设置和配置Keystone

Keystone

NetApp
January 14, 2026

目录

设置和配置Keystone

要求

Keystone Collector 的虚拟基础设施要求

在安装Keystone收集器之前、VMware vSphere系统必须满足多项要求。

Keystone收集器服务器**VM**的前提条件：

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

其他要求

确保满足以下通用要求：

网络要求

下表列出了Keystone收集器的网络连接要求。

Keystone收集器需要Internet连接。您可以通过默认网关(通过NAT)或HTTP代理直接路由来提供Internet连接。此处介绍了这两种变体。

源	目标	服务	协议和端口	类别	目的
Keystone收集器(适用于Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	必需(如果使用Keystone ONTAP)	ONTAP的Keystone收集器使用情况指标收集
Keystone收集器(适用于Keystone StorageGRID)	StorageGRID 管理节点	HTTPS	TCP 443	必需(如果使用Keystone StorageGRID)	StorageGRID的Keystone收集器使用情况指标收集
Keystone收集器(通用)	Internet (根据后面提供的URL要求)	HTTPS	TCP 443	必填(Internet连接)	Keystone收集器软件、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	必填(Internet连接)	Keystone收集器软件、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	必填	DNS解析
Keystone收集器(通用)	客户NTP服务器	NTP	UDP 123	必填	时间同步
Keystone收集器(适用于Keystone ONTAP)	Unified Manager	MySQL	TCP 3306	可选功能	Keystone收集器的性能指标集合
Keystone收集器(通用)	客户监控系统	HTTPS	TCP 7777	可选功能	Keystone收集器运行状况报告
客户的运营工作站	Keystone收集器	SSH	TCP 22	管理	访问Keystone收集器管理
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/回复	可选功能	用于更新ONTAP固件的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、从而无法收集Keystone收集器的性能指标。有关详细信息，请参见 "ONTAP 要求"。

URL访问

Keystone收集器需要访问以下Internet主机：

Address	reason
https://keystone.netapp.com	Keystone收集器软件更新和使用情况报告
https://support.netapp.com	NetApp总部提供计费信息和AutoSupport 交付

Keystone Collector 的 Linux 系统要求

使用所需软件准备Linux系统可确保Keystone收集器的精确安装和数据收集。

确保Linux和Keystone收集器服务器VM具有这些配置。

Linux服务器：

- 操作系统：以下任一操作系统：
  - 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)

- 首字母缩略语时间同步
- 访问标准Linux软件存储库

同一台服务器还应具有以下第三方软件包：

- podman (POD管理器)
- SOS
- 按时间顺序执行
- Python 3（3.9.14 至 3.11.8）

Keystone收集器服务器**VM**：

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

其他要求

确保满足以下通用要求：

网络要求

下表列出了Keystone收集器的网络连接要求。

Keystone收集器需要Internet连接。您可以通过默认网关(通过NAT)或HTTP代理直接路由来提供Internet连接。此处介绍了这两种变体。

源	目标	服务	协议和端口	类别	目的
Keystone收集器(适用于Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	必需(如果使用Keystone ONTAP)	ONTAP的Keystone收集器使用情况指标收集
Keystone收集器(适用于Keystone StorageGRID)	StorageGRID 管理节点	HTTPS	TCP 443	必需(如果使用Keystone StorageGRID)	StorageGRID的Keystone收集器使用情况指标收集
Keystone收集器(通用)	Internet (根据后面提供的URL要求)	HTTPS	TCP 443	必填(Internet连接)	Keystone收集器软件、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	必填(Internet连接)	Keystone收集器软件、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	必填	DNS解析
Keystone收集器(通用)	客户NTP服务器	NTP	UDP 123	必填	时间同步
Keystone收集器(适用于Keystone ONTAP)	Unified Manager	MySQL	TCP 3306	可选功能	Keystone收集器的性能指标集合
Keystone收集器(通用)	客户监控系统	HTTPS	TCP 7777	可选功能	Keystone收集器运行状况报告
客户的运营工作站	Keystone收集器	SSH	TCP 22	管理	访问Keystone收集器管理
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/回复	可选功能	用于更新ONTAP固件的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、从而无法收集Keystone收集器的性能指标。有关详细信息，请参见 "ONTAP 要求"。

URL访问

Keystone收集器需要访问以下Internet主机：

Address	reason
https://keystone.netapp.com	Keystone收集器软件更新和使用情况报告
https://support.netapp.com	NetApp总部提供计费信息和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

如果您只想通过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、请参见以下链接：
   - "使用System Manager在新集群上配置ONTAP"
   - "使用命令行界面设置集群"
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"。
   - * Web UUI *
     i. 使用默认凭据登录到ONTAP系统管理器。要了解更多信息，请参阅 "使用 System Manager 进行集群管理"。
     ii. 创建一个具有"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 *来启用密码身份验证。
   - **CLI**
     i. 使用默认凭据登录到ONTAP命令行界面。要了解更多信息，请参阅 "使用CLI进行集群管理"。
     ii. 创建一个具有"readOnly"角色和"http"应用程序类型的ONTAP用户、并启用密码身份验证。要了解有关身份验证的更多信息，请参见 "启用ONTAP帐户密码访问"。

如果要通过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、请参见以下链接：
   - "在VMware vSphere系统上安装Unified Manager"
   - "在 Linux 系统上安装 Unified Manager"
2. 确保已将ONTAP 集群添加到Unified Manager中。有关添加集群的信息、请参见 "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、请参见 "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到Unified Manager Web UI。请参见 "访问Unified Manager Web UI"。
   b. 使用为Keystone收集器创建服务帐户 `Operator` 用户角色。Keystone收集器服务API使用此服务帐户与Unified Manager进行通信并收集使用情况数据。请参见 "添加用户"。
   c. 创建 `Database` 用户帐户、使用 `Report Schema` 角色。收集性能数据时需要此用户。请参见 "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、从而无法收集Keystone ONTAP的性能数据。可以修改此配置、并使用Unified Manager维护控制台上的选项使此连接可供其他主机使用 `Control access to MySQL port 3306` 。有关信息，请参见 "其他菜单选项"。

4. 在Unified Manager中启用API网关。Keystone收集器可利用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命令行界面运行几个命令来启用API网关。

   Web UI

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

   命令行界面

   要通过Unified Manager命令行界面启用API网关、请执行以下步骤：

   a. 在Unified Manager服务器上、开始SSH会话并登录到Unified Manager命令行界面。
   `um cli login -u <*umadmin*>`有关CLI命令的信息、请参见 "支持的 Unified Manager 命令行界面命令"。

   b. 验证是否已启用API网关。
   `um option list api.gateway.enabled`答 `true` 值表示已启用API网关。

   c. 如果返回的值为 `false`、运行以下命令：
   `um option set api.gateway.enabled=true`

   d. 重新启动Unified Manager服务器：

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

StorageGRID

在StorageGRID 上安装Keystone收集器需要以下配置。

- StorageGRID `11.6.0` 或更高版本。有关升级StorageGRID 的信息、请参见 "Upgrade StorageGRID software： 概述"。
- 应创建StorageGRID 本地管理员用户帐户以收集使用情况数据。Keystone收集器服务使用此服务帐户通过管理员节点API与StorageGRID 进行通信。

  步骤

  a. 登录到网格管理器。请参见 "登录到网格管理器"。
  b. 使用创建本地管理组 `Access mode: Read-only`。请参见 "创建管理组"。
  c. 添加以下权限：
     - 租户帐户
     - 维护
     - 指标查询
  d. 创建Keystone服务帐户用户并将其与管理组关联。请参见 "管理用户"。

安装Keystone收集器

在VMware vSphere系统上部署Keystone收集器

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

向导部署此模板、验证证书的完整性以及验证虚拟机是否已准备就绪。

部署**OVA**模板

请按照以下步骤操作：

步骤

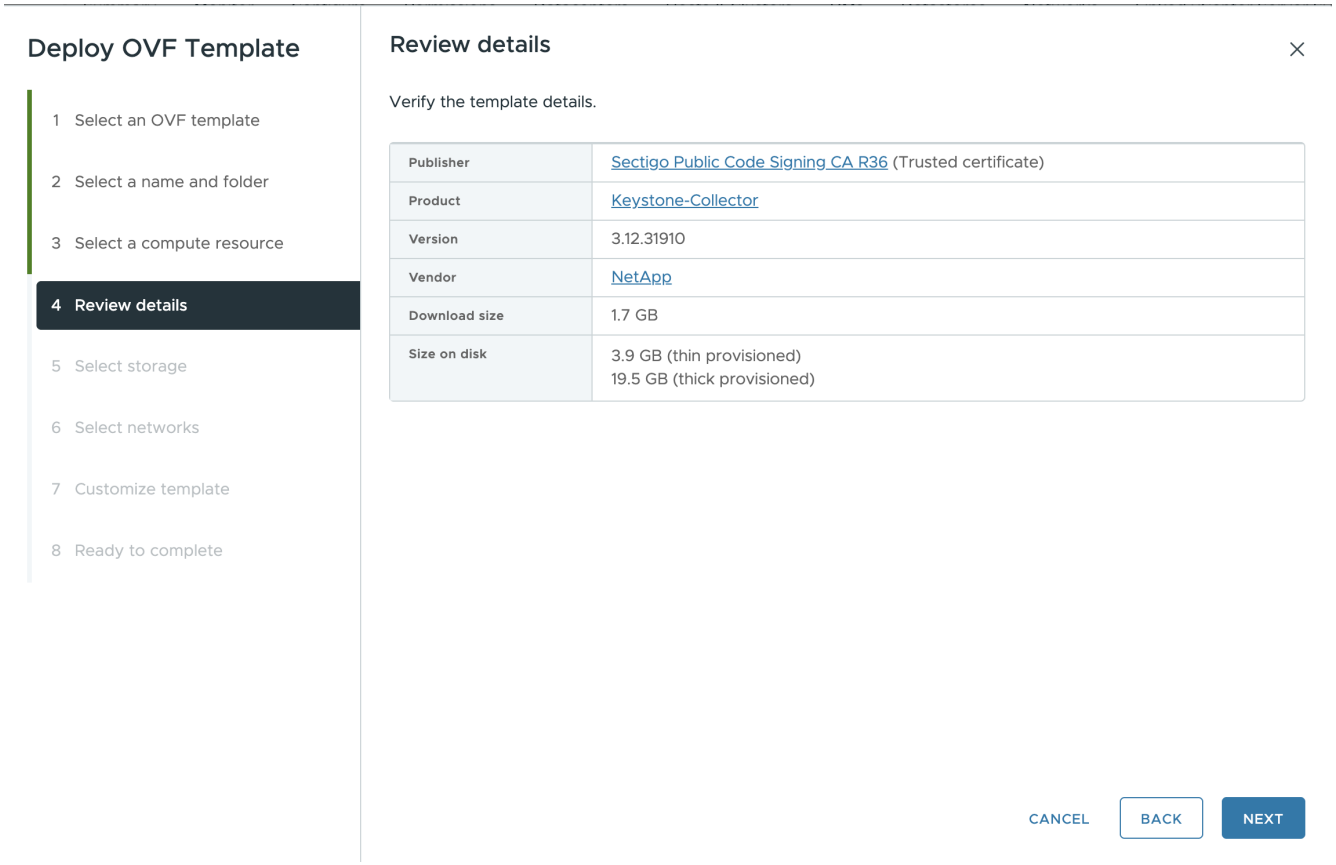
1. 从下载OVA文件 "此链接。" 并将其存储在VMware vSphere系统上。
2. 在VMware vSphere系统上、导航到*虚拟机和模板*视图。
3. 右键单击虚拟机(VM)(如果不使用VM文件夹、则为数据中心)所需的文件夹、然后选择*部署OVF模板*。
4. 在*部署OVF模板*向导的_Step 1_上、单击*选择和OVF模板*以选择已下载的 `KeystoneCollector-latest.ova` 文件
5. 在_Step 2_上、指定VM名称并选择VM文件夹。
6. 在_Step 3_上、指定运行虚拟机所需的计算资源。
7. 在步骤 4：检查细节中，验证 OVA 文件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

   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. 按照中的步骤进行操作 `Resolution` 部分： 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_Step 5_上、指定用于存储VM的位置。
9. 在_Step 6_上、选择虚拟机要使用的目标网络。
10. 在_Step 7 Customize templ板_上、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、应用作启动凭据、以便首次访问VMware vSphere系统。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、使用值24表示子网掩码255.255.255.0。

11. 在*部署OVF模板*向导的_Step 8 Ready to Complete_上、查看配置并验证您是否已正确设置OVA部署的参数。

从模板部署VM并打开其电源后、打开与VM的SSH会话并使用临时管理员凭据登录以验证VM是否已做好配置准备。

初始系统配置

在VMware vSphere系统上执行以下步骤、以便对通过OVA部署的Keystone收集器服务器进行初始配置：

> 完成部署后、您可以使用Keystone收集器管理终端用户界面(TUI)实用程序执行配置和监控活动。您可以使用各种键盘控件(例如Enter键和箭头键)来选择选项并在此TUI中导航。

1. 打开与Keystone收集器服务器的SSH会话。连接后、系统将提示您更新管理员密码。根据需要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将显示。

或者、您也可以通过运行手动启动它 `keystone-collector-tui` CLI命令。

3. 如果需要，请在TUI的*配置>网络部分*中配置代理详细信息。
4. 在*配置>系统*部分中配置系统主机名、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收集器管理TUI实用程序以应用所做的更改。

在**Linux**系统上安装**Keystone**收集器

您可以使用RPM或Debian软件包在Linux服务器上安装Keystone收集器软件。根据您的Linux版本、按照安装步骤进行操作。

使用**RPM**

1. 通过SSH连接到Keystone收集器服务器并升级到 `root` 权限。
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软件包管理器安装keyston-collector软件包：

   `# 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收集器服务器并提升为 `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软件包：
   `# apt-get install keystone-collector`

完成安装后、您可以使用Keystone收集器管理终端用户界面(TUI)实用程序执行配置和监控活动。您可以使用各种键盘控件(例如Enter键和箭头键)来选择选项并在此TUI中导航。请参见 "配置Keystone收集器" 和 "监控系统运行状况" 以了解相关信息。

Keystone软件的自动验证

Keystone存储库已配置为自动验证Keystone软件的完整性、以便您的站点仅安装有效且真

实的软件。

中提供的Keystone YUM存储库客户端配置 `keystonerepo.rpm` 会对通过此存储库下载的所有软件使用强制GPG检查 (`gpgcheck=1`。如果通过Keystone存储库下载的任何RPM未通过签名验证、则无法安装。在Keystone收集器的计划自动更新功能中使用此功能、以确保您的站点仅安装有效且正版的软件。

配置Keystone收集器

要使Keystone收集器能够收集存储环境中的使用情况数据、您需要完成一些配置任务。这是一次性活动、用于激活所需组件并将其与存储环境关联起来。

- Keystone收集器提供了Keystone收集器管理终端用户界面(Terminal User Interface、TUI)实用程序、用于执行配置和监控活动。您可以使用各种键盘控件(例如Enter键和箭头键)来选择选项并在此TUI中导航。
- 可以为无法访问Internet的组织(也称为_dark site_or *private mode*_)配置Keystone收集器。要了解有关的详细信息，请参阅"Keystone处于专用模式"。

步骤

1. 启动Keystone收集器管理TUI实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 转至"**配置">"KS-Collector"*以打开Keystone收集器配置屏幕、查看可用的更新选项。
3. 更新所需选项。

   ** 协议**

   - 收集**ONTAP** 使用量：此选项可用于收集ONTAP 的使用量数据。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：此选项可用于收集ONTAP 的性能数据。默认情况下、此选项处于禁用状态。如果您的环境需要进行性能监控以实现SLA、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、请参见 "创建Unified Manager用户"。
   - 删除私有数据：此选项将删除客户的特定私有数据、默认情况下处于启用状态。有关在启用此选项后从指标中排除哪些数据的信息、请参见 "限制私有数据的收集"。

   ** StorageS卷**

   - 收集**StorageGRID** 使用情况：此选项可用于收集节点使用情况详细信息。添加StorageGRID 节点地址和用户详细信息。
   - 删除私有数据：此选项将删除客户的特定私有数据、默认情况下处于启用状态。有关在启用此选项后从指标中排除哪些数据的信息、请参见 "限制私有数据的收集"。

4. 切换"*使用系统启动KS-Collector"字段。
5. 单击"保存"
   。

6. 返回TUI的主屏幕并验证"*服务状态"*信息、以确保Keystone收集器处于运行状况良好的状态。系统应显示这些服务处于"Overall"：Health"*状态。

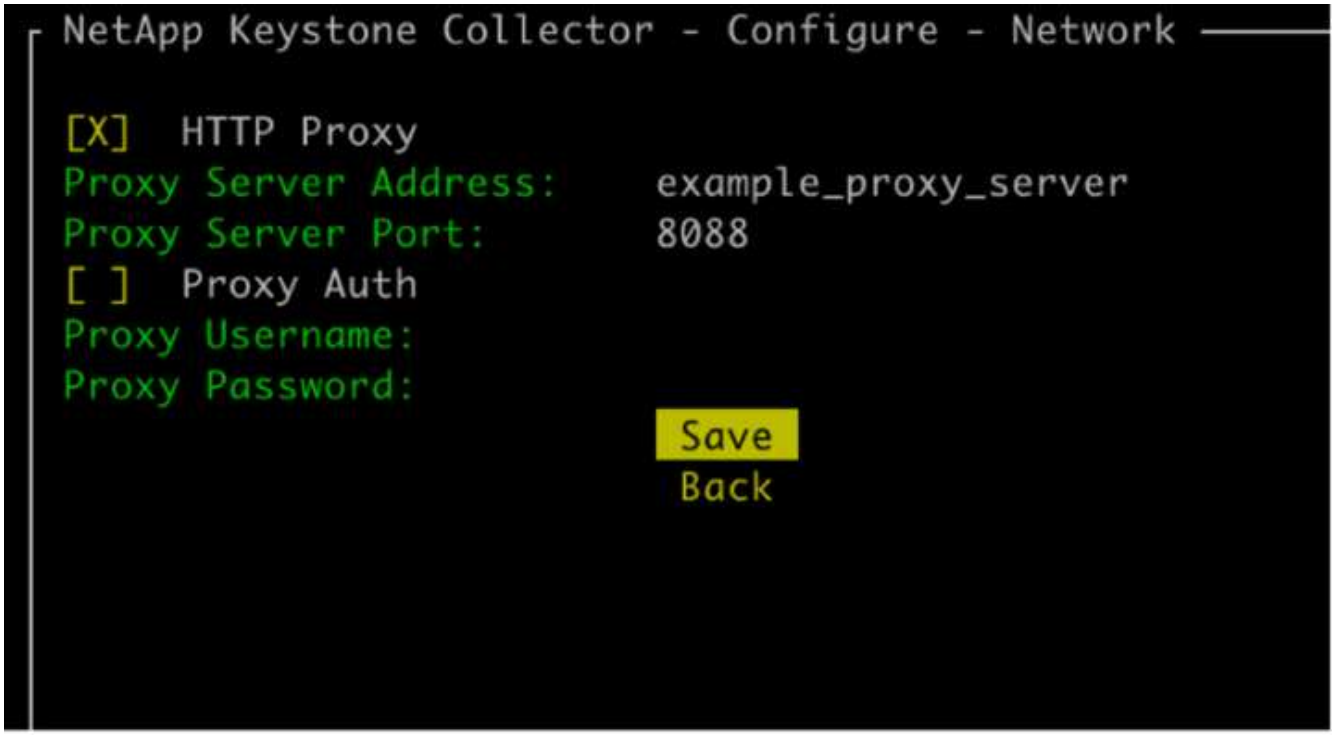
7. 在主屏幕上选择"Exitto Shell"选项、退出Keystone收集器管理TUI。

在Keystone收集器上配置HTTP代理

收集器软件支持使用HTTP代理与Internet进行通信。可以在TUI中配置此功能。

步骤

1. 如果已关闭Keystone收集器管理TUI实用程序、请重新启动该实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 切换"http代理"*字段、如果需要身份验证、请添加HTTP代理服务器、端口和凭据的详细信息。
3. 单击"保存"
   。



限制私有数据的收集

Keystone收集器收集执行订阅计量所需的有限配置、状态和性能信息。您可以选择通过屏蔽上传的内容中的敏感信息来进一步限制收集的信息。这不会影响计费计算。但是、限制信息可能会影响报告信息的可用性、因为某些要素(例如卷名称)会替换为UUID、而这些要素可以由用户轻松识别。

限制特定客户数据的收集是Keystone收集器TUI屏幕上的一个可配置选项。默认情况下、此选项*删除私有数据*处于启用状态。

有关在ONTAP 和StorageGRID 中删除的限制私有数据访问的项的信息、请参见 "限制私有数据访问时删除的项列表"。

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收集器安全功能的一部分。但是、如果需要、您可以将Keystone收集器配置为信任自定义根CA。

如果在系统防火墙中使用SSL/TLS检查、则会导致使用自定义CA证书重新加密基于Internet的流量。在接受根证书并允许进行连接之前、必须先配置相应设置、以将源验证为可信CA。请按照以下步骤操作：

步骤

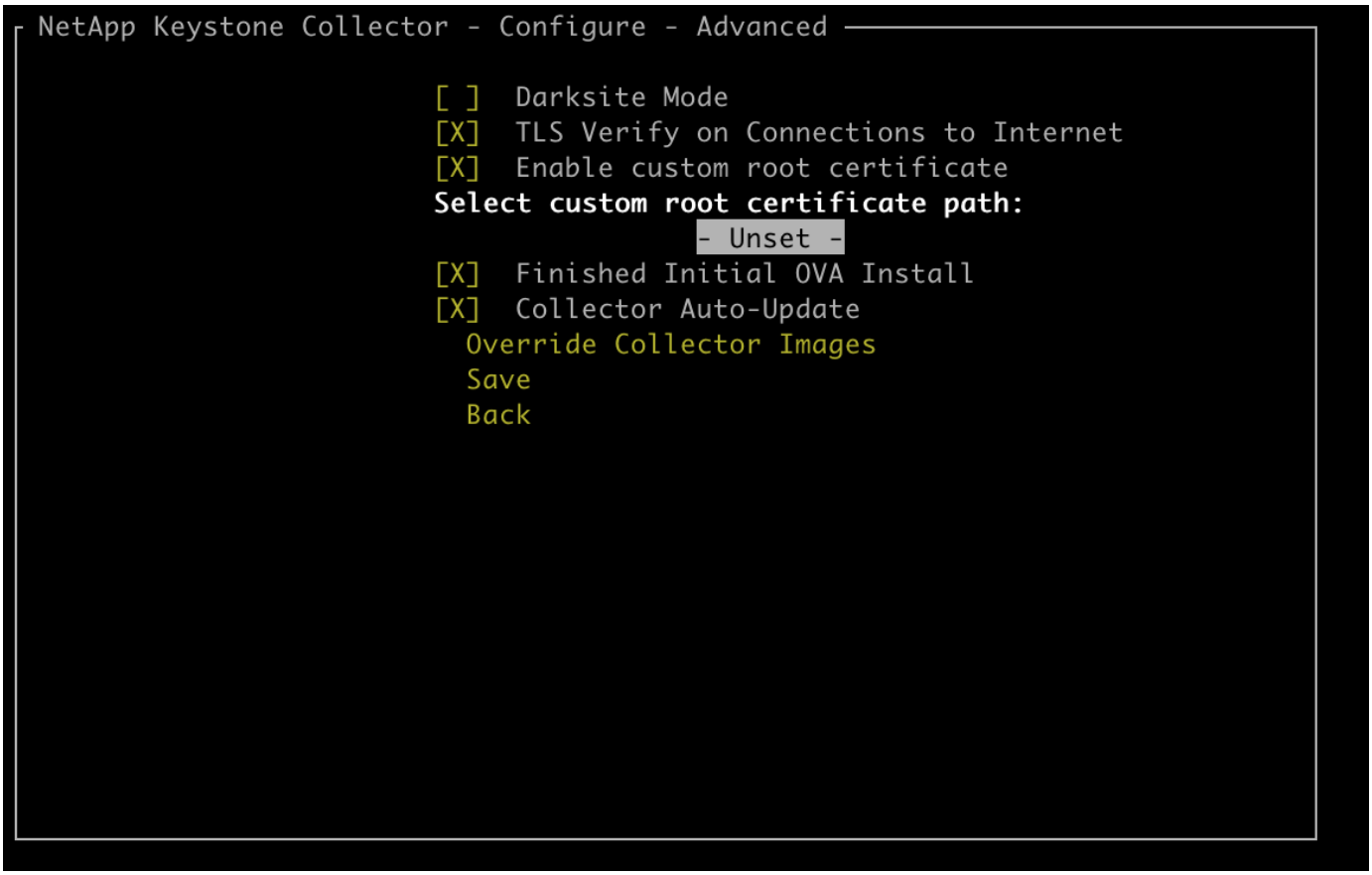
1. 准备CA证书。它应采用_base64编码的X.509文件格式。

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

2. 将证书复制到Keystone收集器服务器。记下文件的复制位置。
3. 打开服务器上的终端并运行管理TUI实用程序。
   ```
   $ keystone-collector-tui
   ```
4. 进入*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：*、请选择 `- Unset -`
7. 按 Enter 键。此时将显示一个对话框、用于选择证书路径。

8. 从文件系统浏览器中选择根证书或输入确切路径。
9. 按 Enter 键。返回到*Advanced*屏幕。
10. 选择 * 保存 * 。此时将应用此配置。

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

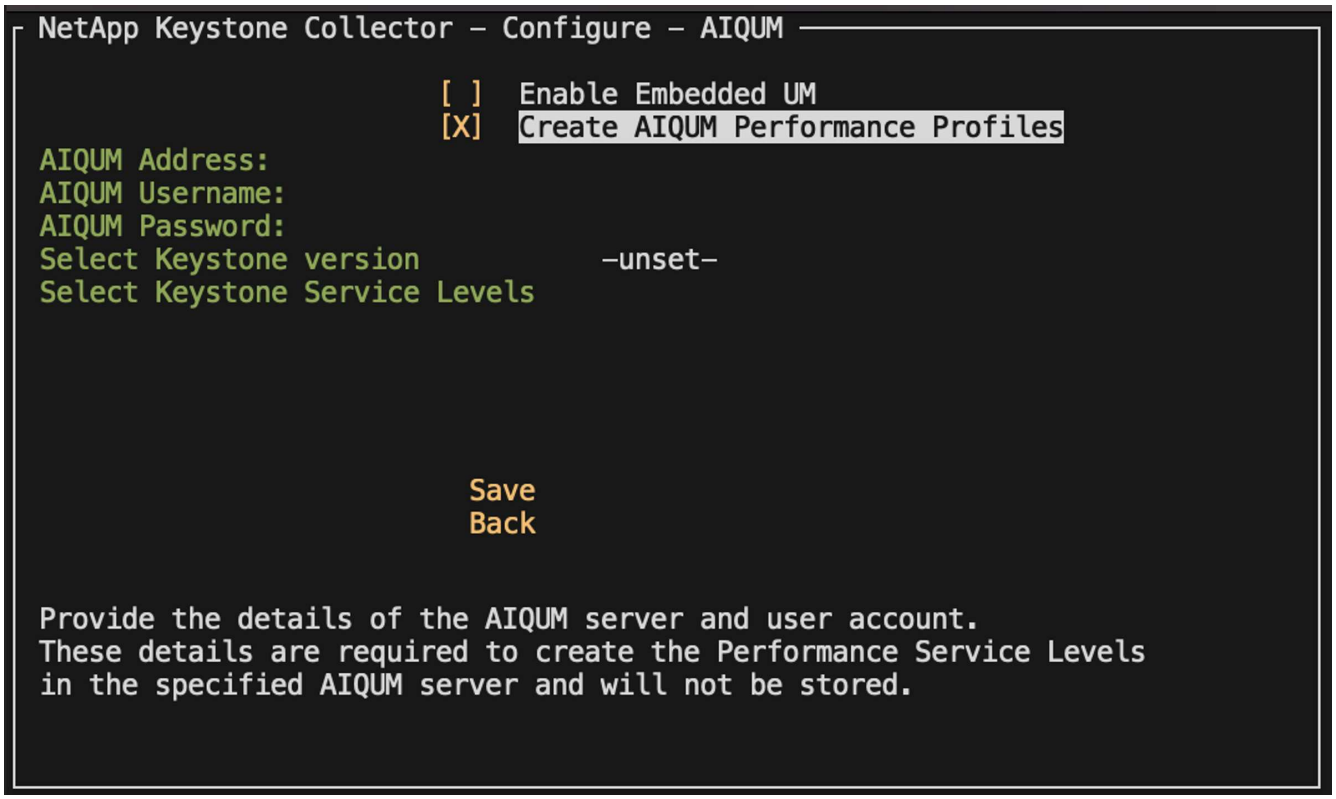
您可以使用Keystone Collector 管理 TUI 实用程序创建性能服务级别 (PSL)。通过 TUI 创建 PSL 会自动选择为每个性能服务级别设置的默认值，从而减少通过Active IQ Unified Manager创建 PSL 时手动设置这些值时可能发生的错误的可能性。

要了解有关PSL的详细信息，请参阅"性能服务级别"。

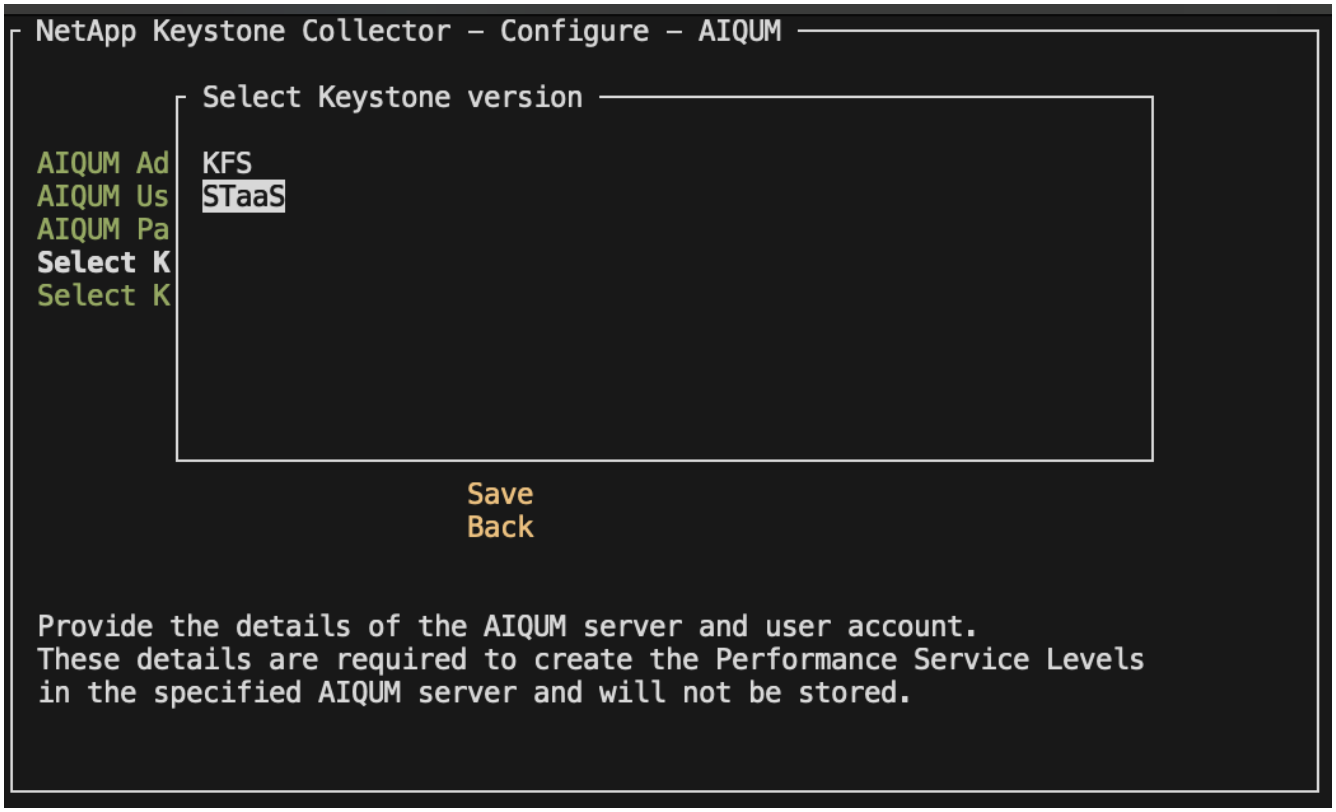
要了解有关服务级别的更多信息，请参见"Keystone中的服务级别"。

步骤

1. 启动Keystone收集器管理TUI实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 转到*Config>AIQUM*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。创建PSL需要这些详细信息、不会存储这些详细信息。

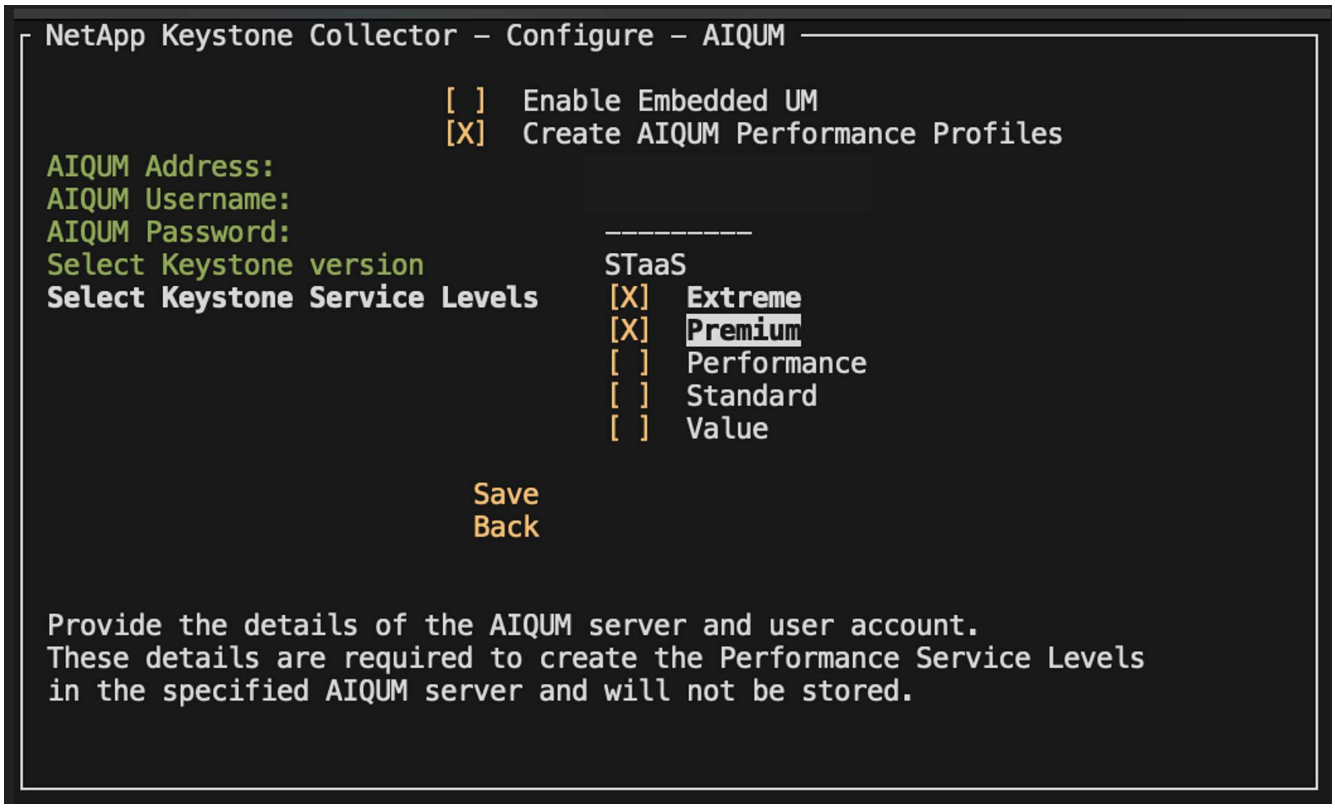


5. 对于*选择Keystone版本*，请选择 `-unset-`。
6. 按Enter键。此时将显示一个对话框、用于选择Keystone版本。
7. 突出显示*STaaS*以指定Keystone STaaS的Keystone版本，然后按Enter键。



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"。

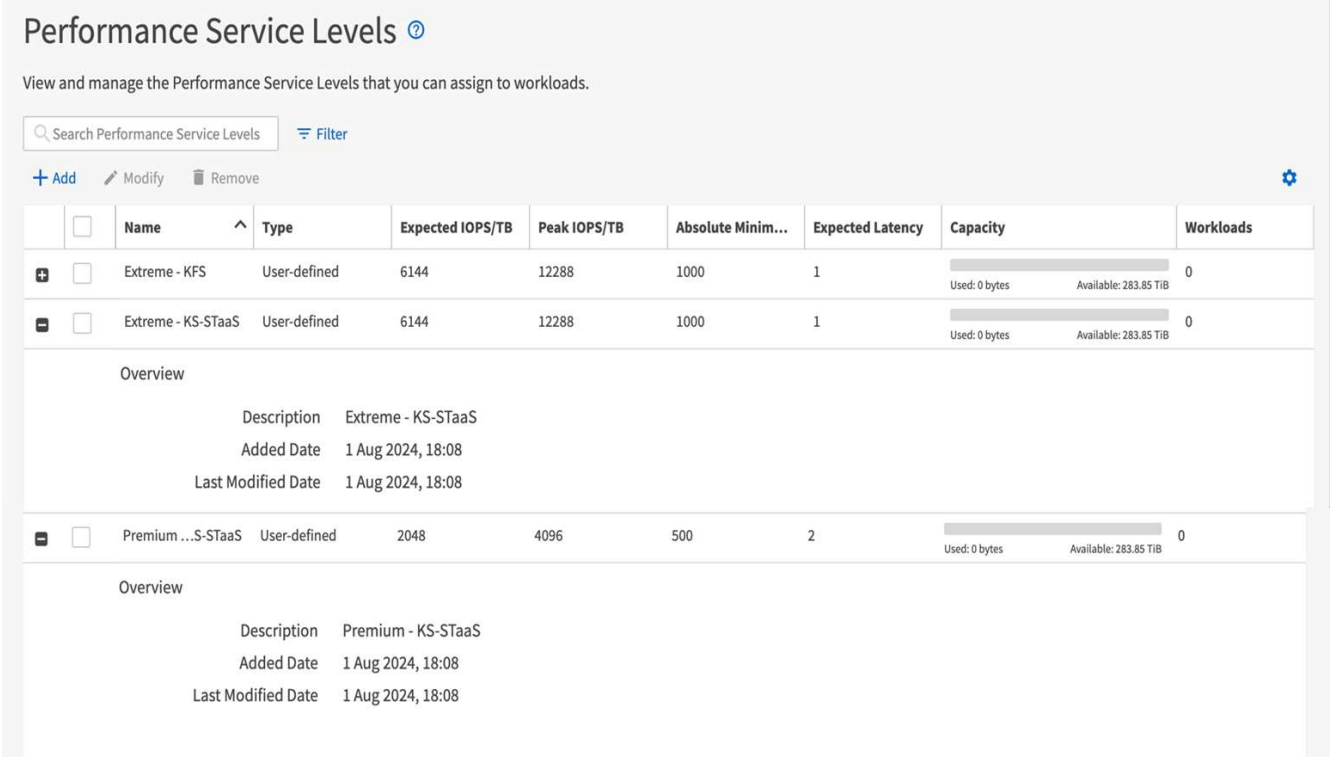
8. 所有受支持的Keystone性能服务级别将显示在指定Keystone版本的 选择**Keystone**服务级别 选项中。从列表中启用所需的性能服务级别。



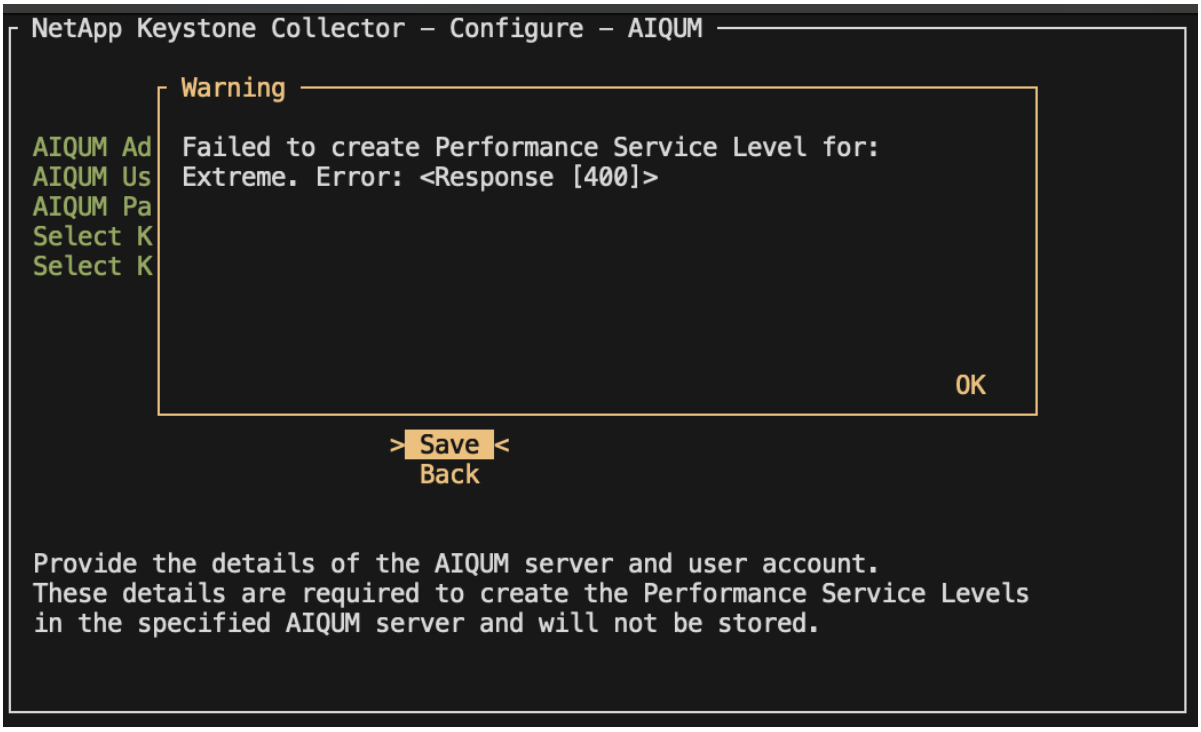
您可以同时选择多个性能服务级别来创建 PSL。

9. 选择*Save*并按Enter键。此时将创建性能服务级别。

   您可以在Active IQ Unified Manager的*性能服务级别*页面上查看已创建的PSL、例如适用于STaaS的Premum-KS-STaaS或适用于KFS的Extreme KFS。如果创建的PSL不符合您的要求、您可以根据需要修改PSL。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收集器

Keystone ITOM Collector 的安装要求

安装ITOM收集器之前、请确保系统已准备好所需的软件、并满足所有必要的前提条件。

ITOM收集器服务器**VM**的前提条件：

- 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

  建议使用Debian 12、Windows Server 2016或更高版本的操作系统。

- 资源要求：根据所监控的NetApp节点数确定的VM资源要求如下：
  - 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：确保在受监控设备上配置了只读帐户和SNMP。如果适用、还需要将ITOM收集器服务器VM配置为NetApp集群和集群交换机上的SNMP陷阱主机和系统日志服务器。

网络要求

下表列出了ITOM收集器的网络连接要求。

源	目标	协议	端口	说明
ITOM收集器	NetApp ONTAP集群管理IP	HTTPS、SNMP	TCP 443、UDP 161	监控ONTAP控制器
NetApp ONTAP集群和节点管理IP	ITOM收集器	SNMP、系统日志	UDP 162、UDP 514	控制器的SNMP陷阱和系统日志
ITOM收集器	集群交换机	SNMP	UDP 161	监控交换机
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陷阱和系统日志
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收集器监控和远程管理
ITOM收集器	本地 DNS	DNS	UDP 53	公共或私有DNS服务
ITOM收集器	选择NTP服务器	NTP	UDP 123	保持时间

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。您可以根据需要将其安装在Windows或Linux系统上。

Keystone支持团队提供了一个动态链接来下载ITOM收集器设置文件、该文件将在两小时后过期。

要在Windows系统上安装ITOM收集器，请参见"在Windows系统上安装ITOM收集器"。

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`软件包以获取ITOM收集器设置文件所需的*xxd*二进制文件。
- 如果计划以非root用户身份运行ITOM收集器、请确保 `sudo package`已安装。

步骤

1. 将ITOM收集器设置文件下载到Linux服务器。
2. 打开服务器上的终端并运行以下命令、以更改权限并使二进制文件可执行：
   `# chmod +x <installer_file_name>.bin`
3. 运行命令以启动ITOM收集器设置文件：
   `#./<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. 选择收集器大小。
   e. 提供代理详细信息(如果适用)。

   对于每个提示符、都会显示一个默认选项。除非您有特定要求、否则建议选择默认选项。按*Enter*键选择默认选项。安装完成后、系统将显示一条消息、确认ITOM收集器已成功安装。

- ITOM收集器设置文件对进行了添加 `/etc/sudoers`、以处理服务重新启动和内存转储。
- 在Linux服务器上安装ITOM收集器会创建一个名为*ITOM*的默认用户，以便在没有根Privileges的情况下运行ITOM收集器。您可以选择其他用户或以root用户身份运行该用户、但建议使用Linux安装脚本创建的ITOM用户。

下一步是什么？

成功安装后、请联系Keystone支持团队、通过ITOM支持门户验证ITOM收集器的安装是否成功。验证后、Keystone支持团队将远程配置ITOM收集器(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消息。如有任何疑问或其他信息、请联系keystone.services@NetApp．com。

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

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

> Keystone支持团队提供了一个动态链接来下载ITOM收集器设置文件、该文件将在两小时后过期。

您可以根据需要将其安装在Linux系统上。要在Linux系统上安装ITOM收集器，请参见"在Linux系统上安装ITOM收集器"。

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收集器服务*作为服务登录*。

步骤

1. 将ITOM收集器设置文件下载到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向导将提取所需的二进制文件并提示您输入凭据。
4. 输入ITOM收集器将在其下运行的帐户的凭据：
   - 如果ITOM收集器未监控其他Windows服务器、请使用本地系统。
   - 如果ITOM收集器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收集器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，使其不会过期，以减少ITOM收集器与其受监控资源之间的身份验证问题。
5. 选择收集器大小。默认值为根据设置文件建议的大小。除非您有特定要求、否则请继续使用建议的大小。
6. 选择_Next_开始安装。您可以使用已填充的文件夹、也可以选择其他文件夹。状态框显示安装进度，然后显示InstallShield向导已完成对话框。

下一步是什么？

成功安装后、请联系Keystone支持团队、通过ITOM支持门户验证ITOM收集器的安装是否成功。验证后、Keystone支持团队将远程配置ITOM收集器(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消息。如有任何疑问或其他信息、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遥测数据计算使用量。要获得所需的粒度级别、您应将AutoSupport配置为在ONTAP集群发送的每日支持包中加入Keystone数据。

关于此任务

在将AutoSupport配置为包含Keystone数据之前、应注意以下事项。

- 您可以使用ONTAP命令行界面编辑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、请参见 "管理 AutoSupport 概述" 和 "集群和 SVM 管理员"。
- 您可以将子系统包含在每日和每周AutoSupport包中、以确保为Keystone精确收集数据。有关AutoSupport子系统的信息、请参见 "什么是 AutoSupport 子系统"。

步骤

1. 以系统管理员用户身份、使用SSH登录到Keystone ONTAP集群。有关信息，请参见 "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
     ```

   - 运行以下命令以修改每周日志内容：

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

有关此命令的详细信息，请参见 "系统节点AutoSupport 触发修改"。

监控和升级

监控Keystone收集器的运行状况

您可以使用支持HTTP请求的任何监控系统来监控Keystone收集器的运行状况。监控运行状况有助于确保Keystone信息板上的数据可用。

默认情况下、Keystone运行状况服务不接受来自本地主机以外的任何IP的连接。Keystone运行状况端点为 `/uber/health`、并侦听端口上Keystone收集器服务器的所有接口 `7777`。查询时、端点将返回一个包含JSON输出的HTTP请求状态代码作为响应、用于描述Keystone收集器系统的状态。
JSON正文提供的整体运行状况 `is_healthy` 属性、布尔值；以及的每个组件状态的详细列表 `component_details` 属性。
以下是一个示例：

```
$ 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 *：表示所有受监控组件运行状况良好
- * 503 *：表示一个或多个组件运行状况不正常
- * 403 ：表示查询运行状况的**HTTP**客户端不在**_allow_**列表中、该列表是一个允许的网络**CIDR**列表。对于此状态、不会返回任何运行状况信息。**_allow_**列表使用网络**CIDR**方法控制允许查询**Keystone**运行状况系统的网络设备。如果收到此错误、请将监控系统添加到 Keystone收集器管理TUI >配置>运行状况监控*中的_allow_列表中。

> **Linux**用户、请注意以下已知问题描述：
>
> 问题描述 收集器：Keystone收集器在使用量计量系统中运行多个容器。如果Red Hat Enterprise Linux 8.x服务器使用美国国防信息系统局(DISA)安全技术实施指南(Stig)策略进行了加固、则会间歇性地看到一个已知的问题描述 with folicyd (文件访问策略守护进程)。此问题描述 标识为 "错误1907870"。*临时解决策 *：在Red Hat Enterprise解决问题之前、NetApp建议您通过输入来解决此问题描述 `fapolicyd` 进入许可模式。在中 `/etc/fapolicyd/fapolicyd.conf`、设置的值 `permissive = 1`。

查看系统日志

您可以使用Keystone收集器系统日志查看系统信息并执行故障排除。Keystone收集器使用主机的_jogal_日志记录系统、可以通过标准_jogalctl_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-collector
- ks-health
- ks-autoupdate

主数据收集服务_ks-collector_使用生成JSON格式的日志 `run-id` 与每个计划的数据收集作业关联的属性。以下是成功收集标准使用情况数据的作业示例：

```
{"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"}
```

以下示例显示了可选性能数据收集作业的成功示例：

```
{"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"}
```

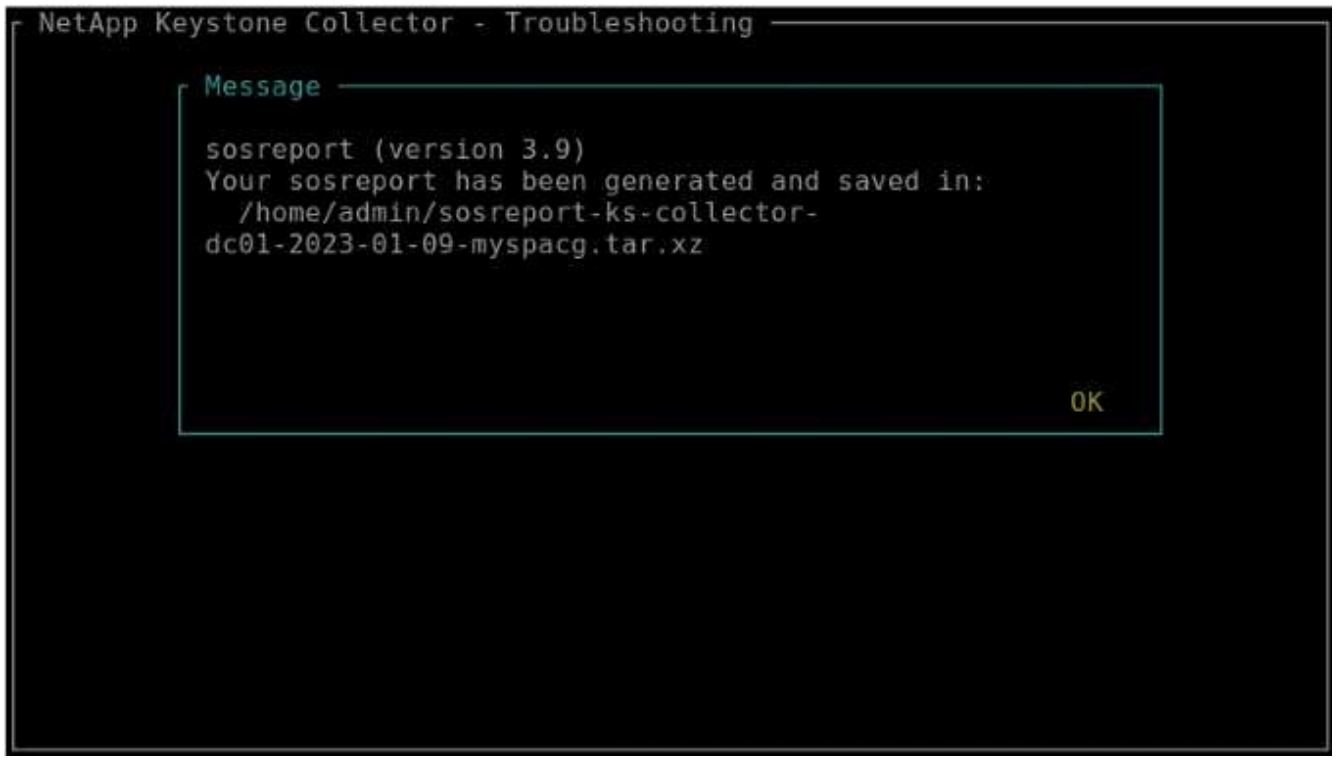
生成并收集支持包

通过Keystone收集器TUI、您可以生成支持包、然后将其添加到服务请求中以解决支持问题。请遵循此操作步骤：

步骤

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

3. 生成时、将显示保存分发包的位置。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。



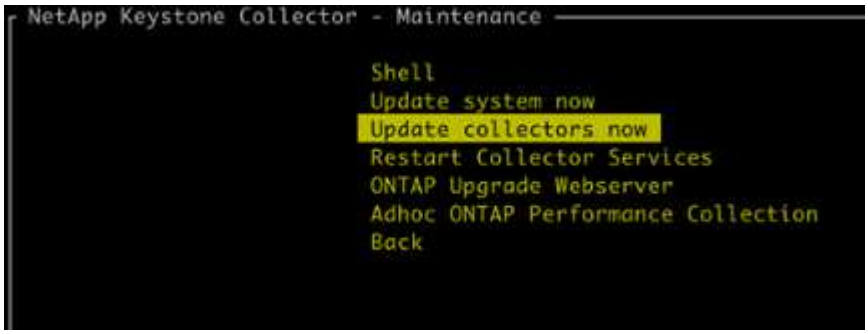
4. 下载文件后，您可以将其附加到Keystone ServiceNow 支持票证。有关提高票数的信息，请参阅 "正在生成服务请求"。

手动升级**Keystone**收集器

默认情况下、Keystone收集器中的自动更新功能处于启用状态、该功能会在每个新版本中自动升级Keystone收集器软件。但是、您可以禁用此功能并手动升级软件。

步骤

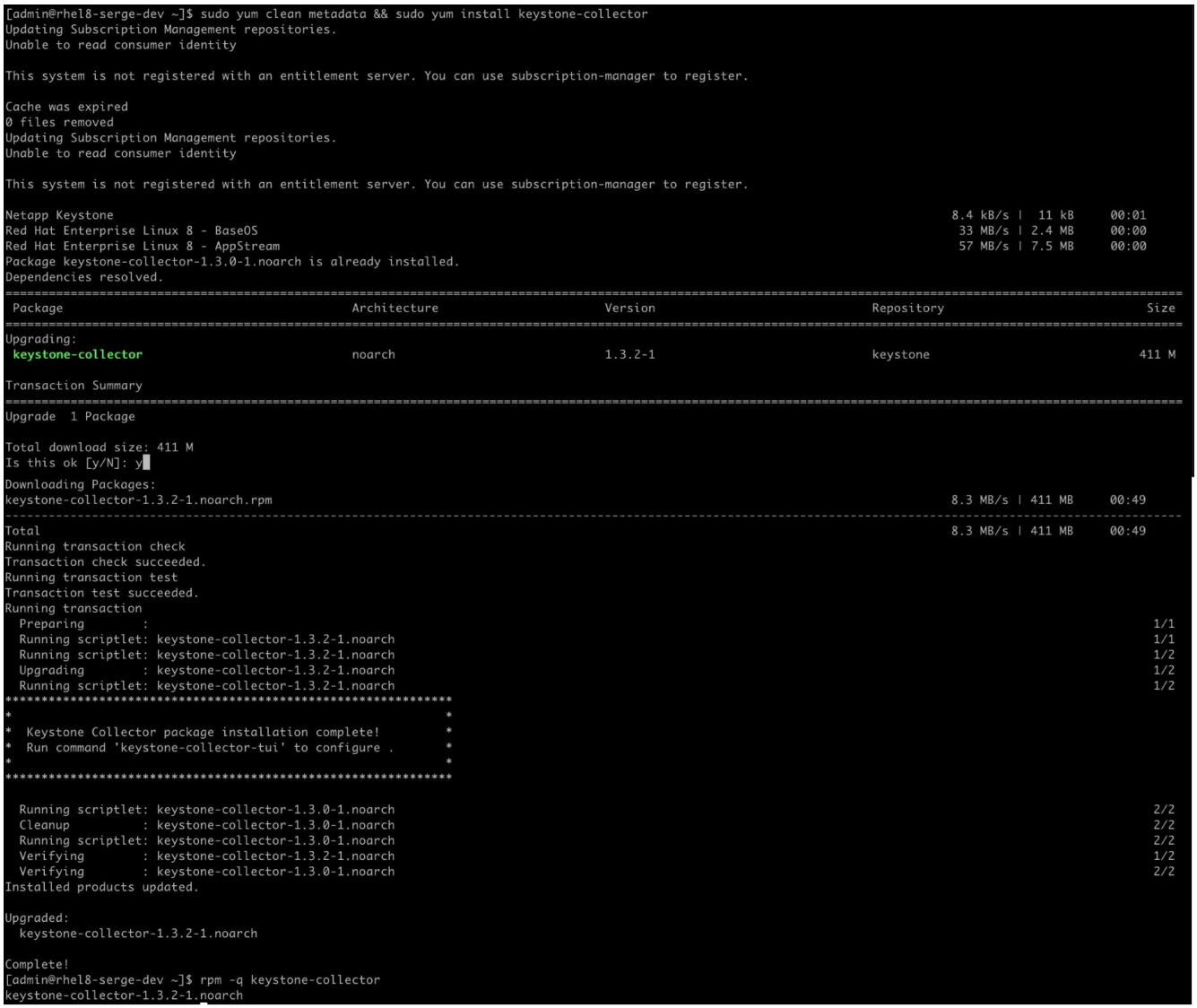
1. 启动Keystone收集器管理TUI实用程序：
   ```
   $ keystone-collector-tui
   ```
2. 在维护屏幕上、选择*立即更新收集器*选项。



或者、也可以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收集器管理TUI、您可以在主屏幕的左上角看到最新版本。

   或者、也可以运行以下命令来查看最新版本：

   对于CentOS：

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

   对于Debian：

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

Keystone收集器安全性

Keystone收集器包括一些安全功能、用于监控Keystone系统的性能和使用情况指标、而不会给客户数据的安全带来风险。

Keystone收集器的运行基于以下安全原则：

- 隐私设计-Keystone收集器收集最低限度的数据，以执行使用情况计量和性能监控。有关详细信息，请参见 "收集用于计费的数据"。。 "删除私有数据" 默认情况下、选项处于启用状态、用于屏蔽和保护敏感信息。
- 最低权限访问-Keystone收集器需要最低权限才能监控存储系统，从而最大限度地降低安全风险并防止意外修改数据。此方法符合最小特权原则、可增强受监控环境的整体安全防护。
- 安全软件开发框架- Keystone在整个开发周期内使用安全软件开发框架，可降低风险、减少漏洞并保护系统免遭潜在威胁。

加强安全性

默认情况下、Keystone收集器配置为使用增强安全性的配置。以下是建议的安全配置：

- Keystone收集器虚拟机的操作系统：
  - 符合CIS Debian Linux 12基准测试标准。在Keystone收集器管理软件之外对操作系统配置进行任何更改可能会降低系统安全性。有关详细信息，请参见 "CIS基准测试指南"。
  - 自动接收并安装由Keystone收集器通过自动更新功能验证的安全修补程序。禁用此功能可能会导致未修补的容易受到攻击的软件。
  - 对从Keystone收集器收到的更新进行身份验证。禁用APT存储库验证可能会导致自动安装未经授权的修补程序、从而可能引入漏洞。
- Keystone收集器会自动验证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收集器支持 "自定义可信CA" 认证。默认情况下、它信任由识别的公共根CA签名的证书 "Mozilla CA证书程序"。通过启用其他受信任的CA、Keystone收集器可以对提供这些证书的端点的连接进行HTTPS证书验证。
- 默认情况下，Keystone收集器启用“*删除私有数据”选项，该选项屏蔽并保护敏感信息。有关详细信息，请参见 "限制私有数据的收集"。禁用此选项会将其他数据传输到Keystone系统。例如、它可以包括用户输入的信息、例如卷名称、这些信息可能被视为敏感信息。
- 相关信息 *
- "Keystone收集器概述"
- "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会从Keystone ONTAP和Keystone StorageGRID订阅中收集配置、状态和使用情况信息，以及从托管Keystone Collector 的虚拟机 (VM) 中收集遥测数据。如果在Keystone Collector 中启用了此选项，则它只能收集ONTAP的性能数据。

ONTAP 数据收集

为**ONTAP**收集的****数据：了解****

以下列表是为ONTAP 收集的容量消耗数据的代表性示例：

- 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
  - version
- 节点
  - 序列号
  - Node name
- Volumes
  - Aggregate name
  - 卷名称
  - 卷实例UUID
  - IsCloneVolume标志
  - IsFlexGroup成分卷标志
  - isSpaceEnforcementLogical标志
  - IsSpaceReportingLogical标志
  - 逻辑空间已用字节时间
  - PercentSnapshotSpace
  - PerformanceTierInactiveUserData
  - PerformanceTierInactiveUserDataPercent
  - QoSAdaptivePolicyGroup名称
  - QoSPolicyGroup名称
  - Size
  - 已用
  - 物理使用
  - SizeUsedBySnapshots
  - Type
  - VolumeStyle扩展
  - Vserver name
  - isvsRoot标志

- SVM
  - VserverName
  - VserverUUID
  - 子类型
- 存储聚合
  - 存储类型
  - Aggregate name
  - 聚合UUID
  - 物理使用
  - 可用大小
  - Size
  - 使用尺寸
- 聚合对象存储
  - ObjectStoreName
  - ObjectStoreUUID
  - ProviderType
  - Aggregate name
- 克隆卷
  - FlexClone
  - Size
  - 已用
  - vserver
  - Type
  - 父卷
  - ParentVserver
  - 等成分卷
  - SplitEssite
  - State
  - FlexCloneUsedPercent
- 存储 LUN
  - LUN UUID
  - LUN 名称
  - Size
  - 已用
  - isReserved标志
  - 已申请标志

- 逻辑单元名称
- QoSPolicyUUID
- QoSPolicyName
- 卷UUID
- 卷名称
- SVMUUID
- SVM 名称

- 存储卷
  - 卷实例UUID
  - 卷名称
  - SVMName
  - SVMUUID
  - QoSPolicyUUID
  - QoSPolicyName
  - 容量层占用空间
  - 性能层占用空间
  - 总占用空间
  - 层策略
  - IsProtected标志
  - IsDestination标志
  - 已用
  - 物理使用
  - CloneParentUUID
  - 逻辑空间已用字节时间
- QoS 策略组
  - PolicyGroup
  - QoSPolicyUUID
  - 最大吞吐量
  - 最小吞吐量
  - 最大ThroughputIOPS
  - 最大ThroughputMBps
  - 最小ThroughputIOPS
  - 最小ThroughputMBps
  - IsSharred标志
- ONTAP 自适应QoS策略组

- QoSPolicyName
- QoSPolicyUUID
- PeakIOPS
- PeakIOPSAllocation
- 绝对最小IOPS
- 已指定IOPS
- ExpectedIOPSAllocation
- 块大小

- 占用空间
  - vserver
  - Volume
  - 总占用空间
  - VolumeBlocksFooprintBin0
  - VolumeBlocksFooprintBin1
- MetroCluster
  - 节点
  - 聚合
  - LIF
  - 配置复制
  - 连接
  - 集群
  - Volumes
- MetroCluster 集群
  - 集群UUID
  - 集群名称
  - 远程集群UUID
  - RemoteCluserName
  - 本地配置状态
  - RemoteConfiguration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
- 收集器的可观察性指标
    - 收集时间
    - 已查询Active IQ Unified Manager API端点
    - 响应时间
    - 记录数
    - AIQUMInstance IP
    - CollectorInstance ID

为**ONTAP**收集的****数据：了解****

以下列表是为ONTAP 收集的性能数据的代表性示例：

- 集群名称
- 集群UUID
- 对象ID
- 卷名称
- 卷实例UUID
- vserver
- VserverUUID
- 节点串行
- ONTAPVersion
- AIQUM版本
- 聚合
- 聚合UUID
- ResourceKey
- 时间戳
- IOPSPerTb
- 延迟
- 读取延迟
- 写入MBps
- QoSMinThroughputLatency
- QoSNBladeLatency
- UsedHeadRoom
- CacheMissRatio
- 其他延迟
- QoSAgregateLatency
- IOPS
- QoSNetworkLetency
- 可用操作
- 写入延迟
- QoSCSPOICY延迟
- QoSClusterInterconnectLatency
- 其他MBps
- QoSCopLatency
- QoSDBlade延迟

- 利用率
- 读取IOPS
- MBps
- 其他IOPS
- QoSPolicyGroupLatency
- 读取MBps
- QoSSyncSnapmirrorLatency
- 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

限制私有数据访问时删除的****项目的清单：了解** mON2.**

如果在Keystone收集器上启用了*删除私有数据*选项、则不会为ONTAP 提供以下使用信息。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
- Aggregate name
- 卷名称
- QoSAdaptivePolicyGroup名称
- QoSPolicyGroup名称
- Vserver name
- 存储LUN名称
- Aggregate name
- 逻辑单元名称
- SVM 名称
- AIQUMInstance IP
- FlexClone
- RemoteClusterName

StorageGRID 数据收集

为**StorageGRID**收集的****数据：了解****

以下列表是的代表性示例 `Logical Data` 为StorageGRID 收集：

- StorageGRID ID
- 帐户 ID
- 帐户名称
- 帐户配额字节
- Bucket Name
- 存储分段对象计数
- 存储分段数据字节

以下列表是的代表性示例 `Physical Data` 为StorageGRID 收集：

- StorageGRID ID
- 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

限制私有数据访问时删除的****项目的清单：了解** mON2.**

如果在Keystone收集器上启用了*删除私有数据*选项、则不会为StorageGRID 提供以下使用信息。默认情况下，此选项处于启用状态。

- 帐户名称
- BucketName
- 站点名称
- 实例/NodeName

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处于专用模式

了解Keystone (专用模式)

Keystone提供了一种_privi_部署模式(也称为_dark site_）、以满足您的业务和安全要求。此模式适用于具有连接限制的组织。

NetApp提供专为Internet连接受限或无Internet连接的环境(也称为非公开站点)定制的Keystone STaaS部署。这些环境是安全或隔离的环境、由于安全性、合规性或操作要求、外部通信会受到限制。

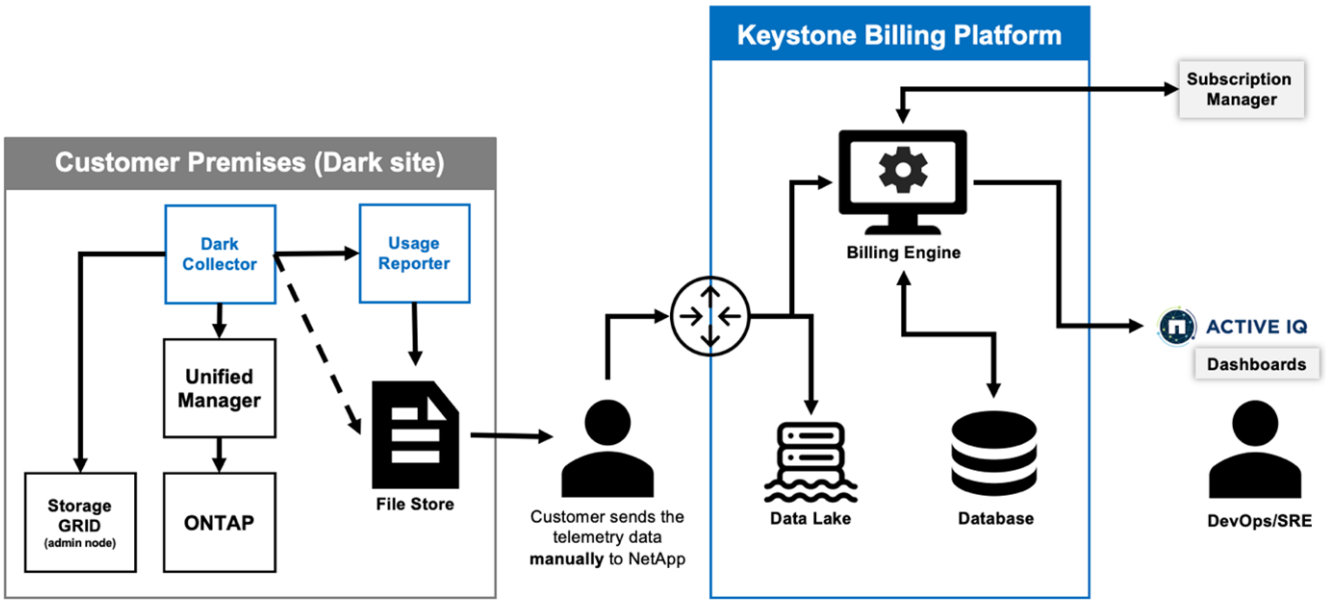
对于NetApp Keystone而言、为非公开站点提供服务意味着以尊重这些环境约束的方式提供Keystone灵活存储订阅服务。这包括：

- 本地部署：Keystone可以独立地在隔离环境中配置、确保不需要Internet连接或外部人员进行设置访问。
- 脱机操作：具有运行状况检查和计费功能的所有存储管理功能均可脱机操作。
- 安全性和合规性：Keystone可确保部署满足非公开站点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24x7全球支持、并为每个客户分配一个专用的Keystone成功经理、以提供帮助和故障排除。

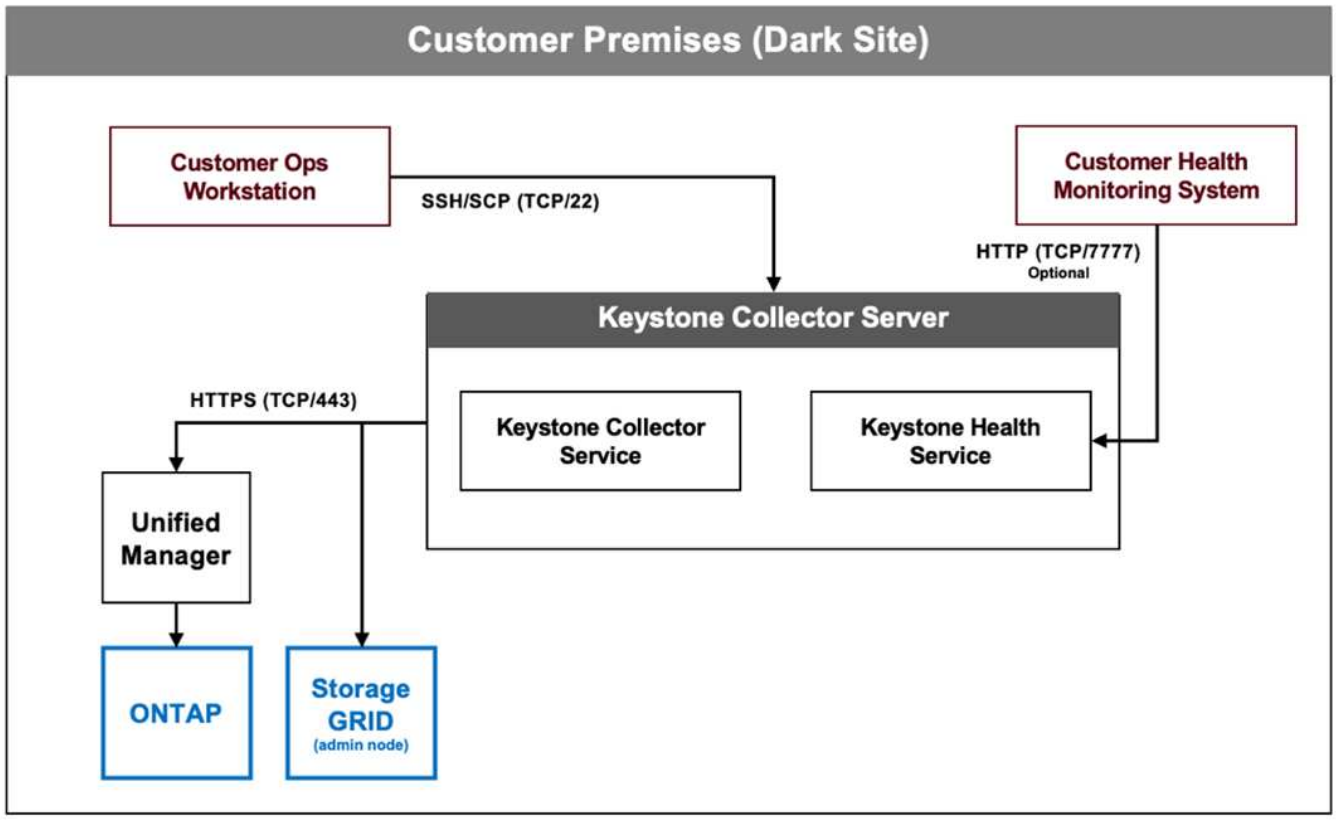
Keystone收集器可以在配置时不受连接限制、也称为_standard_模式。要了解更多信息，请参阅"了解Keystone收集器"。

Keystone收集器处于私用模式

Keystone收集器负责定期从存储系统收集使用情况数据、并将指标导出到脱机使用情况报告程序和本地文件存储。然后、在验证检查后、用户会将以加密和纯文本格式创建的生成文件手动转发到NetApp。收到这些文件后、NetApp的Keystone计费平台将对这些文件进行身份验证和处理、并将其集成到计费和订阅管理系统中以计算每月费用。



服务器上的Keystone收集器服务的任务是定期收集使用情况数据、处理此信息以及在服务器本地生成使用情况文件。运行状况服务可执行系统运行状况检查、并可与客户使用的运行状况监控系统连接。用户可以脱机访问这些报告、以便进行验证并帮助解决问题。



准备以私有模式安装**Keystone Collector**

在无法访问Internet的环境(也称为_dark site_or *private mode*_)中安装Keystone收集器之前、请确保您的系统已准备好必要的软件并满足所有必需的前提条件。

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
- RAM： 2 GB
- 磁盘空间：20 GB vDisk

Linux的要求

- 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个CPU

- RAM： 4 GB
- 磁盘空间：50 GB vDisk
  - 至少2 GB空闲空间 `/var/lib/`
  - 至少48 GB空闲空间 `/opt/netapp`

同一服务器还应安装以下第三方软件包。如果可通过存储库获得这些软件包、则这些软件包将作为前提条件自动安装：

- RHEL 8.6+ (8.x)
  - python3 >=v3.5.8、python3 <=v3.9.13
  - podman
  - SOS
  - yum-utils
  - python3-dnf-plugin-vervonlock
- RHEL 9.0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - podman
  - SOS
  - yum-utils
  - python3-dnf-plugin-vervonlock
- Debian v12
  - python3 >= v3.1.0、python3 <= v3.12.0
  - podman
  - sosreport

网络要求

Keystone收集器的网络连接要求如下：

- 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收集器服务器应可通过端口443 (HTTPS)访问Unified Manager服务器。
- 应在Unified Manager服务器上为Keystone收集器设置具有应用程序用户权限的服务帐户。
- 不需要外部Internet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Keystone帮助"。

在私用模式下安装**Keystone**收集器

完成几个步骤、在无法访问Internet的环境(也称为_dark site_or *private mode*）中安装Keystone收集器。此类安装非常适合您的安全站点。

您可以根据需要在VMware vSphere系统上部署Keystone收集器、也可以在Linux系统上安装Keystone收集器。按照与所选选项对应的安装步骤进行操作。

在**VMware vSphere**上部署

请按照以下步骤操作：

1. 从下载OVA模板文件 "NetApp Keystone Web门户"。
2. 有关使用OVA文件部署Keystone收集器的步骤，请参阅一节"部署OVA模板"。

在**Linux**上安装

Keystone收集器软件使用提供的.deb或.rpm文件安装在Linux服务器上、具体取决于Linux分发版本。

按照以下步骤在Linux服务器上安装软件：

1. 将Keystone收集器安装文件下载或传输到Linux服务器：

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

2. 打开服务器上的终端并运行以下命令开始安装。

   - 正在使用**Debian**软件包

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

   - 正在使用**RPM**文件

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

     或

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

3. `y`当系统提示您安装软件包时、输入。

在专用模式下配置**Keystone**收集器

完成一些配置任务、使Keystone收集器能够在无法访问Internet的环境(也称为_dark site_or *private mode*）中收集使用情况数据。这是一次性活动、用于激活所需组件并将其与存储环境关联起来。配置后、Keystone收集器将监控由Active IQ Unified Manager管理的所有ONTAP集群。

Keystone收集器提供了Keystone收集器管理终端用户界面(Terminal User Interface、TUI)实用程序、用于执行配置和监控活动。您可以使用各种键盘控件(例如Enter键和箭头键)来选择选项并在此TUI中导航。

步骤

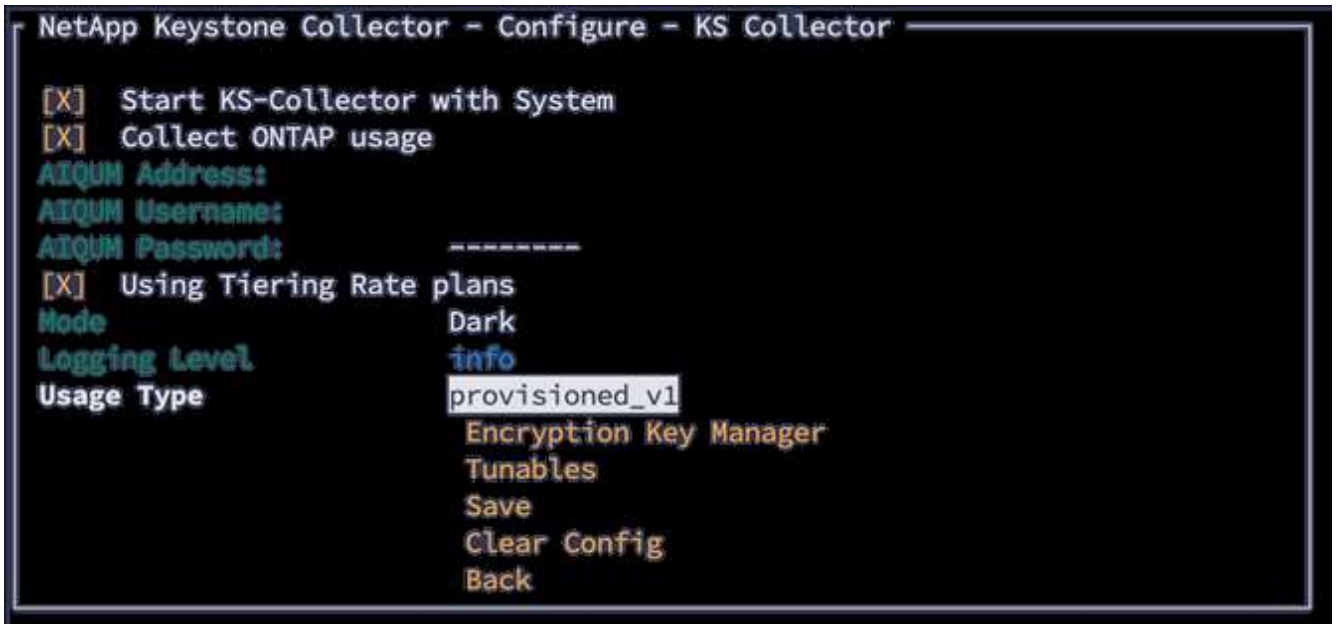
1. 启动Keystone收集器管理TUI实用程序：

```
keystone-collector-tui
```

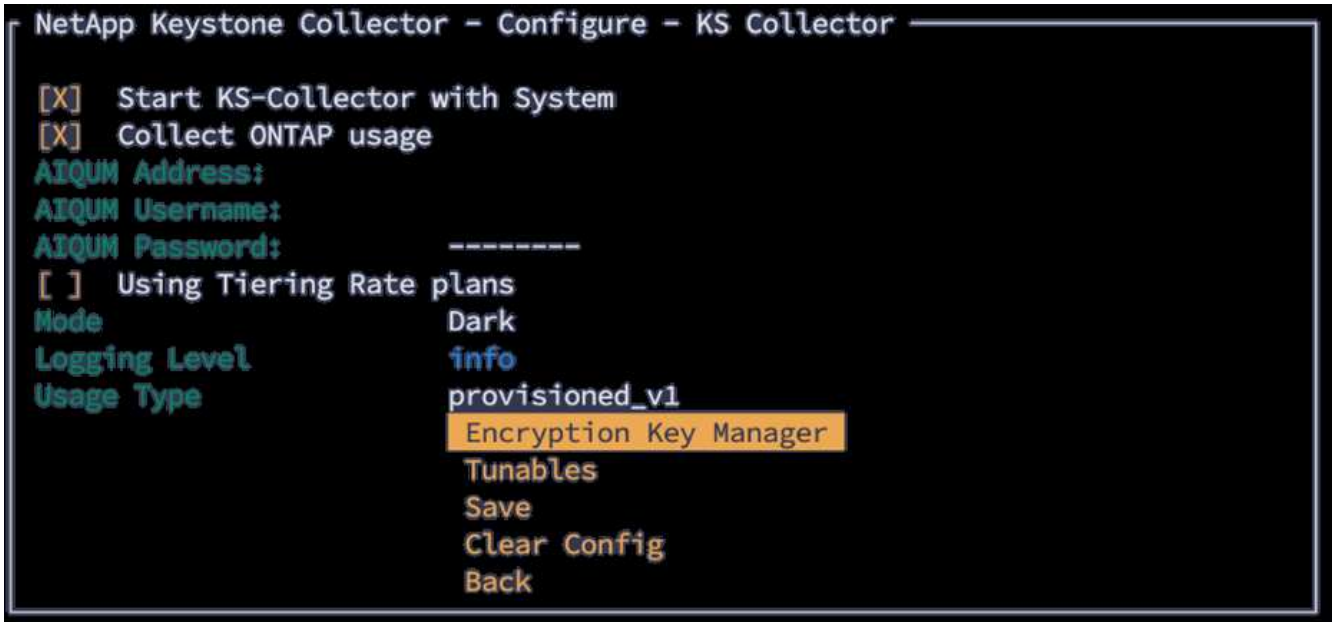
2. 转到*Configure > Advanced*。
3. 切换*Darksite Mode*选项。

4. 选择 * 保存 * 。
5. 转到*Configure > KS-Collector *以配置Keystone收集器。
6. 切换*Start KS Collector with System*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*使用分层速率计划*字段。
9. 根据所购买的订阅类型，更新*使用类型*。

> 在配置之前、请确认与NetApp订阅关联的使用类型。

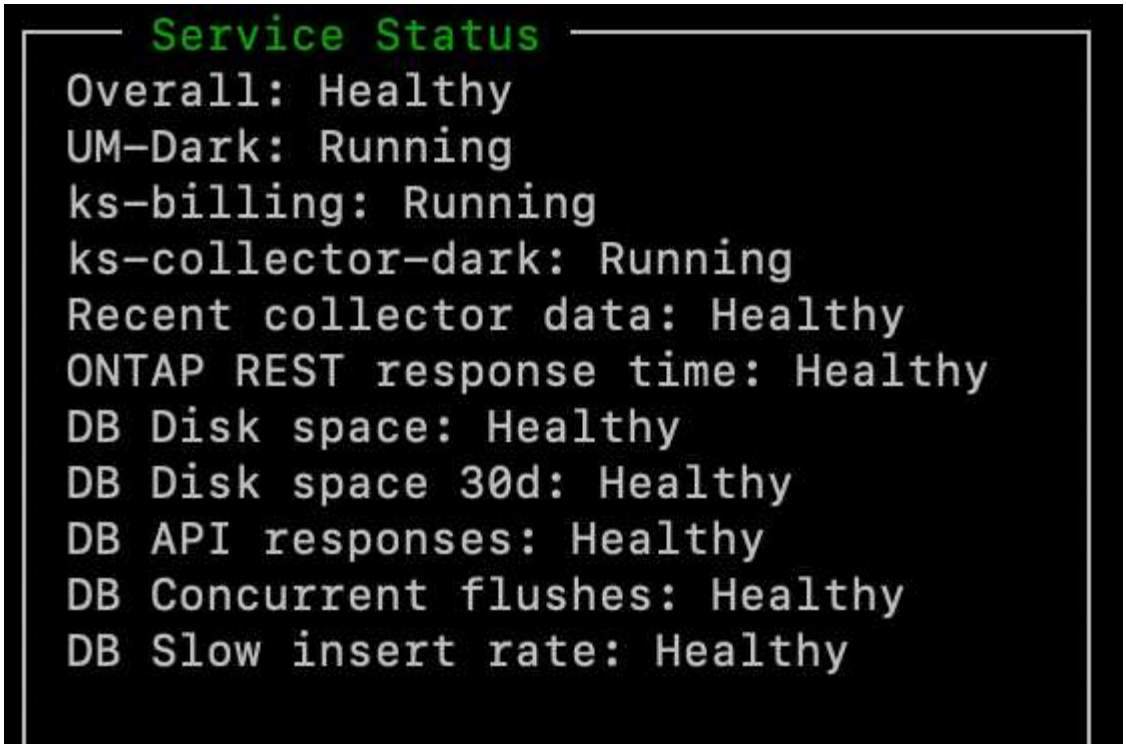


10. 选择 * 保存 * 。
11. 转到*Configure > KS-Collector *以生成Keystone收集器密钥对。
12. 进入*加密密钥管理器*并按Enter键。



13. 选择*Generate Collector Keypair (生成收集器密件压缩)*，然后按Enter键。

14. 返回TUI的主屏幕并验证*服务状态*信息、以确保Keystone收集器运行状况良好。系统应显示这些服务处于*整体：运行状况良好*状态。等待10分钟、如果在此期间后整体状态仍然不正常、请查看先前的配置步骤并联系NetApp支持团队。



15. 通过在主屏幕上选择*退出到Shell*选项退出Keystone收集器管理TUI。
16. 检索生成的公共密钥：

    ```
    ~/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

您应在每月底向NetApp发送每月使用情况摘要报告。您可以手动生成此报告。

按照以下步骤生成使用情况报告：

1. 转到Keystone收集器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收集器会生成一个清除文件和一个加密文件、这些文件应手动发送到NetApp。清除文件报告包含以下详细信息、可由客户验证。

```
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收集器支持通过TUI升级ONTAP。

按照以下步骤升级ONTAP：

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

3. `http://<collector-ip>:8000`请转到使用Web浏览器获取升级帮助。

重新启动**Keystone**收集器

您可以通过TUI重新启动Keystone收集器服务。转到TUI中的*维护>重新启动收集器*服务。此操作将重新启动所有收集器服务、并且可以从TUI主屏幕监控其状态。

在私用模式下监控**Keystone**收集器的运行状况

您可以使用支持HTTP请求的任何监控系统来监控Keystone收集器的运行状况。

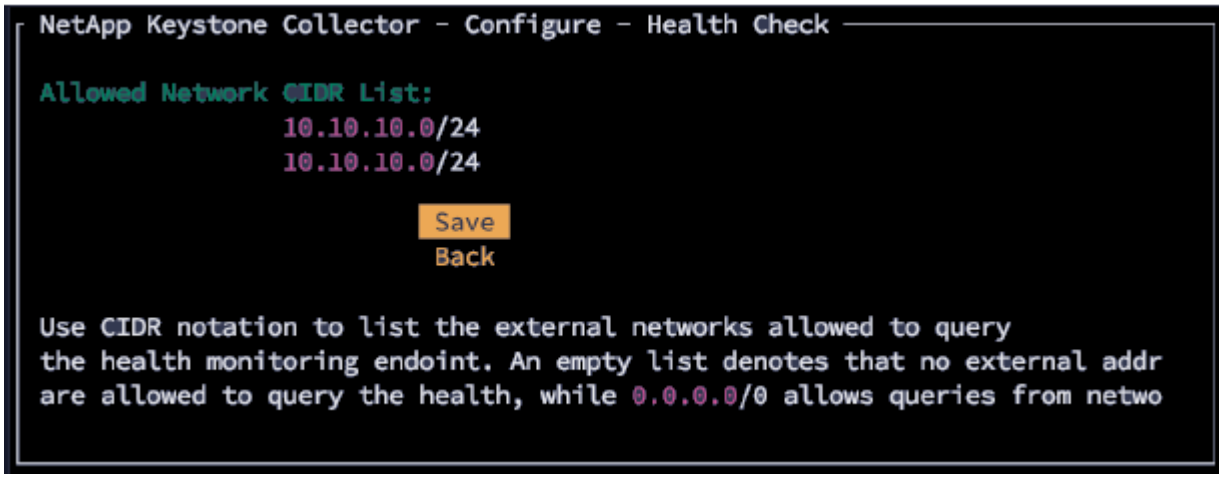
默认情况下、Keystone运行状况服务不接受来自本地主机以外的任何IP的连接。Keystone运行状况端点为 `/uber/health`、并侦听端口上Keystone收集器服务器的所有接口 `7777`。查询时、端点将返回一个包含JSON输出的HTTP请求状态代码作为响应、用于描述Keystone收集器系统的状态。
JSON正文提供的整体运行状况 `is_healthy` 属性、布尔值；以及的每个组件状态的详细列表 `component_details` 属性。
以下是一个示例：

```
$ 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 *：表示所有受监控组件运行状况良好
- * 503 *：表示一个或多个组件运行状况不正常
- * 403 *：表示查询运行状况的HTTP客户端不在_allow_列表中、该列表是一个允许的网络CIDR列表。对于此状态、不会返回任何运行状况信息。

  _allow_列表使用网络CIDR方法控制允许查询Keystone运行状况系统的网络设备。如果收到403错误，请通过*Keystone收集器管理TUI >配置>运行状况监控*将监控系统添加到_ALLOWE_列表中。

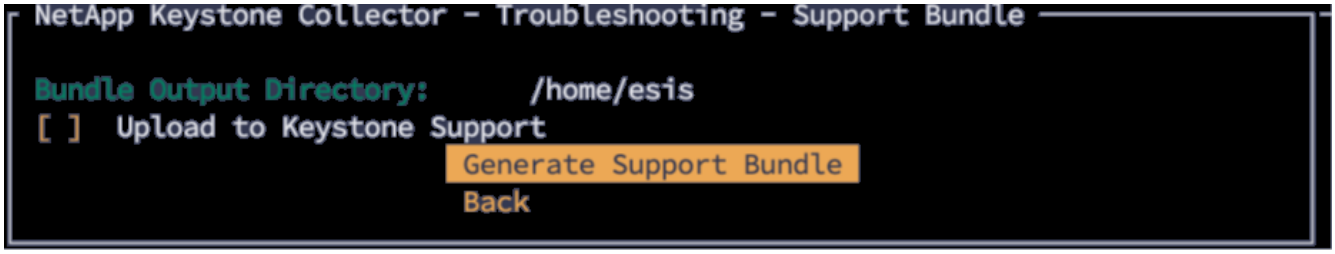


生成并收集支持包

要对Keystone收集器的问题进行故障排除、您可以与NetApp支持人员联系、他们可能会要求提供_.tar_文件。您可以通过Keystone收集器管理TUI实用程序生成此文件。

按照以下步骤生成_.tar_文件：

1. 转至*故障排除>生成支持包*。
2. 选择保存分发包的位置，然后单击*Generate Support Bundle*。



此过程会 `tar`在所述位置创建一个软件包、可与NetApp共享该软件包以解决问题。

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 "正在生成服务请求"。