 收集器	选择的 NTP 服务器	NTP	UDP 123	计时

在 **Linux** 系统上安装**Keystone ITOM Collector**

完成几个步骤来安装 ITOM Collector，它会收集您的存储环境中的指标数据。根据您的要求，您可以在 Windows 或 Linux 系统上安装它。

Keystone支持团队提供了一个动态链接来下载 ITOM Collector 安装文件，该文件将在两小时后过期。

要在 Windows 系统上安装 ITOM Collector，请参阅"在 Windows 系统上安装 ITOM Collector"。

按照以下步骤在 Linux 服务器上安装软件：

开始之前

- 验证 Bourne shell 是否可用于 Linux 安装脚本。
- 安装 `vim-common`包以获取 ITOM Collector 安装文件所需的 **xxd** 二进制文件。
- 确保 `sudo package`如果计划以非 root 用户身份运行 ITOM Collector，则安装。

步骤

1. 将 ITOM 收集器安装文件下载到您的 Linux 服务器。
2. 在服务器上打开终端并运行以下命令来更改权限并使二进制文件可执行：
   ```
   # chmod +x <installer_file_name>.bin
   ```
3. 运行命令启动ITOM收集器安装文件：
   ```
   #./<installer_file_name>.bin
   ```
4. 运行安装文件会提示您：
   a. 接受最终用户许可协议 (EULA)。
   b. 输入安装的用户详细信息。
   c. 指定安装父目录。
   d. 选择收集器尺寸。
   e. 如果适用，请提供代理详细信息。

   对于每个提示，都会显示一个默认选项。除非有特殊要求，建议选择默认选项。按 **Enter** 键选择默认选项。安装完成后，会出现一条消息确认 ITOM Collector 已成功安装。

- ITOM Collector 安装文件添加了 `/etc/sudoers`处理服务重启和内存转储。
- 在 Linux 服务器上安装 ITOM Collector 会创建一个名为 **ITOM** 的默认用户，以在没有 root 权限的情况下运行 ITOM Collector。您可以选择其他用户或以root身份运行，但建议使用Linux安装脚本创建的ITOM用户。

下一步是什么？

安装成功后，请联系Keystone支持团队通过 ITOM 支持门户验证 ITOM Collector 是否安装成功。验证后，Keystone支持团队将远程配置 ITOM Collector，包括进一步的设备发现和监控设置，并在配置完成后发送确

认。如有任何疑问或需要更多信息，请联系 keystone.services@netapp.com。

在 Windows 系统上安装Keystone ITOM Collector

通过下载 ITOM Collector 安装文件、运行 InstallShield 向导并输入所需的监控凭据，在 Windows 系统上安装 ITOM Collector。

Keystone支持团队提供了一个动态链接来下载 ITOM Collector 安装文件，该文件将在两小时后过期。

您可以根据需要在 Linux 系统上安装它。要在 Linux 系统上安装 ITOM Collector，请参阅"在 Linux 系统上安装 ITOM Collector"。

按照以下步骤在 Windows 服务器上安装 ITOM 收集器软件：

开始之前

确保在 Windows 服务器的本地安全策略设置中的本地策略/用户权限分配下授予 ITOM Collector 服务*作为服务登录*。

步骤

1. 将 ITOM 收集器安装文件下载到您的 Windows 服务器。
2. 打开安装文件以启动 InstallShield 向导。
3. 接受最终用户许可协议 (EULA)。 InstallShield 向导提取必要的二进制文件并提示您输入凭据。
4. 输入 ITOM Collector 将在其下运行的帐户的凭据：
   - 如果 ITOM Collector 没有监控其他 Windows 服务器，请使用本地系统。
   - 如果 ITOM Collector 正在监控同一域中的其他 Windows 服务器，请使用具有本地管理员权限的域帐户。
   - 如果 ITOM Collector 正在监控不属于同一域的其他 Windows 服务器，请使用本地管理员帐户并使用本地管理员凭据连接到每个资源。您可以选择设置密码以使其不会过期，以减少 ITOM Collector 与其监控资源之间的身份验证问题。
5. 选择收集器尺寸。默认值是根据安装文件推荐的大小。除非您有特殊要求，否则请按照建议的尺寸进行。
6. 选择“下一步”开始安装。您可以使用已填充的文件夹或选择其他文件夹。状态框显示安装进度，然后出现 InstallShield Wizard 完成对话框。

下一步是什么？

安装成功后，请联系Keystone支持团队通过 ITOM 支持门户验证 ITOM Collector 是否安装成功。验证后，Keystone支持团队将远程配置 ITOM Collector，包括进一步的设备发现和监控设置，并在配置完成后发送确认。如有任何疑问或需要更多信息，请联系 keystone.services@netapp.com。

为Keystone配置AutoSupport

使用AutoSupport遥测机制时， Keystone会根据AutoSupport遥测数据计算使用情况。为了达到必要的粒度级别，您应该配置AutoSupport以将Keystone数据纳入ONTAP集群发送的每日支持包中。

关于此任务

在配置AutoSupport以包含Keystone数据之前，您应该注意以下事项。

- 您可以使用ONTAP CLI 编辑AutoSupport遥测选项。有关管理AutoSupport服务和系统（集群）管理员角色的信息，请参阅 "管理AutoSupport概览"和 "集群和 SVM 管理员"。
- 您将子系统包含在每日和每周的AutoSupport包中，以确保为Keystone精确收集数据。有关AutoSupport子系统的信息，请参阅 "AutoSupport子系统是什么"。

步骤

1. 以系统管理员用户身份，使用 SSH 登录Keystone ONTAP集群。有关信息，请参阅 "使用 SSH 访问集群"。
2. 修改日志内容。

   - 对于ONTAP 9.16.1 及更高版本，运行以下命令修改每日日志内容：

     ```
     autosupport trigger modify -node * -autosupport-message
     management.log -basic-additional
     wafl,performance,snapshot,object_store_server,san,raid,snapmirror
     -troubleshooting-additional wafl
     ```

     如果集群采用MetroCluster配置，请运行以下命令：

     ```
     autosupport trigger modify -node * -autosupport-message
     management.log -basic-additional
     wafl,performance,snapshot,object_store_server,san,raid,snapmirror,met
     rocluster -troubleshooting-additional wafl
     ```

   - 对于早期版本的ONTAP ，运行以下命令来修改每日日志内容：

     ```
     autosupport trigger modify -node * -autosupport-message
     management.log -basic-additional
     wafl,performance,snapshot,platform,object_store_server,san,raid,snapm
     irror -troubleshooting-additional wafl
     ```

     如果集群采用MetroCluster配置，请运行以下命令：

     ```
     autosupport trigger modify -node * -autosupport-message management.log
     -basic-additional
     wafl,performance,snapshot,platform,object_store_server,san,raid,snapmirr
     or,metrocluster -troubleshooting-additional wafl
     ```

   - 运行此命令来修改每周日志内容：

```
autosupport trigger modify -autosupport-message weekly
-troubleshooting-additional wafl -node *
```

有关此命令的更多信息，请参见 "system node autosupport trigger modify"。

监控和升级

监控**Keystone Collector** 的健康状况

您可以使用任何支持 HTTP 请求的监控系统来监控Keystone Collector 的健康状况。监测健康状况有助于确保Keystone仪表板上的数据可用。

默认情况下， Keystone健康服务不接受来自 localhost 以外的任何 IP 的连接。 Keystone健康端点是 `/uber/health`，并在端口上监听Keystone Collector 服务器的所有接口 `7777`。查询时，端点将返回一个带有 JSON 输出的 HTTP 请求状态代码作为响应，描述Keystone Collector 系统的状态。 JSON 主体提供了 `is_healthy`属性，它是一个布尔值；以及每个组件的详细状态列表 `component_details`属性。以下是一个例子：

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

返回以下状态代码：

- **200**：表示所有被监控的组件都是健康的
- **503**：表示一个或多个组件不健康
- **403**：表示查询健康状态的 HTTP 客户端不在_允许_列表中，该列表是允许的网络 CIDR 列表。对于此状态，不会返回任何健康信息。 *allow* 列表使用网络 CIDR 方法来控制哪些网络设备被允许查询Keystone健康系统。如果您收到此错误，请从 * Keystone Collector 管理 TUI > 配置 > 健康监控* 将您的监控系统添加到_允许_列表中。

> **Linux** 用户请注意此已知问题：
>
> 问题描述： Keystone Collector 作为使用计量系统的一部分运行许多容器。当使用美国国防信息系统局 (DISA) 安全技术实施指南 (STIG) 策略强化 Red Hat Enterprise Linux 8.x 服务器时，会间歇性地出现 fapolicyd (文件访问策略守护进程) 的已知问题。该问题被认定为"错误 1907870"。 解决方法：在 Red Hat Enterprise 解决之前， NetApp建议您通过以下方式解决此问题：`fapolicyd`**进入宽容模式。在**/`etc/fapolicyd/fapolicyd.conf`，设置值 `permissive = 1`。

查看系统日志

您可以查看Keystone Collector 系统日志来查看系统信息并使用这些日志执行故障排除。 Keystone Collector 使用主机的 *journald* 日志系统，并且可以通过标准 *journalctl* 系统实用程序查看系统日志。您可以使用以下关键服务来检查日志：

- ks-收集器
- ks-健康
- ks-自动更新

主要数据收集服务 *ks-collector* 生成 JSON 格式的日志，其中包含 `run-id`与每个计划数据收集作业相关的属性。以下是标准使用数据收集成功作业的示例：

```
{"level":"info","time":"2022-10-31T05:20:01.831Z","caller":"light-
collector/main.go:31","msg":"initialising light collector with run-id
cdflm0f74cgphgfon8cg","run-id":"cdflm0f74cgphgfon8cg"}
{"level":"info","time":"2022-10-
31T05:20:04.624Z","caller":"ontap/service.go:215","msg":"223 volumes
collected for cluster a2049dd4-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:18.821Z","caller":"ontap/service.go:215","msg":"697 volumes
collected for cluster 909cbacc-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:41.598Z","caller":"ontap/service.go:215","msg":"7 volumes
collected for cluster f7b9a30c-55dc-11ed-9c88-005056b3d66f","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.247Z","caller":"ontap/service.go:215","msg":"24 volumes
collected for cluster a9e2dcff-ab21-11ec-8428-00a098ad3ba2","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.786Z","caller":"worker/collector.go:75","msg":"4 clusters
collected","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.839Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193648.tar.gz type=ontap to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.840Z","caller":"reception/reception.go:76","msg":"File bytes
123425","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}
```


以下是可选性能数据收集成功作业的示例：

```
{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:28","msg":"initialising MySql
service at 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:55","msg":"Opening MySql db
connection at server 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:39","msg":"Creating MySql db
config object"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:69","msg":"initialisi
ng SLA service"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:71","msg":"SLA
service successfully initialised"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"worker/collector.go:217","msg":"Performance
data would be collected for timerange: 2022-10-31T10:24:52~2022-10-
31T10:29:52"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"worker/collector.go:244","msg":"New file
generated: 65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz type=ontap-perf to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:31.386Z","caller":"reception/reception.go:76","msg":"File bytes
17767","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:33.025Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"light-
collector/main.go:88","msg":"exiting","run-id":"cdflm0f74cgphgfon8cg"}
```

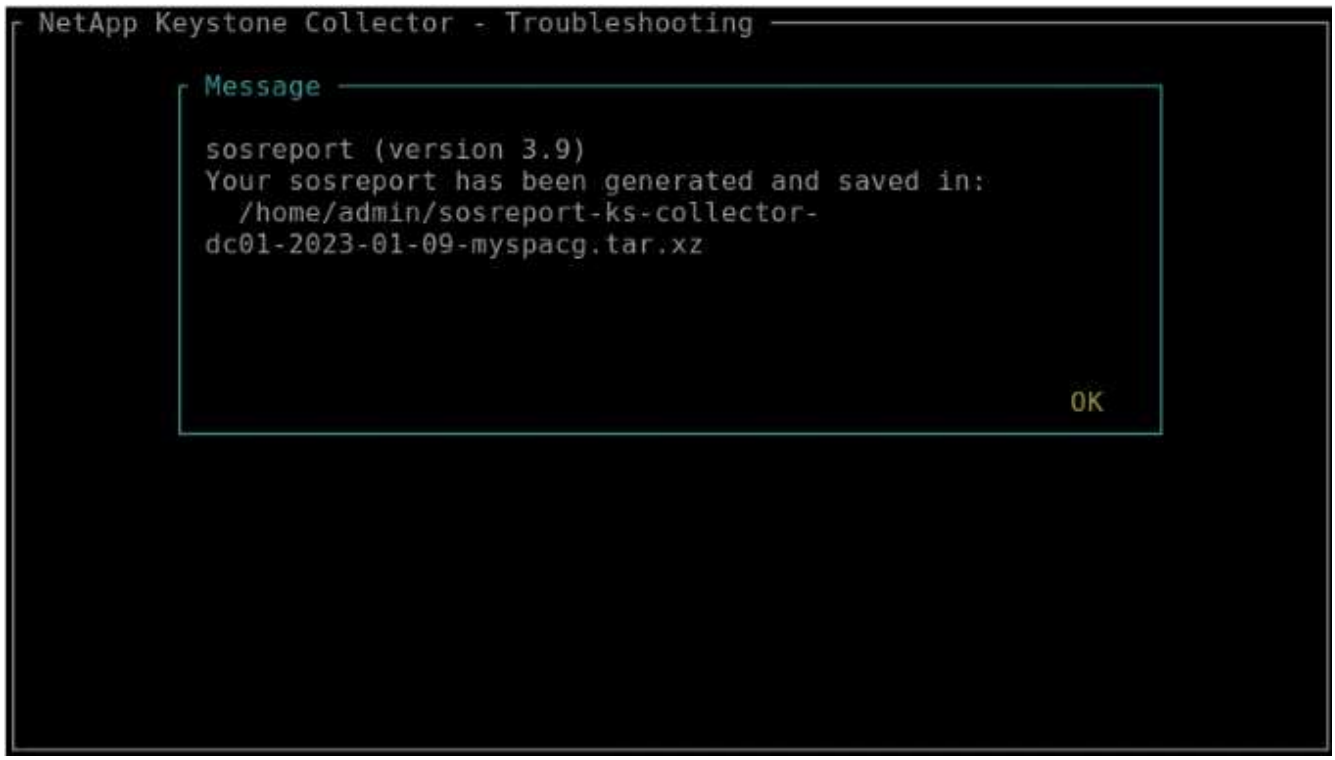
生成并收集支持包

Keystone Collector TUI 使您能够生成支持包并将其添加到服务请求中以解决支持问题。请遵循以下步骤：

步骤

1. 启动Keystone Collector 管理 TUI 实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 转到*故障排除>生成支持包*
   。

3. 生成后，会显示该包的保存位置。使用 FTP、SFTP 或 SCP 连接到该位置并将日志文件下载到本地系统。



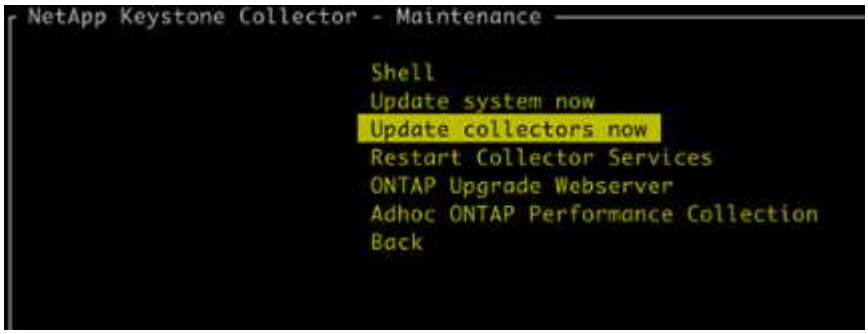
4. 下载文件后，您可以将其附加到Keystone ServiceNow 支持票证。有关提高票数的信息，请参阅 "生成服务请求"。

手动升级**Keystone Collector**

Keystone Collector 中的自动更新功能默认启用，每次发布新版本时都会自动升级Keystone Collector 软件。但是，您可以禁用此功能并手动升级软件。

步骤

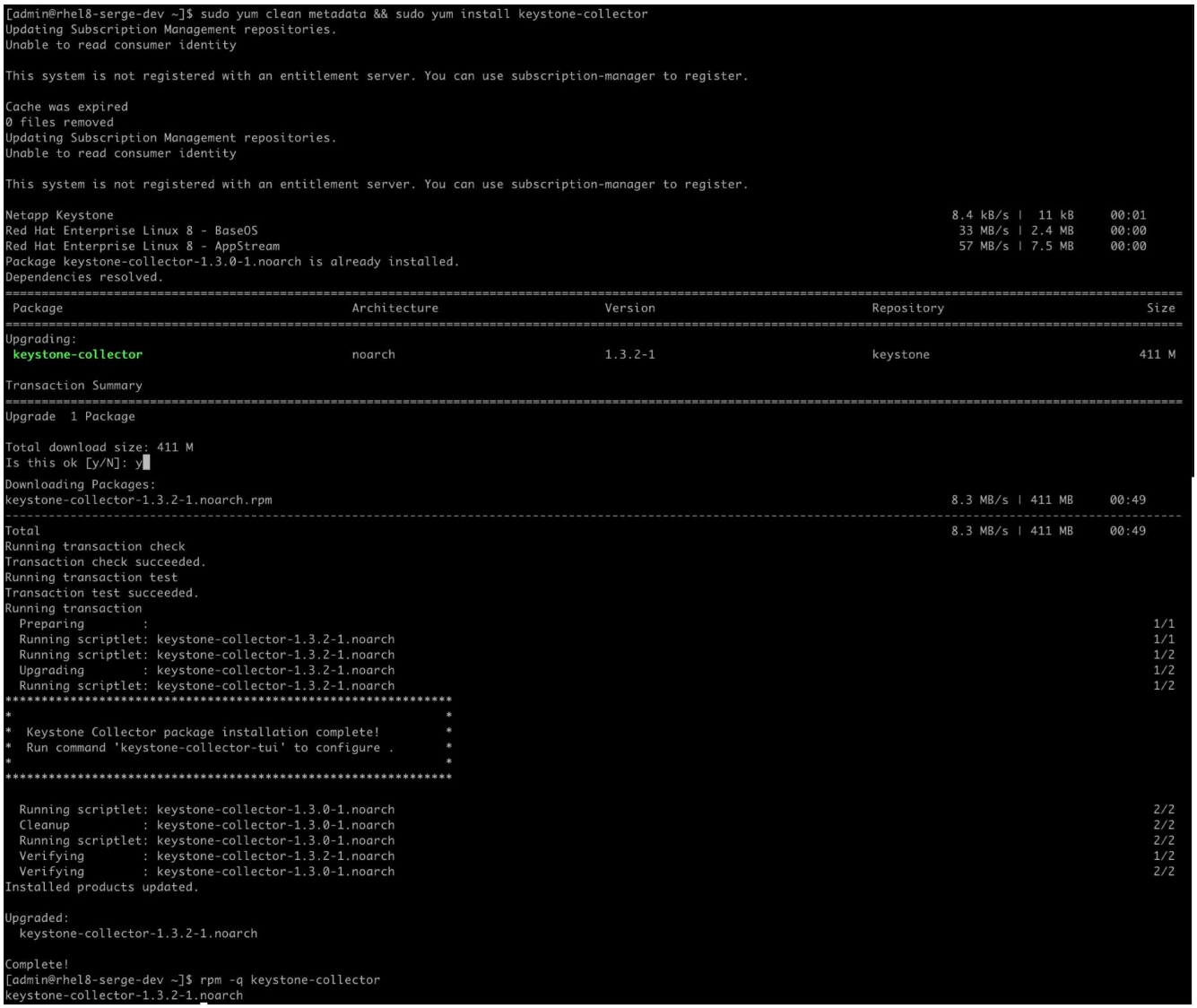
1. 启动Keystone Collector 管理 TUI 实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 在维护屏幕上，选择*立即更新收集器*选项。



或者，运行以下命令来升级版本：

对于 CentOS：

```
sudo yum clean metadata && sudo yum install keystone-collector
```



对于 Debian：

```
sudo apt-get update && sudo apt-get upgrade keystone-collector
```

3. 重新启动Keystone Collector管理TUI，您可以在主屏幕的左上角看到最新版本。

   或者，运行以下命令查看最新版本：

   对于 CentOS：

   ```
   rpm -q keystone-collector
   ```

   对于 Debian：

```
dpkg -l | grep keystone-collector
```

Keystone Collector 安全性

Keystone Collector 包含安全功能，可监控Keystone系统的性能和使用情况指标，而不会危及客户数据的安全。

Keystone Collector 的运行基于以下安全原则：

- 设计隐私- Keystone Collector 收集最少数据来执行使用情况计量和性能监控。有关更多信息，请参阅"为计费而收集的数据" 。这"删除私人数据"默认情况下启用该选项，它可以屏蔽和保护敏感信息。
- 最小特权访问- Keystone Collector 需要最小权限来监控存储系统，从而最大限度地降低安全风险并防止对数据进行任何意外的修改。这种方法符合最小特权原则，增强了受监控环境的整体安全态势。
- 安全的软件开发框架- Keystone在整个开发周期中使用安全的软件开发框架，从而降低风险、减少漏洞并保护系统免受潜在威胁。

安全强化

默认情况下， Keystone Collector 配置为使用安全强化的配置。以下是推荐的安全配置：

- Keystone Collector 虚拟机的操作系统：
  - 符合 CIS Debian Linux 12 Benchmark 标准。在Keystone Collector 管理软件之外对操作系统配置进行任何更改都可能会降低系统安全性。有关更多信息，请参阅"CIS 基准指南" 。
  - 通过自动更新功能自动接收并安装由Keystone Collector 验证的安全补丁。禁用此功能可能会导致未修补的易受攻击的软件。
  - 对从Keystone Collector 收到的更新进行验证。禁用 APT 存储库验证可能会导致自动安装未经授权的补丁，从而可能引入漏洞。
- Keystone Collector 自动验证 HTTPS 证书以确保连接安全。禁用此功能可能会导致模拟外部端点和使用数据泄露。
- Keystone Collector 支持"自定义受信任的 CA"认证。默认情况下，它信任由公共根 CA 签发的证书，这些证书由"Mozilla CA 证书计划"。通过启用额外的受信任 CA， Keystone Collector 可以对出示这些证书的端点的连接启用 HTTPS 证书验证。
- Keystone收集器默认启用“删除私人数据”选项，该选项可以屏蔽和保护敏感信息。有关更多信息，请参阅"限制收集私人数据" 。禁用此选项会导致额外的数据被传送到Keystone系统。例如，它可以包含用户输入的信息（如卷名），这些信息可能被视为敏感信息。

相关信息

- "Keystone Collector 概述"
- "虚拟基础架构要求"
- "配置Keystone收集器"

Keystone收集的用户数据类型

Keystone从Keystone ONTAP和Keystone StorageGRID订阅收集配置、状态和使用信息，以及从托管Keystone Collector 的虚拟机 (VM) 收集遥测数据。如果在Keystone Collector中启用此选项，它只能收集ONTAP的性能数据。

ONTAP数据收集

为ONTAP收集的使用情况数据：了解详情

以下列表是针对ONTAP收集的容量消耗数据的代表性样本：

- 集群
  - 集群UUID
  - 集群名称
  - 序列号
  - 位置（基于ONTAP集群中的值输入）
  - 联系方式
  - 版本
- 节点
  - 序列号
  - 节点名称
- 卷
  - 聚合名称
  - 卷名称
  - 卷实例UUID
  - IsCloneVolume 标志
  - IsFlexGroupConstituent 标志
  - IsSpaceEnforcementLogical 标志
  - IsSpaceReportingLogical 标志
  - Afs 使用的逻辑空间
  - 快照空间百分比
  - PerformanceTierInactiveUserData
  - 性能层级非活动用户数据百分比
  - QoSAdaptivePolicyGroup名称
  - QoS策略组名称
  - 大小
  - 已用
  - 物理已使用
  - 快照使用的大小
  - 类型
  - 音量样式扩展
  - SVM 名称
  - IsVsRoot 标志

- 虚拟服务器
  - 虚拟服务器名称
  - 虚拟服务器UUID
  - 子类型
- 存储聚合
  - 存储类型
  - 聚合名称
  - 聚合 UUID
  - 物理使用
  - 可用大小
  - 大小
  - 使用尺寸
- 聚合对象存储
  - 对象存储名称
  - 对象存储UUID
  - 提供者类型
  - 聚合名称
- 克隆卷
  - FlexClone
  - 大小
  - 已用
  - SVM
  - 类型
  - 父卷
  - 父服务器
  - 是成分
  - 分割估计
  - 状态
  - FlexCloneUsedPercent
- 存储 LUN
  - LUN UUID
  - LUN 名称
  - 大小
  - 已用
  - IsReserved 标志

- IsRequested 标志
- 逻辑单元名称
- QoS策略UUID
- QoS策略名称
- 卷UUID
- 卷名
- SVMUUID
- SVM 名称

- 存储卷
  - 卷实例UUID
  - 卷名
  - SVM名称
  - SVMUUID
  - QoS策略UUID
  - QoS策略名称
  - 容量层级足迹
  - 性能层足迹
  - 总足迹
  - 分层策略
  - IsProtected 标志
  - IsDestination 标志
  - 已用
  - 物理已使用
  - 克隆父UUID
  - Afs 使用的逻辑空间
- QoS 策略组
  - 政策组
  - QoS策略UUID
  - 最大吞吐量
  - 最小吞吐量
  - 最大吞吐量IOPS
  - 最大吞吐量MBps
  - 最小吞吐量IOPS
  - 最小吞吐量MBps

    - IsShared 标志
- ONTAP自适应 QoS 策略组
    - QoS策略名称
    - QoS策略UUID
    - 峰值IOPS
    - PeakIOPS分配
    - 绝对最小IOPS
    - 预期IOPS
    - 预期IOPS分配
    - 块大小
- 足迹
    - SVM
    - 卷
    - 总足迹
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - 节点
    - 聚合
    - LIF
    - 配置复制
    - 连接
    - 集群
    - 卷
- MetroCluster集群
    - 集群UUID
    - 集群名称
    - 远程集群UUID
    - 远程集群用户名
    - 本地配置状态
    - 远程配置状态
- MetroCluster节点
    - DR镜像状态
    - 集群间 LIF
    - 节点可达性

- 灾难恢复伙伴节点
- DR辅助合作伙伴节点
- DR、DR Aux 和 HA 节点对称关系
- 自动计划外切换

- MetroCluster配置复制
  - 远程心跳
  - 上次发送的心跳
  - 收到的最后一个心跳
  - 虚拟服务器流
  - 集群流
  - 存储
  - 正在使用的存储量
- MetroCluster调解器
  - 调解员地址
  - 中介端口
  - 中介器已配置
  - 中介者可达
  - 模式
- 收集器可观察性指标
  - 收集时间
  - 已查询Active IQ Unified Manager API 端点
  - 响应时间
  - 记录数
  - AIQUM实例IP
  - 收集器实例 ID

为ONTAP收集的性能数据：了解详情

以下列表是针对ONTAP收集的性能数据的代表性示例：

- 集群名称
- 集群 UUID
- 对象 ID
- 卷名
- 卷实例 UUID
- SVM
- 虚拟服务器UUID
- 节点串行
- ONTAP版本
- AIQUM 版本
- 聚合
- 聚合UUID
- 资源键
- 时间戳
- 每TB IOPS
- 延迟
- 读取延迟
- 写入MBps
- QoS最小吞吐量延迟
- QoSNBladeLatency
- 已使用净空
- 缓存未命中率
- 其他延迟
- QoS聚合延迟
- IOPS
- QoS网络延迟
- 可用操作
- 写入延迟
- QoS云延迟
- QoS集群互连延迟
- 其他MBps
- QoS延迟

- QoS刀片延迟
- 利用率
- 读取IOPS
- MBps
- 其他IOPS
- QoS策略组延迟
- 读取MBps
- QoS同步SnapMirror延迟
- 系统级数据
  - 写入/读取/其他/总 IOPS
  - 写入/读取/其他/总吞吐量
  - 写入/读取/其他/总延迟
- 写入IOPS

****因限制私人数据访问而移除的项目列表：了解详情****

当在Keystone Collector 上启用“删除私有数据”选项时， ONTAP的以下使用信息将被消除。默认情况下，此选项处于启用状态。

- 集群名称
- 集群位置
- 集群联系人
- 节点名称
- 聚合名称
- 卷名称
- QoSAdaptivePolicyGroup名称
- QoS策略组名称
- SVM 名称
- 存储 LUN 名称
- 聚合名称
- 逻辑单元名称
- SVM 名称
- AIQUM实例IP
- FlexClone
- 远程集群名称

StorageGRID数据收集

为StorageGRID收集的使用情况数据：了解详情

以下列表是 `Logical Data`为StorageGRID收集：

- StorageGRIDID
- 帐户 ID
- 帐户名称
- 账户配额字节数
- 存储桶名称
- 桶对象计数
- 桶数据字节数

以下列表是 `Physical Data`为StorageGRID收集：

- StorageGRIDID
- 节点ID
- 站点 ID
- 站点名称
- 实例
- StorageGRID存储利用率字节数
- StorageGRID存储利用率元数据字节

以下列表是 `Availability/Uptime Data`为StorageGRID收集：

- SLA 正常运行时间百分比

因限制私人数据访问而移除的项目列表：了解详情

当在Keystone Collector 上启用“删除私人数据”选项时， StorageGRID的以下使用信息将被消除。默认情况下，此选项处于启用状态。

- 帐户名称
- 存储桶名称
- 站点名称
- 实例/节点名称

遥测数据收集

从Keystone Collector VM 收集的遥测数据：了解详情

以下列表是针对Keystone系统收集的遥测数据的代表性样本：

- 系统信息
  - 操作系统名称
  - 操作系统版本
  - 操作系统 ID
  - 系统主机名
  - 系统默认IP地址
- 系统资源使用情况
  - 系统正常运行时间
  - CPU 核心数
  - 系统负载（1分钟、5分钟、15分钟）
  - 总内存
  - 释放内存
  - 可用内存
  - 共享内存
  - 缓冲存储器
  - 缓存内存
  - 总掉期
  - 免费掉期
  - 缓存交换
  - 磁盘文件系统名称
  - 磁盘大小
  - 使用的磁盘
  - 磁盘可用
  - 磁盘使用率
  - 磁盘挂载点
- 已安装的软件包
- 收集器配置
- 服务日志
  - 来自Keystone服务的服务日志

Keystone处于私人模式

了解Keystone （私人模式）

Keystone提供一种_私有_部署模式（也称为_暗站_），以满足您的业务和安全需求。此模式适用于连接受限的组织。

NetApp提供专门的Keystone STaaS 部署，适用于互联网连接有限或没有互联网连接的环境（也称为暗站）。这些是安全或隔离的环境，其中外部通信由于安全、合规性或操作要求而受到限制。

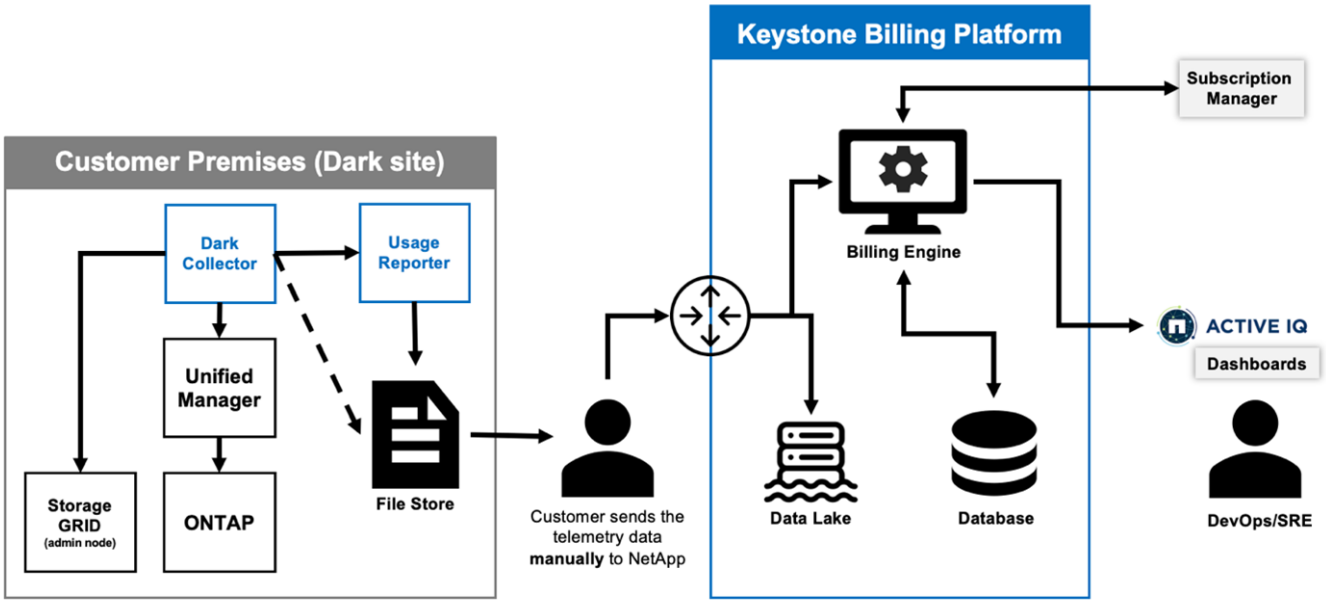
对于NetApp Keystone来说，为暗站提供服务意味着以尊重这些环境约束的方式提供Keystone灵活存储订阅服务。这涉及：

- 本地部署： Keystone可以在隔离环境中独立配置，确保无需互联网连接或外部人员进行设置访问。
- 离线操作：所有存储管理功能（包括健康检查和计费）均可离线操作。
- 安全性和合规性： Keystone确保部署满足暗网的安全性和合规性要求，其中可能包括高级加密、安全访问控制和详细的审计功能。
- 帮助和支持： NetApp提供全天候全球支持，并为每个帐户指派一名专门的Keystone成功经理来提供帮助和故障排除。

Keystone Collector 可以配置为不受连接限制，也称为_标准_模式。要了解更多信息，请参阅"了解Keystone Collector"。

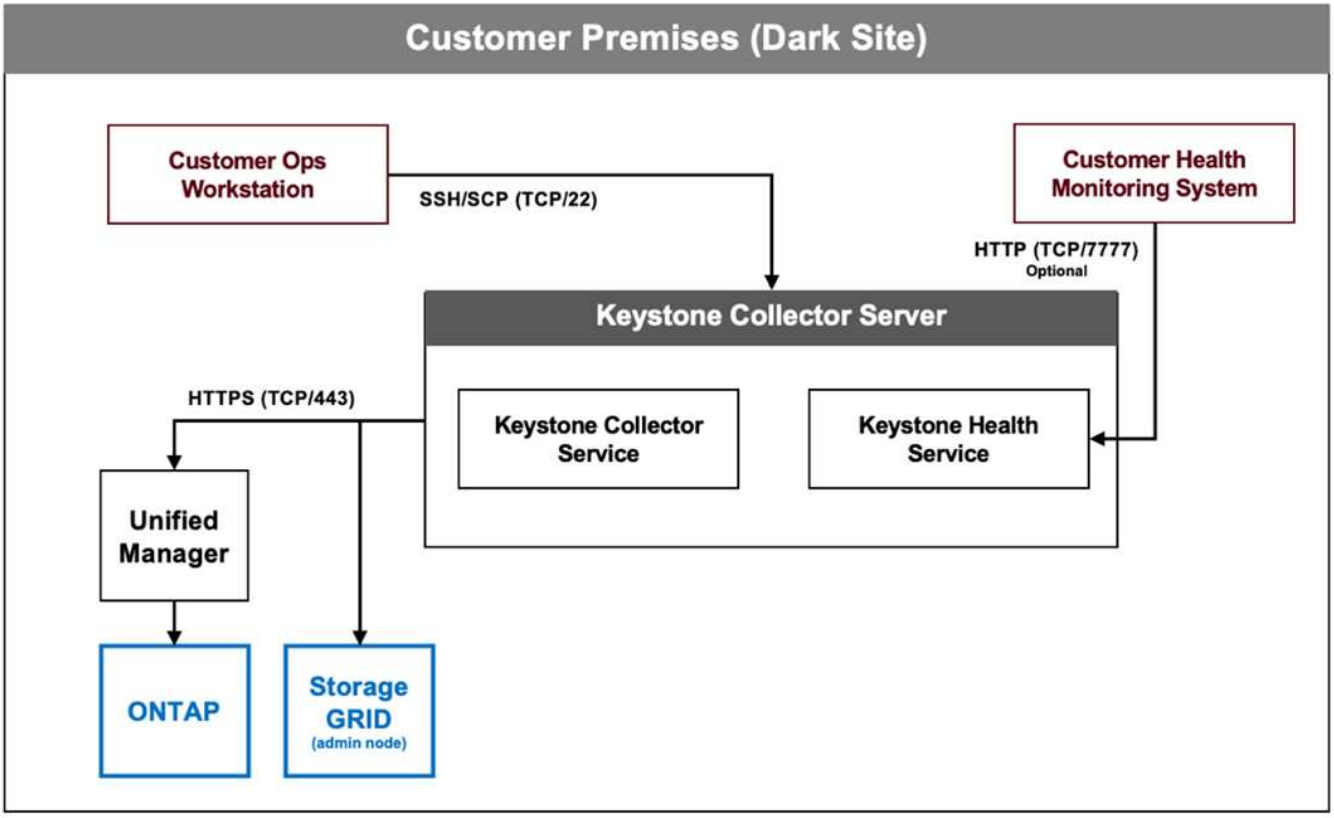
私人模式下的Keystone Collector

Keystone Collector 负责定期从存储系统收集使用情况数据，并将指标导出到离线使用情况报告器和本地文件存储。生成的文件以加密和纯文本格式创建，经过验证检查后由用户手动转发给NetApp 。收到后，NetApp 的Keystone计费平台会验证和处理这些文件，并将其集成到计费和订阅管理系统中以计算每月的费用。



服务器上的Keystone Collector 服务负责定期收集使用数据、处理这些信息并在服务器本地生成使用文件。健康

服务进行系统健康检查，并旨在与客户使用的健康监测系统进行交互。用户可以离线访问这些报告，以便进行验证并帮助解决问题。



准备以私有模式安装Keystone Collector

在没有互联网访问的环境（也称为_暗站_或_私人模式_）中安装Keystone Collector 之前，请确保您的系统已准备好必要的软件并满足所有必需的先决条件。

VMware vSphere 的要求

- 操作系统：VMware vCenter 服务器和 ESXi 8.0 或更高版本
- 核心：1 个 CPU
- 内存：2 GB
- 磁盘空间：20 GB vDisk

Linux 要求

- 操作系统（选择一项）：
  - Red Hat Enterprise Linux (RHEL) 8.6 或任何更高版本的 8.x 系列
  - Red Hat Enterprise Linux 9.0 或更高版本
  - Debian 12
- 核心：2 CPU

- 内存：4 GB
- 磁盘空间：50 GB vDisk
  - 至少 2 GB 可用空间 `/var/lib/`
  - 至少 48 GB 可用空间 `/opt/netapp`

同一台服务器还应该安装以下第三方软件包。如果通过存储库可用，这些包将作为先决条件自动安装：

- RHEL 8.6+ (8.x)
  - python3 >=v3.6.8, python3 <=v3.9.13
  - podman
  - 求救
  - yum实用程序
  - python3-dnf-插件-版本锁
- RHEL 9.0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - podman
  - 求救
  - yum实用程序
  - python3-dnf-插件-版本锁
- Debian v12
  - python3 >= v3.9.0, python3 <= v3.12.0
  - podman
  - sos报告

网络要求

Keystone Collector 的网络要求包括以下内容：

- Active IQ Unified Manager （Unified Manager）9.10 或更高版本，在启用了 API 网关功能的服务器上配置。
- Keystone Collector 服务器应该可以通过端口 443 (HTTPS) 访问 Unified Manager 服务器。
- 应该为 Unified Manager 服务器上的Keystone Collector 设置具有应用程序用户权限的服务帐户。
- 不需要外部互联网连接。
- 每个月从Keystone Collector 导出一个文件并通过电子邮件发送给NetApp支持团队。如需了解如何联系支持团队的更多信息，请参阅 "获取有关Keystone的帮助"。

以私人模式安装**Keystone Collector**

完成几个步骤即可在没有互联网访问的环境中安装Keystone Collector，也称为_暗站_或_私人模式_。这种类型的安装非常适合您的安全站点。

根据您的要求，您可以在 VMware vSphere 系统上部署Keystone Collector，也可以将其安装在 Linux 系统上。按照与您选择的选项相对应的安装步骤进行操作。

在 **VMware vSphere** 上部署

按照下面的步骤进行操作：

1. 从以下位置下载 OVA 模板文件 "NetApp Keystone门户网站"。
2. 有关使用 OVA 文件部署Keystone收集器的步骤，请参阅"部署 OVA 模板"。

在 **Linux** 上安装

根据 Linux 发行版， Keystone Collector 软件使用提供的 .deb 或 .rpm 文件安装在 Linux 服务器上。

按照以下步骤在 Linux 服务器上安装该软件：

1. 下载或传输Keystone Collector 安装文件到 Linux 服务器：

   ```
   keystone-collector-<version>.noarch.rpm
   ```

2. 在服务器上打开终端并运行以下命令开始安装。

   - 使用 **Debian** 软件包

     ```
     dpkg -i keystone-collector_<version>_all.deb
     ```

   - 使用 **RPM** 文件

     ```
     yum install keystone-collector-<version>.noarch.rpm
     ```

     或

   ```
   rpm -i keystone-collector-<version>.noarch.rpm
   ```

3. 进入 `y`当提示安装包时。

以私有模式配置**Keystone Collector**

完成一些配置任务，以使Keystone Collector 能够在没有互联网访问的环境中收集使用数据，也称为_暗站_或_私人模式_。这是一次性活动，用于激活所需组件并将其与您的存储环境关联起来。配置完成后， Keystone Collector 将监控由Active IQ Unified Manager管理的所有ONTAP集群。

Keystone Collector 为您提供了Keystone Collector 管理终端用户界面 (TUI) 实用程序来执行配置和监控活动。您可以使用各种键盘控制（例如 Enter 和箭头键）来选择选项并浏览此 TUI。

步骤

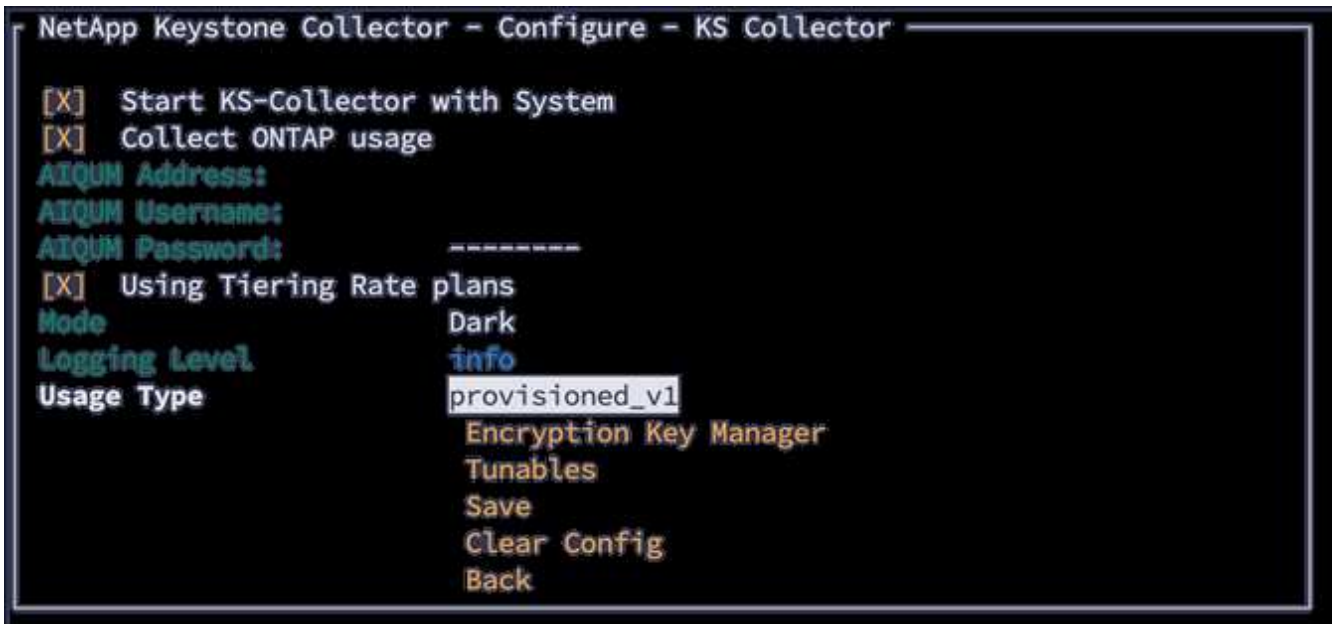
1. 启动Keystone Collector 管理 TUI 实用程序：

   ```
   keystone-collector-tui
   ```

2. 转到*配置>高级*。
3. 切换*暗站模式*选项。

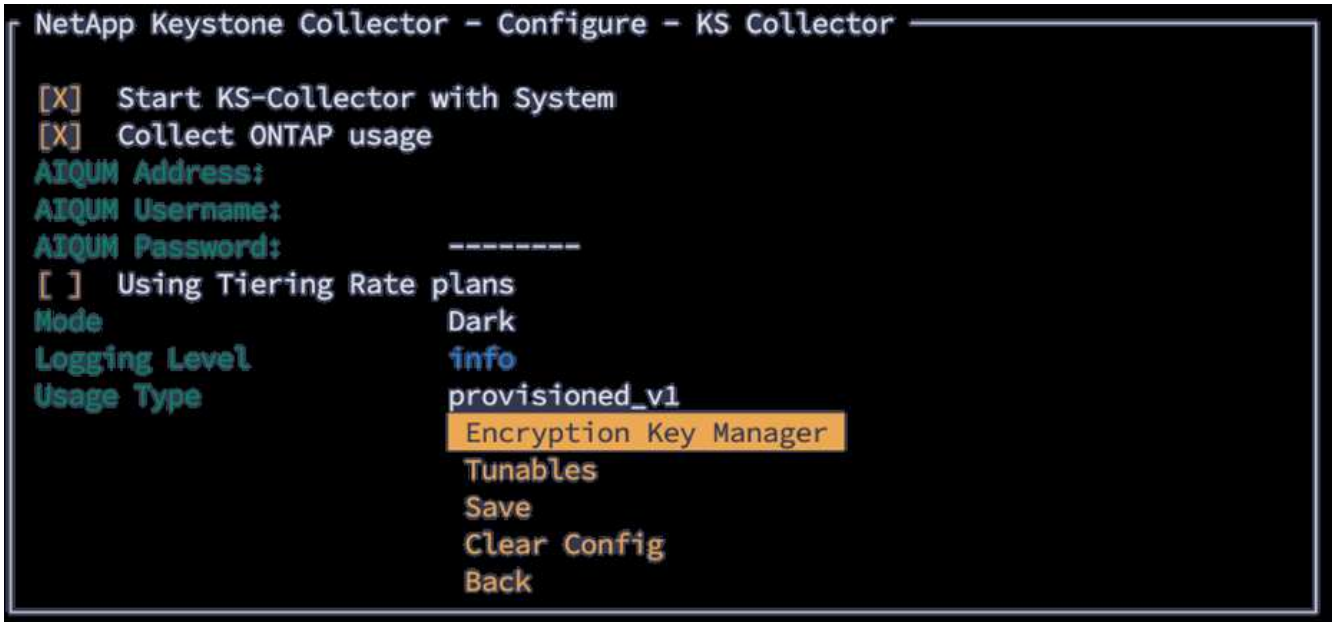
4. 选择*保存*。
5. 转到*配置> KS-Collector*来配置Keystone Collector。
6. 切换*使用系统启动 KS 收集器*字段。
7. 切换“收集ONTAP使用情况”字段。添加Active IQ Unified Manager （Unified Manager）服务器和用户帐户的详细信息。
8. 可选：如果订阅需要数据分层，请切换*使用分层费率计划*字段。
9. 根据购买的订阅类型，更新*使用类型*。

> 配置之前，请确认与NetApp订阅相关的使用类型。



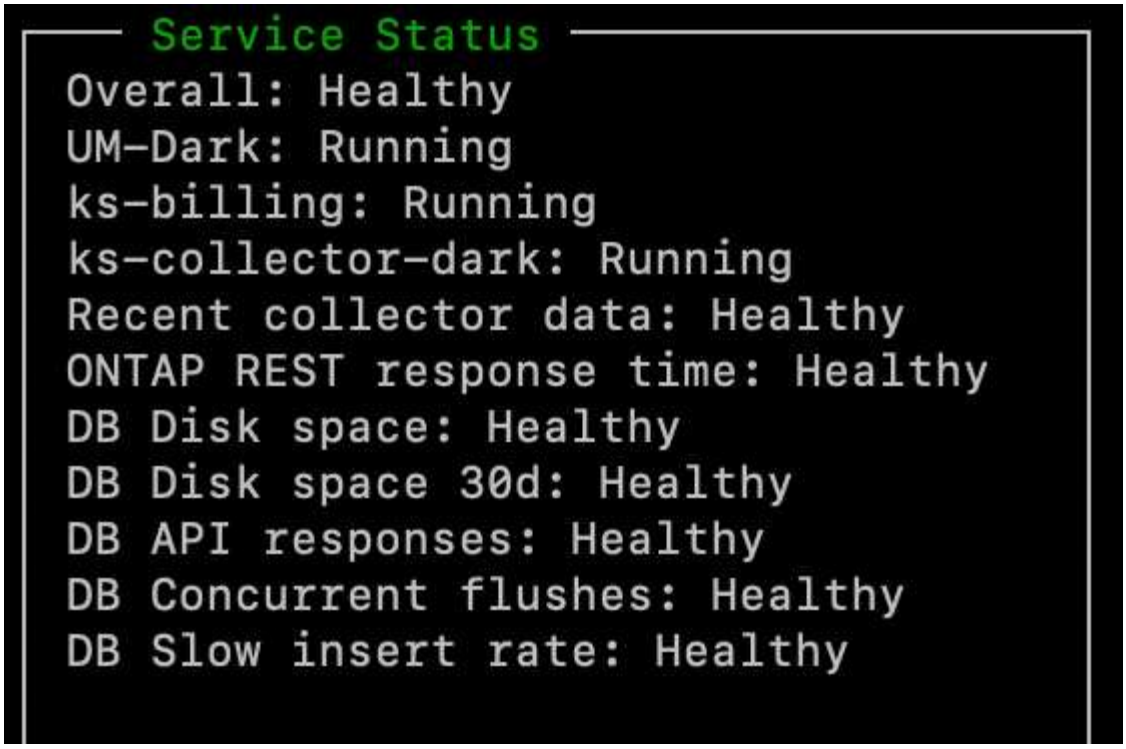
10. 选择*保存*。
11. 转到*配置> KS-Collector*以生成Keystone Collector 密钥对。

12. 转到*加密密钥管理器*并按 Enter。



13. 选择*生成收集器密钥对*并按 Enter。

14. 通过返回 TUI 主屏幕并验证 服务状态 信息，确保Keystone Collector 处于健康状态。系统应显示服务处于*总体：健康*状态。等待最多 10 分钟，如果在此期间后整体状态仍然不健康，请查看之前的配置步骤并联系NetApp支持团队。



15. 通过选择主屏幕上的“退出到 Shell”选项退出Keystone Collector 管理 TUI。
16. 检索生成的公钥：

    ```
    ~/collector-public.pem
    ```

17. 将此文件通过电子邮件发送至 ng-keystone-secure-site-upload@netapp.com（用于安全的非 USPS 站点）或 ng-keystone-secure-site-usps-upload@netapp.com（用于安全的 USPS 站点）。

导出使用情况报告

您应该在每个月末向NetApp发送每月使用情况摘要报告。您可以手动生成此报告。

请按照以下步骤生成使用情况报告：

1. 转到Keystone Collector TUI 主屏幕上的 导出使用情况。
2. 收集文件并将其发送至 ng-keystone-secure-site-upload@netapp.com（用于安全的非 USPS 站点）或发送至 ng-keystone-secure-site-usps-upload@netapp.com（用于安全的 USPS 站点）。

   Keystone Collector 会生成一个明文文件和一个加密文件，需要手动将其发送给NetApp。清晰的文件报告包含以下可供客户验证的详细信息。

```
node_serial,derived_service_level,usage_tib,start,duration_seconds
123456781,extreme,25.0,2024-05-27T00:00:00,86400
123456782,premium,10.0,2024-05-27T00:00:00,86400
123456783,standard,15.0,2024-05-27T00:00:00,86400

<Signature>
31b3d8eb338ee319ef1

-----BEGIN PUBLIC KEY-----
31b3d8eb338ee319ef1
-----END PUBLIC KEY-----
```

升级**ONTAP**

Keystone Collector 支持通过 TUI 进行ONTAP升级。

按照以下步骤升级ONTAP：

1. 转到*维护> ONTAP升级 Web 服务器*。
2. 将ONTAP升级映像文件复制到 **/opt/netapp/ontap-upgrade/**，然后选择 **Start Webserver** 启动 Web 服务器。

3. 前往 `http://<collector-ip>:8000`使用网络浏览器获取升级帮助。

重启**Keystone**收集器

您可以通过 TUI 重新启动Keystone Collector 服务。在 TUI 中转到 维护 **>** 重新启动收集器 服务。这将重新启动所有收集器服务，并且可以从 TUI 主屏幕监控它们的状态。

以私人模式监控**Keystone Collector** 的健康状况

您可以使用任何支持 HTTP 请求的监控系统来监控Keystone Collector 的健康状况。

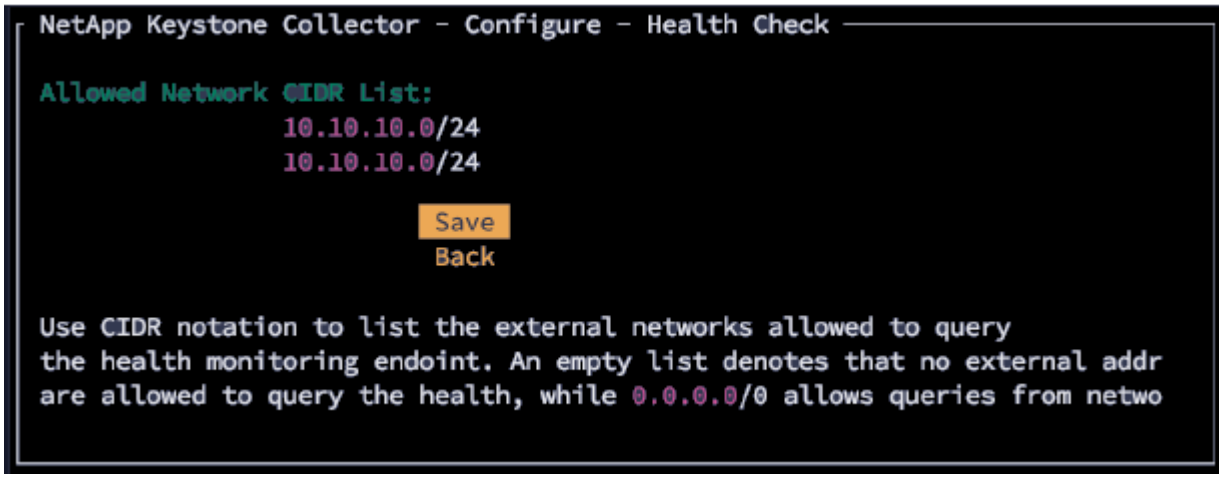
默认情况下， Keystone健康服务不接受来自 localhost 以外的任何 IP 的连接。 Keystone健康端点是 `/uber/health`，并在端口上监听Keystone Collector 服务器的所有接口 `7777`。查询时，端点将返回一个带有 JSON 输出的 HTTP 请求状态代码作为响应，描述Keystone Collector 系统的状态。 JSON 主体提供了 `is_healthy`属性，它是一个布尔值；以及每个组件的详细状态列表 `component_details`属性。以下是一个例子：

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

返回以下状态代码：

- **200**：表示所有被监控的组件都是健康的
- **503**：表示一个或多个组件不健康
- **403**：表示查询健康状态的 HTTP 客户端不在_允许_列表中，该列表是允许的网络 CIDR 列表。对于此状态，不会返回任何健康信息。

  allow 列表使用网络 CIDR 方法来控制哪些网络设备被允许查询Keystone健康系统。如果您收到 403 错误，请从 * Keystone Collector 管理 TUI > 配置 > 健康监控* 将您的监控系统添加到_允许_列表中。

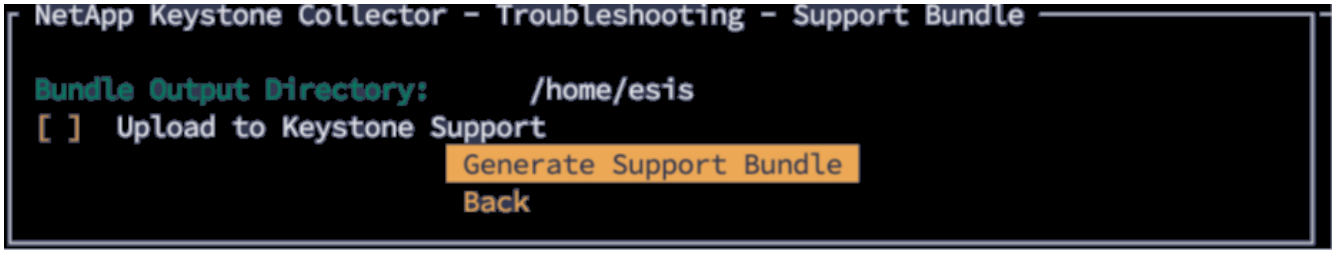


生成并收集支持包

要解决Keystone Collector 的问题，您可以与NetApp支持人员合作，他们可能会要求提供 *.tar* 文件。您可以通过Keystone Collector 管理 TUI 实用程序生成此文件。

按照以下步骤生成 *.tar* 文件：

1. 转到*故障排除>生成支持包*。
2. 选择保存包的位置，然后单击“生成支持包”。



这个过程创造了 `tar`位于上述位置的软件包可以与NetApp共享，以便解决问题。

3. 下载文件后，您可以将其附加到Keystone ServiceNow 支持票证。有关提高票数的信息，请参阅 "生成服务请求"。