



规划 ONTAP 9

NetApp
February 13, 2026

目录

- 规划 1
 - 准备使用ONTAP AutoSupport 1
 - 向NetApp传送AutoSupport消息 1
 - 其他配置注意事项 2
 - 安装服务器证书 2
 - 设置ONTAP AutoSupport 4

规划

准备使用ONTAP AutoSupport

您可以将ONTAP集群配置为向NetApp传送AutoSupport消息。在此过程中、您还可以将消息副本发送到本地电子邮件地址、通常是在您的组织内。您应通过查看可用选项来准备配置AutoSupport。

向NetApp传送AutoSupport消息

可以使用HTTPS或SMTP协议将AutoSupport消息传送到NetApp。从ONTAP 9.15.1开始、您还可以将TLS与SMTP结合使用。



尽可能使用HTTPS与AutoSupport OnDemand通信并上传大型文件。

另请注意以下事项：

- 只能为NetApp AutoSupport消息配置一个传送通道。您不能使用两种协议向NetApp传送AutoSupport消息。
- AutoSupport 会限制每个协议的最大文件大小。如果AutoSupport消息的大小超过配置的限制、则AutoSupport会尽可能多地发送消息、但会发生消息被删除。
- 您可以根据需要更改最大文件大小。有关的详细信息 `system node autosupport modify`，请参见["ONTAP 命令参考"](#)。
- 这两种协议都可以根据名称解析到的地址系列通过IPv4或IPv6进行传输。
- ONTAP为发送AutoSupport消息而建立的TCP连接是临时的、短暂的。

HTTPS

这提供了最强大的功能。请注意以下事项：

- 支持AutoSupport OnDemand和大型文件传输。
- 首先尝试HTTPS放置请求。如果此请求在传输期间失败、则此请求将从停止位置重新启动。
- 如果服务器不支持Put、则改用HTTPS POST方法。
- HTTPS传输的默认限制为50 MB。
- HTTPS 协议使用端口 443 。

SMTP

一般情况下、只有在不允许或不支持HTTPS的情况下、才应使用SMTP。请注意以下事项：

- 不支持AutoSupport OnDemand和传输大型文件。
- 如果配置了SMTP登录凭据、则会以未加密的方式以明文形式发送这些凭据。
- 默认传输限制为5 MB。
- 不安全的SMTP协议使用端口25。

利用TLS提高SMTP安全性

使用SMTP时、所有流量均未加密、可以轻松截获和读取。从ONTAP 9.15.1开始、您还可以将TLS与SMTP (SMTPS)结合使用。在这种情况下、会使用_explicit_tls_、以便在建立TCP连接后激活安全通道。

以下端口通常用于SMTPS：端口587

其他配置注意事项

配置AutoSupport时、还需要考虑一些其他注意事项。

有关与这些注意事项相关的命令的详细信息，请参见["设置 AutoSupport"](#)。

使用电子邮件发送本地副本

无论使用哪种协议将AutoSupport消息传送到NetApp、您都可以将每条消息的副本发送到一个或多个本地电子邮件地址。例如、您可以向内部支持组织或合作伙伴组织发送消息。



如果您使用SMTP (或SMTPS)将消息传送到NetApp、同时还发送了这些消息的本地电子邮件副本、则会使用相同的电子邮件服务器配置。

HTTP 代理

根据您的网络配置、HTTPS协议可能需要对代理URL进行额外配置。如果使用HTTPS向技术支持发送AutoSupport消息、并且您有代理、则必须标识此代理的URL。如果代理使用的端口不是默认端口(端口3128)、则可以为该代理指定端口。您也可以选择为代理身份验证指定用户名和密码。

安装服务器证书

对于TLS (HTTPS或SMTPS)、ONTAP会根据根CA证书对从服务器下载的证书进行验证。在使用HTTPS或SMTPS之前、您需要确保根证书已安装在ONTAP中、并且ONTAP可以验证服务器证书。此验证将根据签署服务器证书的CA来执行。

ONTAP包含大量预安装的根CA证书。在许多情况下、ONTAP可以立即识别服务器的证书、而无需进行额外配置。根据服务器证书的签名方式、您可能需要安装根CA证书和任何中间证书。

如果需要、请使用以下过程安装证书。您应在集群级别安装所有必需的证书。

示例 1. 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*Security*部分。
3. 选择 → *Certificates*旁边的。
4. 在“可信证书颁发机构”选项卡下，单击“添加”。
5. 单击*Import*并选择证书文件。
6. 完成环境的配置参数。
7. 单击 * 添加 *。

命令行界面

1. 开始安装：

```
security certificate install -type server-ca
```

有关的详细信息 security certificate install，请参见["ONTAP 命令参考"](#)。

2. 查找以下控制台消息：

```
Please enter Certificate: Press <Enter> when done
```

3. 使用文本编辑器打开证书文件。
4. 复制整个证书、包括以下行：

```
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----END CERTIFICATE-----
```

5. 在命令提示符后、将证书粘贴到终端中。
6. 按*Enter*键完成安装。
7. 运行以下命令之一以确认证书已安装：

```
security certificate show-user-installed
```

```
security certificate show
```

有关的详细信息 security certificate show，请参见["ONTAP 命令参考"](#)。

相关信息

- ["设置 AutoSupport"](#)
- ["ONTAP 命令参考"](#)

设置ONTAP AutoSupport

您可以配置ONTAP集群、以便向NetApp技术支持传送AutoSupport消息、并向内部支持组织发送电子邮件副本。在此过程中、您还可以先对配置进行测试、然后再在生产环境中使用它。

关于此任务

从ONTAP 9.5开始、您可以同时为集群中的所有节点启用和配置AutoSupport。当新节点加入集群时、该节点会自动继承相同的AutoSupport配置。为此、请查看CLI命令的范围 `system node autosupport modify` 是集群级别的。。 `-node` 为了向后兼容、保留了命令选项、但会将其忽略。



在ONTAP 9.4及更早版本中、命令 `system node autosupport modify` 特定于每个节点。如果集群运行的是ONTAP 9.4或更早版本、则需要在集群中的每个节点上启用和配置AutoSupport。

开始之前

将AutoSupport消息传送到NetApp时、建议使用HTTPS (HTTP与TLS)传输配置。此选项可提供最强大的功能和最佳的安全性。

请查看 ["准备使用AutoSupport"](#) 了解有关配置ONTAP集群之前的详细信息。

步骤

1. 确保已启用 AutoSupport :

```
system node autosupport modify -state enable
```

2. 如果您希望NetApp技术支持接收AutoSupport消息、请使用以下命令:

```
system node autosupport modify -support enable
```

如果要使 AutoSupport 能够与 AutoSupport OnDemand 配合使用,或者要将核心转储和性能归档文件等大型文件上传到技术支持或指定 URL,则必须启用此选项。



默认情况下、AutoSupport OnDemand处于启用状态、如果配置为使用HTTPS传输协议向技术支持发送消息、则该功能正常运行。

3. 如果您启用了NetApp技术支持以接收AutoSupport消息、请指定用于这些消息的传输协议。

您可以从以下选项中进行选择:

如果您要 ...	然后设置的以下参数 <code>system node autosupport modify</code> 命令...
使用默认 HTTPS 协议	a. 设置 <code>-transport to https</code> 。 b. 如果使用代理、请设置 <code>-proxy-url</code> 代理的URL。此配置支持与 AutoSupport OnDemand 通信以及上传大型文件。
使用 SMTP	设置 <code>-transport to smtp</code> 。 此配置不支持 AutoSupport OnDemand 或上传大型文件。

4. 如果您希望内部支持组织或支持合作伙伴接收 AutoSupport 消息，请执行以下操作：

- a. 通过设置的以下参数、确定组织中的收件人 `system node autosupport modify` 命令：

设置此参数 ...	目标位置 ...
<code>-to</code>	您的内部支持组织中最多五个将接收关键 AutoSupport 消息的电子邮件地址或分发列表，以逗号分隔
<code>-noteto</code>	您的内部支持组织中最多有五个以逗号分隔的单个电子邮件地址或分发列表，这些地址或分发列表将接收专为手机和其他移动设备设计的关键 AutoSupport 消息的简略版本
<code>-partner-address</code>	您的支持合作伙伴组织中最多五个以逗号分隔的单个电子邮件地址或分发列表，这些电子邮件地址或分发列表将接收所有 AutoSupport 消息

- b. 通过使用列出目标来检查是否已正确配置地址 `system node autosupport destinations show` 命令：

5. 如果您在上一步中为内部支持组织配置了收件人地址、或者为发送给技术支持的消息选择了SMTP传输、请通过设置命令的以下参数来配置SMTP `system node autosupport modify`：

- 设置 `-mail-hosts` 发送到一个或多个邮件主机、以逗号分隔。

最多可以设置五个。

您可以通过在邮件主机名后面指定冒号和端口号来为每个邮件主机配置端口值：例如、`mymailhost.example.com:5678`，其中5678是邮件主机的端口。

- 设置 `-from` 发送AutoSupport消息的电子邮件地址。

6. 配置 DNS 。

7. (可选)如果要更改特定设置、请添加命令选项：

如果要执行此操作 ...	然后设置的以下参数 <code>system node autosupport modify</code> 命令...
通过删除，屏蔽或对消息中的敏感数据进行编码来隐藏私有数据	设置 <code>-remove-private-data to true</code> 。如果您从进行了更改 <code>false to true</code> ，所有AutoSupport历史记录和所有关联文件都将被删除。
停止在定期 AutoSupport 消息中发送性能数据	设置 <code>-perf to false</code> 。

8. 如果您使用SMTP向NetApp传送AutoSupport消息、则可以选择启用TLS以提高安全性。

a. 显示可用于新参数的值：

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

b. 为SMTP消息传送启用TLS：

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

c. 显示当前配置：

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. 使用检查整体配置 `system node autosupport show` 命令 `-node` 参数。

10. 使用验证AutoSupport操作 `system node autosupport check show` 命令：

如果报告任何问题、请使用 `system node autosupport check show-details` 命令以查看详细信息。

11. 测试是否正在发送和接收 AutoSupport 消息：

a. 使用 `system node autosupport invoke` 命令 `-type` 参数设置为 `test`：

```
cluster1::> system node autosupport invoke -type test -node node1
```

b. 确认 NetApp 正在接收您的 AutoSupport 消息：

```
system node autosupport history show -node local
```

最新传出AutoSupport消息的状态最终应更改为 `sent-successful` 所有适当的协议目标。

c. (可选)通过检查为配置的任何地址的电子邮件来确认AutoSupport消息正在发送到您的内部支持组织或您的支持合作伙伴 `-to`，`-noteto`` 或 ``-partner-address` 的参数 `system node autosupport`

modify 命令：

相关信息

- ["准备使用AutoSupport"](#)
- ["ONTAP 命令参考"](#)

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。