



Plan

ONTAP 9

NetApp
February 04, 2026

目次

Plan	1
ONTAP AutoSupportを使用する準備	1
NetAppへのAutoSupportメッセージの配信	1
設定に関するその他の考慮事項	2
サーバ証明書のインストール	2
ONTAP AutoSupportのセットアップ	4

Plan

ONTAP AutoSupportを使用する準備

AutoSupportメッセージをNetAppに配信するようにONTAPクラスタを設定できます。その一環として、ローカルの（通常は組織内の）Eメールアドレスにメッセージのコピーを送信することもできます。使用可能なオプションを確認して、AutoSupportを設定する準備をしておく必要があります。

NetAppへのAutoSupportメッセージの配信

AutoSupport メッセージは、HTTPS または SMTP プロトコルを使用して NetApp に配信できます。ONTAP 9.15.1 からは、SMTP で TLS も使用できます。



AutoSupport OnDemandとの通信や大きなファイルのアップロードには、可能な限りHTTPSを使用してください。

次の点にも注意してください。

- AutoSupportメッセージに対して設定できる、NetAppへの配信チャネルは1つだけです。2つのプロトコルを使用してAutoSupportメッセージをNetAppに配信することはできません。
- AutoSupportでは、プロトコルごとに最大ファイルサイズが制限されます。AutoSupportメッセージのサイズが設定した制限を超えると、できる限り多くのメッセージが配信されますが、切り捨てが発生します。
- 必要に応じて最大ファイルサイズを変更できます。`'system node autosupport modify'`の詳細については、["ONTAPコマンド リファレンス"](#)を参照してください。
- どちらのプロトコルも、名前が解決されるアドレス ファミリーに応じてIPv4またはIPv6で転送されます。
- AutoSupportメッセージを送信するためにONTAPによって確立されたTCP接続は、一時的で短時間です。

HTTPS

これは最も堅牢な機能を提供します。次の点に注意してください。

- AutoSupport OnDemandと大容量ファイルの転送はサポートされません。
- 最初にHTTPS PUT要求が試行されます。要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。
- サーバがPUTをサポートしていない場合は、代わりにHTTPS POSTメソッドが使用されます。
- HTTPS転送のデフォルトの制限は50MBです。
- HTTPSプロトコルはポート443を使用します。

SMTP

原則として、HTTPSが許可されていない、またはサポートされていない場合にのみSMTPを使用してください。以下の点にご注意ください：

- ・AutoSupport OnDemandと大容量ファイルの転送はサポートされません。
- ・SMTPサインイン クレデンシャルが設定されている場合は、暗号化されずにクリア テキストで送信されます。
- ・転送のデフォルトの制限は5MBです。
- ・セキュアでないSMTPプロトコルはポート25を使用します。

TLSでSMTPセキュリティを強化

SMTPを使用する場合、すべてのトラフィックは暗号化されていないため、容易に傍受され、読み取られる可能性があります。ONTAP 9.15.1以降では、SMTPでTLS (SMTPLS) を使用することもできます。この場合、_explicit TLS_が使用され、TCP接続が確立された後にセキュアチャネルがアクティブ化されます。

SMTPLSには通常、次のポートが使用されます：ポート587

設定に関するその他の考慮事項

AutoSupportを設定する際は、さらにいくつかの考慮事項があります。

これらの考慮事項に関連するコマンドの詳細については、["AutoSupportのセットアップ"](#)を参照してください。

電子メールを使用してローカルコピーを送信する

NetAppへのAutoSupportメッセージの配信に使用されるプロトコルに関係なく、各メッセージのコピーを1つ以上のローカルEメール アドレスに送信することもできます。たとえば、社内のサポート部門やパートナー組織にメッセージを送信できます。



SMTPLS（またはSMTPLS）を使用してNetAppにメッセージを配信し、それらのメッセージのローカルEメール コピーも送信する場合は、同じEメール サーバ設定を使用します。

HTTPプロキシ

ネットワーク構成によっては、HTTPSプロトコルを使用するにはプロキシURLの追加設定が必要になる場合があります。HTTPSを使用してAutoSupportメッセージをテクニカルサポートに送信し、プロキシを使用している場合は、プロキシのURLを指定する必要があります。プロキシがデフォルト（ポート3128）以外のポートを使用している場合は、そのプロキシのポートを指定できます。また、プロキシ認証用のユーザー名とパスワードも任意で指定できます。

サーバ証明書のインストール

TLS（HTTPSまたはSMTPLS）を使用する場合、サーバからダウンロードされた証明書は、ルートCA証明書に基づいてONTAPによって検証されます。HTTPSまたはSMTPLSを使用する前に、ルート証明書がONTAPにインストールされていること、およびONTAPがサーバ証明書を検証できることを確認する必要があります。この検証は、サーバ証明書に署名したCAに基づいて実行されます。

ONTAPには、多数のルートCA証明書がプリインストールされています。多くの場合、サーバの証明書は追加の設定なしでONTAPによってすぐに認識されます。サーバ証明書の署名方法によっては、ルートCA証明書と中間証明書のインストールが必要になる場合があります。

必要に応じて、以下の手順に従って証明書をインストールしてください。必要な証明書はすべてクラスタレベルでインストールする必要があります。

例 1. 手順

System Manager

1. System Managerで、クラスター > *設定*を選択します。
2. *セキュリティ*セクションまで下にスクロールします。
3. *証明書*の横にある → を選択します。
4. *信頼された証明機関*タブで*追加*をクリックします。
5. *Import*をクリックし、証明書ファイルを選択します。
6. 環境に合わせて、パラメータの設定を完了します。
7. *[追加]*をクリックします。

CLI

1. インストールを開始します。

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

`security certificate install`
の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html>["ONTAPコマンド リファレンス"]をご覧ください。

2. 次のコンソール メッセージを探します。

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

3. テキストエディタで証明書ファイルを開きます。
4. 次の行を含めて、証明書全体をコピーします。

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

5. コマンドプロンプトの末尾に証明書を貼り付けます。
6. **Enter** を押してインストールを完了します。
7. 次のいずれかのコマンドを実行して、証明書がインストールされていることを確認します：

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

```
security certificate show
```

`security certificate show`
の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-certificate-show.html> ["ONTAPコマンド リファレンス" ^]をご覧ください。

関連情報

- ・ "AutoSupportのセットアップ"
- ・ "ONTAPコマンド リファレンス"

ONTAP AutoSupportのセットアップ

AutoSupportメッセージをNetAppテクニカル サポートに配信し、社内のサポート部門にEメール コピーを送信するように、ONTAPクラスタを設定できます。その一環として、本番環境で使用する前に構成をテストすることもできます。

タスク概要

ONTAP 9.5以降では、クラスタ内のすべてのノードに対してAutoSupportを同時に有効化および設定できます。新しいノードがクラスタに参加すると、そのノードは自動的に同じAutoSupport設定を継承します。これをサポートするため、CLIコマンド `system node autosupport modify` のスコープはクラスタレベルです。`-node` コマンドオプションは下位互換性のために保持されていますが、無視されます。



ONTAP 9.4以前のリリースでは、`system node autosupport modify` コマンドは各ノードに固有です。クラスタでONTAP 9.4以前を実行している場合は、クラスタ内の各ノードでAutoSupport を有効化および設定する必要があります。

開始する前に

AutoSupportメッセージをNetAppに配信する際の推奨される転送設定はHTTPS（TLSを使用したHTTP）です。このオプションは、最も堅牢な機能と最高レベルのセキュリティを提供します。

ONTAPクラスタを構成する前に、詳細については["AutoSupportを使用するための準備"](#)を確認してください。

手順

1. AutoSupportが有効になっていることを確認します。

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

2. NetAppテクニカル サポートがAutoSupportメッセージを受信できるようにするには、次のコマンドを使用します。

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

AutoSupportでAutoSupport OnDemandを使用可能にする場合や、大容量ファイル（コアダンプファイルやパフォーマンスアーカイブファイルなど）をテクニカルサポートまたは指定のURLにアップロードする場合は、このオプションを有効にする必要があります。



HTTPS転送プロトコルを使用してテクニカルサポートにメッセージを送信するよう設定している場合は、AutoSupport OnDemandがデフォルトで有効になっており、機能しています。

3. NetAppテクニカルサポートがAutoSupportメッセージを受信できるように設定した場合は、これらのメッセージに使用するトランスポートプロトコルを指定します。

次のオプションから選択できます。

状況	次に、 <code>system node autosupport modify</code> コマンドの次のパラメータを設定します...
デフォルトのHTTPSプロトコルを使用する	<ol style="list-style-type: none">`-transport` を `https` に設定します。プロキシを使用する場合は、`-proxy-url` をプロキシのURLに設定してください。この設定は、AutoSupport OnDemandとの通信と大きなファイルのアップロードをサポートします。
SMTPを使用する	<p>`-transport` を `smtp` に設定します。</p> <p>この設定では、AutoSupport OnDemandや大容量ファイルのアップロードはサポートされません。</p>

4. 社内のサポート部門またはサポートパートナーにAutoSupportメッセージを送信するには、次の操作を実行します。

- a. `system node autosupport modify` コマンドの次のパラメータを設定して、組織内の受信者を識別します：

設定するパラメータ	パラメータの値
-to	重要なAutoSupportメッセージを受信する社内サポート組織内の最大5つの個別の電子メールアドレスまたは配布リストをコンマで区切って指定します
-noteto	携帯電話やその他のモバイルデバイス向けに設計された重要なAutoSupportメッセージの短縮版を受信する、社内サポート組織内の最大5つの個別の電子メールアドレスまたは配布リスト（カンマで区切る）

-partner-address	すべてのAutoSupportメッセージを受信するサポート パートナー組織内の最大 5 つの個別の電子メール アドレスまたは配布リストをコンマで区切って指定します
------------------	---

- b. `system node autosupport destinations show` コマンドを使用して宛先を一覧表示し、アドレスが正しく設定されていることを確認します。
5. 前の手順で社内サポート組織の受信者アドレスを構成した場合、またはテクニカル サポートへのメッセージに SMTP トランスポートを選択した場合は、`system node autosupport modify` コマンドの次のパラメータを設定して SMTP を構成します：
- `mail-hosts` を、カンマで区切った 1 つ以上のメール ホストに設定します。
最大5件のメール ホストを設定できます。
メール ホスト名の後にコロンとポート番号を指定することにより、各メール ホストのポート値を設定できます：たとえば、`mymailhost.example.com:5678`では、5678がメール ホストのポートです。
 - `from` をAutoSupportメッセージを送信するメールアドレスに設定します。
6. DNS を設定します。
7. (オプション) 特定の設定を変更する場合は、コマンドのオプションを追加します。

実行する処理	次に、`system node autosupport modify` コマンドの次のパラメータを設定します...
メッセージ内の機密データの削除、マスキング、またはエンコーディングによってプライベート データを非表示にする	`remove-private-data` を `true` に設定します。 `false` から `true` に変更すると、すべてのAutoSupport履歴とすべての関連ファイルが削除されます。
定期的なAutoSupportメッセージでのパフォーマンス データの送信を停止する	`perf` を `false` に設定します。

8. SMTPを使用してAutoSupportメッセージをNetAppに配信する場合は、必要に応じてTLSを有効にしてセキュリティを強化できます。

- a. 新しいパラメータに使用できる値を表示します。

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

- b. SMTPメッセージ配信に対してTLSを有効にします。

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

- c. 現在の設定を表示します。

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

9. `node` パラメータを指定した `system node autosupport show` コマンドを使用して、全体的な構成を確認します。

10. `system node autosupport check show` コマンドを使用して AutoSupport 操作を確認します。

問題が報告された場合は、 `system node autosupport check show-details` コマンドを使用して 詳細情報を表示します。

11. AutoSupport メッセージが送受信されていることをテストします。

- a. `system node autosupport invoke` コマンドを `type` パラメータを `test` に設定して使用します：

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

- b. NetApp が AutoSupport メッセージを受信していることを確認します。

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

最新の送信 AutoSupport メッセージのステータスは、すべての適切なプロトコルの宛先に対して最終的に `sent-successful` に変更されるはずです。

- c. オプションで、 `system node autosupport modify` コマンドの `--to`、`-noteto`、または `partner-address` パラメータに設定したアドレスの電子メールをチェックして、AutoSupport メッセージが社内のサポート組織またはサポート パートナーに送信されていることを確認します。

関連情報

- ["AutoSupport を使用するための準備"](#)
- ["ONTAP コマンド リファレンス"](#)

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。