



テクニカル レポート

AutoSupportとAutoSupport On Demand の設定

NetApp
Brett Albertson
2023年8月 | TR-4444

概要

このガイドは、NetApp®ストレージシステムでAutoSupport™およびAutoSupport On Demand™を設定する際に、お客様、パートナー、およびNetAppを支援することを目的としています。

ご意見やご質問は、ng-activeiq-feedback@netapp.comまでEメールでお問い合わせください

<<本レポートは機械翻訳による参考訳です。公式な内容はオリジナルである英語版をご確認ください。>>

目次

はじめに.....	3
AutoSupport	3
AutoSupportのメリット	3
Data ONTAPでのAutoSupportの管理	4
Active IQデジタルアドバイザー	6
AutoSupportオンデマンド	7
AutoSupportオンデマンドのメリット.....	7
AutoSupportオンデマンドセキュリティ.....	7
Data ONTAP でのAutoSupportの設定.....	9
Data ONTAP でのAutoSupportのセットアップ.....	10
AutoSupport構成のテスト	14
EシリーズでのAutoSupportの設定	15
StorageGRIDでのAutoSupportの設定.....	15
SolidFireおよびHCIでのAutoSupportの設定.....	15
Data ONTAPでのAutoSupportのトラブルシューティング	16
メッセージが受信されない場合のAutoSupportのトラブルシューティング	16
HTTPS経由のAutoSupportのトラブルシューティング	16
SMTP経由のAutoSupportのトラブルシューティング	17
AutoSupportのコンテンツの切り捨て (AutoSupport予算)	19
証明書検証が有効な状態でHTTPS経由で送信されたAutoSupportメッセージをNetAppが受信しない.....	22
追加情報.....	24
バージョン履歴.....	24

表一覧

表1) AutoSupportメッセージ	5
----------------------------	---

図一覧

図1) Active IQデジタルアドバイザーのメインダッシュボード.....	6
図2) AutoSupport On Demandのデータフロー.....	8
図3) HTTPS暗号化通信図.....	23

はじめに

AutoSupport™(ASUP™)は、テレメトリデータを含むメッセージをNetAppに送信するメカニズムです。このデータによって、多くのツール、サポートユースケース、サポートケースの自動化など、その他のデータワークフローが可能になります。システムでAutoSupportを有効にすると、サポートケースの迅速な解決とシステムのアップタイムの最大化を目的としたサポートツールの基本データが提供されます。

テクニカルサポートへのAutoSupportメッセージの送信はデフォルトで有効になっていますが、無効にすることもできます。転送方法や、メッセージを社内のサポート部門またはパートナーのサポート部門にコピーするなどのオプションを設定できます。

このドキュメントでは、ONTAPベースのストレージシステムでAutoSupportおよびAutoSupport On Demandを設定するために必要な手順について説明します。また、他のタイプのNetAppストレージシステムへのリンクも含まれています。

AutoSupport

AutoSupportは、Data ONTAP®オペレーティングシステムソフトウェアなどのNetApp®ストレージオペレーティングシステムの機能であり、統合された効率的な監視およびレポート機能やサポートデータ収集のためのデータを提供します。AutoSupportを使用すると、システムの健全性ステータスメッセージをNetApp、パートナー、および自社に直接送信できます。サポートインシデントが発生した場合は、NetAppなどの指定された宛先に情報が自動的に送信され、インシデントを迅速に解決できます。また、AutoSupportは定期的に診断データをNetAppに送信し、将来のシステムの安定性とパフォーマンスに影響する可能性がある既知の問題やリスクがないかどうかを自動的に分析します。お客様がこのデータにアクセスするための主要なツールの1つがActive IQデジタルアドバイザーです。このアドバイザーには、AIと機械学習の手法を使用した予測的かつプロアクティブな推奨事項が含まれています。Active IQデジタルアドバイザーは、NetAppの主要なAIOpsプラットフォームであり、そのすべてがAutoSupportデータの分析を通じて機能します。

AutoSupportのメリット

NetAppは、データセキュリティポリシーで禁止されている場合以外は、AutoSupportを有効にすることをベストプラクティスとして推奨しています。実際、AutoSupportを有効にすると、既存のセキュリティリスクを監査し、潜在的な攻撃ベクトルについて警告することで、セキュリティが強化されます。AutoSupportの機能を有効にして常に使用できる状態にしておくことには、多くのメリットがあります。

以下にその一部を紹介します。

- 重要なイベントに関する自動コールホーム機能—ハードウェア交換のリクエストなど、重要なイベントのサポートケースが自動的にオープンされます。
- 問題発生時にお客様の妨げにならない形で通知し、修正措置を講じるための情報をNetAppに転送
- Active IQデジタルアドバイザーやBlueXPなどの分析ツールを使用して、構成に関する既知の問題に関するメッセージを監視
- 数百ものシステムパラメータを対象とした継続的な健全性チェック分析と、検出された問題を解決策情報にインテリジェントにリンク
- 返品承認 (RMA) リクエストへのお客様の対応なし
- システムアラートをNetAppとお客様指定の通知先に送信
- Active IQ、BlueXP、System Managerなどの強力なツール
- サポート契約の更新、アドオン、機器更改 (Tech Refresh) アクティビティなどのワークフローを実現

AutoSupportのデータをNetAppに送信することができない場合でも、サポートが必要な問題にとってこのデータは重要な要素です。サポートケースがオープンされた場合、NetAppサポートは、トラブルシューティングを迅速に行うために、AutoSupportメッセージを手動で再送信または転送するよう要求します。

Data ONTAPでのAutoSupportの管理

ONTAPでは、クラスタ管理者のみがAutoSupport管理を実行できます。Storage Virtual Machine (SVM) 管理者がAutoSupportにアクセスすることはできません。

AutoSupportはいつでも無効にできますが、常に有効にしておくことを推奨します。AutoSupportを有効にしておくと、ストレージシステムに問題が発生したときに、迅速に原因を突き止めて解決できます。AutoSupportの情報は、AutoSupportを無効にしている場合でも、デフォルトで収集されてローカルに格納されます。

AutoSupportは、ストレージの初回の設定時にデフォルトで有効になり、AutoSupportは、システムの初回電源投入から24時間後にNetAppサポートへのメッセージ送信を開始します。この間隔を24時間より短くするには、システムをアップグレードまたはリバートするか、AutoSupport設定を変更するか、システム時間を24時間以外に変更します。

AutoSupportは、メッセージの種類に応じた宛先にメッセージを送信します。AutoSupportがメッセージを送信するタイミングと場所を把握することは、電子メールで受信したメッセージやActive IQデジタルアドバイザーで表示されたメッセージを理解するのに役立ちます。

Active IQデジタルアドバイザーは、NetApp Support Siteの一部であるWebベースのアプリケーションです。システムから受信したAutoSupportメッセージを集約し、推奨事項やビューを提供して、システムの可用性と効率を向上させます。詳細については、[Active IQデジタルアドバイザーのマニュアル](#)を参照してください。

修正措置を必要とするシステムでイベントが発生した場合には、AutoSupportからイベントトリガー型メッセージが自動的に送信されます。

AutoSupportは、次のプロセスを使用してイベントトリガー型AutoSupportメッセージを作成し、送信します。

1. ノードのイベント管理システム (EMS) がトリガー イベントを処理すると、EMSがAutoSupportモジュールに要求を送信します。

トリガーイベントは、AutoSupportのデスティネーションと callhome. プレフィックスで始まる名前を含むEMSイベントです。

2. AutoSupportによってイベントトリガー型AutoSupportメッセージが作成されます。

AutoSupportは、トリガーに関連付けられたサブシステムから基本的な情報とトラブルシューティング情報を収集し、トリガー イベントに関連する情報のみが含まれたメッセージを作成します。各トリガーには一連のデフォルトのサブシステムが関連付けられていますが、system node autosupport trigger modify コマンドを使用すると、トリガーに関連付けるサブシステムを追加で選択できます。

3. AutoSupportは system node autosupport modify -to-noteto、`-partner-address`、の `-support` 各パラメータを使用して、コマンドで定義した受信者にイベントトリガー型AutoSupportメッセージを送信します。

system node autosupport trigger modify コマンドで `-to -noteto` パラメータとパラメータを指定すると、特定のトリガーに対するAutoSupportメッセージの配信を有効または無効にできます。

また、AutoSupportはいくつかのメッセージを定期的に送信します。AutoSupportメッセージは手動で送信または再送信できます。NetAppテクニカルサポートは、AutoSupportオンデマンド機能を使用してAutoSupportからのメッセージを要求できます。

表1に、AutoSupportメッセージの種類とその内容を示します。

表1) AutoSupportメッセージ

メッセージの種類	メッセージに含まれるデータの種類
イベントトリガー型	イベントに関連する特定のサブシステムについての状況に応じたデータが含まれるファイル
毎日	ログ ファイル
パフォーマンス	過去24時間以内にサンプリングされたパフォーマンス データ
毎週	設定データおよびステータス データ
system node autosupport invoke コマンドによるトリガー	<p>-type パラメータで指定した値によって異なります。</p> <ul style="list-style-type: none"> test いくつかの基本データを含むユーザトリガー型メッセージを送信します。また、-to オプションを使用すると、テクニカルサポートからの自動応答Eメールが指定したEメールアドレス宛てに送信されるため、AutoSupportメッセージが受信されていることを確認できます。 performance パフォーマンスデータを送信します。 all 各サブシステムのトラブルシューティングデータを含む一連のデータを含むユーザトリガー型メッセージを送信します。一般に、テクニカル サポートからはこのメッセージが要求されます。
system node autosupport invoke-core- upload コマンドによるトリガー	<p>ノードのコア ダンプ ファイル</p> <p>このコマンドは、NetAppサポート ケース番号を指定して呼び出すこともできます。ケース番号を指定すると、アップロードされたコア ダンプ ファイルが正しいテクニカル ケースに関連付けられるため、問題を早期に解決できます。</p> <p>例：</p> <pre>cluster1::> system node autosupport invoke-core-dump -core-filename core.4070309011.2014-12-20.17_06_03.nz -message "Latest core of problem" -case-number 2006123456</pre>
system node autosupport invoke- performance-archive コマンドによるトリガー	<p>指定した期間のパフォーマンスアーカイブファイル。</p> <p>このコマンドは、ケース番号を指定して呼び出すこともできます。ケース番号を指定すると、アップロードされたパフォーマンス アーカイブが正しいテクニカル ケースに関連付けられるため、問題を早期に解決できます。</p> <pre>cluster1::> system node autosupport invoke-performance-archive -start-date 12/20/2014 19:19:47 -end-date 12/20/2014 25:00:00 -message "Some perf date for 12/20" -case-number 2006123456</pre>
NetAppサポートがAutoSupport On Demandを使用してトリガー	<p>AutoSupport On Demandでは、処理に失敗したメッセージを再転送したり、リモートの指示 (CLIが提供するAutoSupportのinvokeコマンドに相当) をリレーできます。</p> <ul style="list-style-type: none"> system node autosupport invoke system node invoke-performance-archive system node autosupport invoke-core-upload system node invoke-diagnostic (診断モード)

Active IQ Digital Advisor

Active IQ デジタルアドバイザーはWebベースのアプリケーションで、AutoSupportなどのデータソースの情報を使用して予測に基づくプロアクティブなインサイトを提供し、可用性、効率性、パフォーマンスの向上を支援します。

Active IQ デジタルアドバイザーポータルを継続的に監視し、サポート情報が送信されていないシステムを確認することが重要です。これは、サポート問題を迅速に解決するために重要な情報です。プロアクティブで予測性に優れたAutoSupportの特長を活かせば、リスクを最小限に抑えて問題を未然に防止することができます。

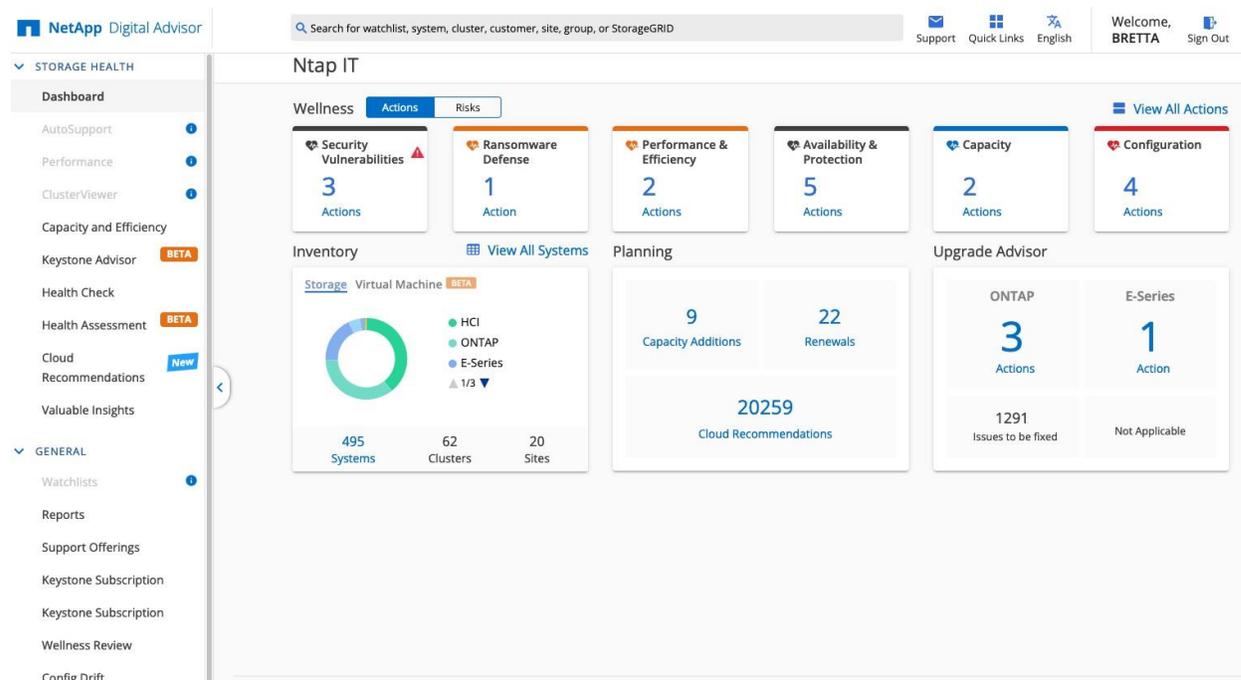
システムがNetAppにデータを送信するよう、AutoSupportを有効にして設定しておく必要があります。

Active IQ デジタルアドバイザーのメリット：

- ノード、クラスター、サイト、お客様、監視リストと呼ばれるグループを表示できます。
- ストレージ容量の増大を予測し、容量追加の時期を特定
- ONTAPシステムのアップグレードを推奨し、アップグレード計画を提示
- 設定上の問題や既知のバグに関連するシステム リスクをプロアクティブに特定
- NetAppシステムの管理を容易にする、設定、容量、効率性、パフォーマンスに関するビューとレポートを提供
- レポートを生成します

Active IQ デジタルアドバイザーにアクセスするには、<https://activeiq.netapp.com/>にアクセスします。

図1) Active IQ デジタルアドバイザーのメインダッシュボード



NetAppストレージのシリアル番号かシステムID、またはサイト名を検索ボックスに入力します。ダッシュボードが開き、NetAppに送信された最新のAutoSupport情報が表示されます。

AutoSupport On Demand

AutoSupport On Demand (AOD) は、ケースを解決するためにAutoSupport情報を収集する機能で、収集に際してお客様の介入は必要ありません。AutoSupport On Demandを使用すると、定期的なAutoSupportメッセージの送信を待たずにAutoSupportメッセージがオンデマンドで送信されます。

AutoSupport On Demandは、Data ONTAPのAutoSupport機能に欠かせないソリューションです。HTTPS経由でAutoSupportメッセージを配信するように設定されたData ONTAPストレージシステムは、テクニカルサポートと定期的に通信し、AutoSupportメッセージの処理（配信、再配信、拒否）に関するAutoSupport On Demandの配信指示を受け取ります。

AutoSupport On Demandのメリット

カスタマーサポートの満足度が向上

- お客様が時間を割いてトラブルシューティング用の診断データを収集する必要がない
- 最小限のお客様の構成でNetAppのケース

を迅速に解決

- 最新の診断情報と設定情報を確認
- NetAppのサポートおよびサポートパートナーは、営業時間外でも、お客様の関与なしに、必要なすべての情報を取得できます。
- 一時的なネットワークや配信の問題で失われたASUP情報を再配信可能なため、AutoSupportの信頼性が向上

AutoSupport On Demandのセキュリティ

AutoSupport On Demandは、NetApp AutoSupportにシームレスかつセキュアに統合されています。

- On Demandの指示はすべて、ストレージシステムからのクエリーに対する応答として、暗号化されたHTTPS経由で送信されます（アウトバウンド通信のみ）。
- On Demandで使用できるのは、事前定義された以下のAutoSupport指示のみです。
 - システムの現在の状態を判断するために、最新のAutoSupportデータの収集を要求する
 - 複雑なケースを解決するために、必要に応じてより詳細なAutoSupportデータ（ASUP診断メッセージ、コアファイル、パフォーマンスアーカイブ）を要求する
- On Demandは、NetAppサポートサイトの有効なクレデンシアルを持つ、業務上適切な立場にあるユーザー（テクニカルサポートエンジニア、サポートアカウントマネージャー、所定のストレージシステムの操作を許可されたサポートパートナー）のみが使用できます。
- On Demandでは処理の透明性が確保されています。
 - お客様は、事前定義された配信指示をData ONTAPのCLIを使用してすべて確認し、実行することができる
 - 設定により、お客様やパートナーにAutoSupportメッセージのコピーが送信される
 - On Demandの使用状況は追跡および表示可能
 - On Demandの要求は毎日管理ログに記録される
 - 生成されたAutoSupportメッセージはタイトルに「On Demand」と記載され、Active IQから確認できる

AutoSupport On Demandの仕組み

AutoSupport On Demandは次のコンポーネントで構成されています。

- 各ノードで稼働するAutoSupport On Demandクライアント

- NetAppのテクニカル サポートで稼働するAutoSupport On Demandサービス

AutoSupport On Demandクライアントは、AutoSupport On Demandサービスを定期的にポーリングし、テクニカル サポートから配信指示を取得します。たとえば、テクニカル サポートは、AutoSupport On Demandサービスを使用して、新しいAutoSupportメッセージを生成するよう要求できます。AutoSupport On DemandクライアントはAutoSupport On Demandサービスをポーリングして、配信指示を取得し、要求に応じて新しいAutoSupportメッセージをオンデマンドで配信します。

AutoSupport On Demandは、以下の最小要件を満たしたシステムでデフォルトで有効になります。

- AutoSupportが有効になっている
- 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AutoSupportが設定されている
- ストレージコントローラでONTAP 8.2以降が実行されている。

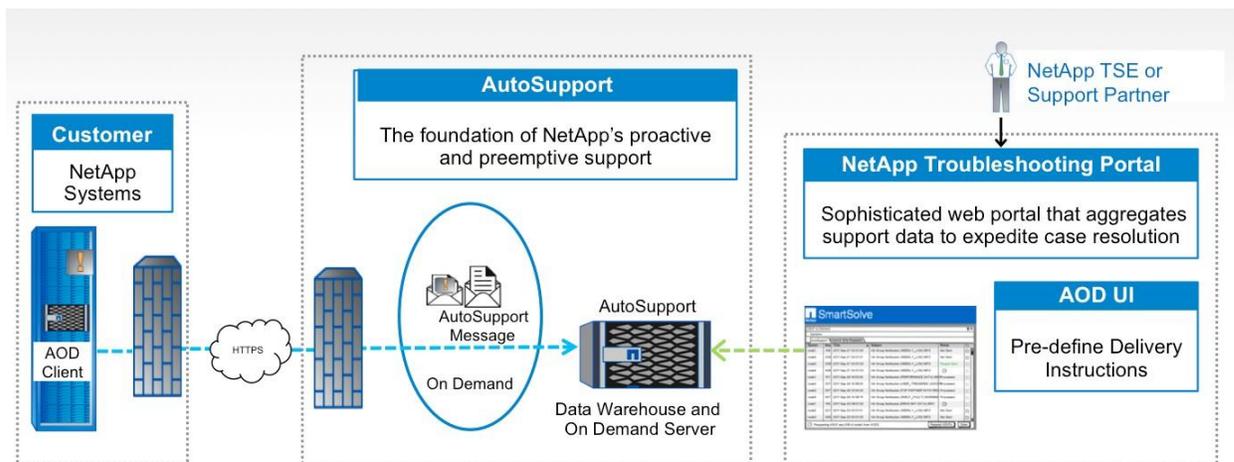
AutoSupport On Demandクライアントは、AutoSupportメッセージの送信先と同じテクニカル サポートにHTTPS要求を送信します。AutoSupport On Demandクライアントは、着信接続は受け入れません。

注： AutoSupport On Demandでは、事前定義された「AutoSupport」ローカルユーザアカウントを使用して、AutoSupport On Demand機能の管理を容易にします。このアカウントを削除することはできません。

AutoSupport On Demandを無効にし、AutoSupportは有効なまま、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に設定する場合は、テクニカルサポートにお問い合わせください。

図3に、AutoSupport On Demandがテクニカル サポートにHTTPS要求を送って配信指示を取得する処理を示します。

図2) AutoSupport On Demandのデータフロー



AutoSupport On Demand available for Data ONTAP® 8.2 + systems and HTTPS only

配信指示には、AutoSupportが行う処理として、次の要求を含めることができます。

- 新しいAutoSupportメッセージの生成（テクニカル サポートは、問題の優先度を選別するために新たなAutoSupportメッセージを要求することがあります）

- コア ダンプ ファイルやパフォーマンス アーカイブ ファイルをNetAppサポート サイトにアップロードする、新しいAutoSupportメッセージの生成（テクニカル サポートは、問題の優先度を選別するためにコア ダンプ ファイルやパフォーマンス アーカイブ ファイルを要求することがあります）
- 以前生成したAutoSupportメッセージの再配信（再配信は、配信エラーやOn Demandの処理の延期が原因でメッセージを受信できなかった場合に、手動または自動で要求できます）
- 特定のトリガー イベントに対してAutoSupportメッセージの配信を延期（テクニカル サポートは、ほとんど必要ないデータや冗長なデータの配信を無効化することがあります）

Data ONTAPでのAutoSupportの設定

この章では、Data ONTAPシステムでAutoSupportを設定する方法について詳しく説明し、基本的なシステム要件について説明します。

AutoSupportの要件

セキュリティを確保し、AutoSupportの最新機能をすべてサポートするには、HTTPSを使用してAutoSupportメッセージを配信します。AutoSupportではAutoSupportメッセージの配信にSMTPがサポートされていますが、HTTPSが推奨されます。

注: HTTPの使用は廃止されました。

サポートされるプロトコル

HTTPS

HTTPSはTCPポート443を使用します。HTTPSはデフォルトの転送プロトコルです。このプロトコルでは、AutoSupport On Demandと大容量ファイルのアップロードがサポートされます。

AutoSupportメッセージの送信にHTTPSを使用すると、NetApp AutoSupportサーバのX.509証明書が認証され、メッセージのコンテンツが暗号化されます。

NetAppは以下の理由から、AutoSupportメッセージの配信にHTTPS転送プロトコルを使用することを強く推奨しています。

- SMTPよりもはるかにセキュアで信頼性が高い
- SMTPのようにEメール サイズが制限されない
- 設定と管理が容易
- お客様の社内担当者やシステム向けのSMTPによる配信との併用が可能
- AutoSupport On Demandの機能を統合してケースを早期に解決できる

SMTP

- SMTPはTCPポート25を使用します。AutoSupportでは別のポートを使用するように設定できます。
- このプロトコルは、ネットワーク接続でHTTPSが許可されない場合にのみ使用してください。
- このプロトコルでは、大容量ファイルのアップロードやAutoSupport On Demandはサポートされません。
- SMTPデータはノードによって暗号化されませんが、最新のメールサーバのほとんどは社外に送信されるSMTPメッセージを暗号化します。NetAppは暗号化SMTPの受信をサポートします。
- SMTPインフラでは、メッセージ サイズが大幅に制限されます。

外部メール サーバ

SMTPを使用して社内のサポート部門やテクニカル サポートにAutoSupportメッセージを送信する場合は、外部のメール サーバを設定する必要があります。ストレージ システムはメール サーバとしては機能しないため、メール送信用に外部のメール サーバが別途必要になります。このメール サーバにはSMTPポート (25)

または別のポートをリスンするホストを使用し、8ビットのMultipurpose Internet Mail Extensions (MIME) エンコーディングを送受信するように設定する必要があります。メールホストには、たとえば、SMTPサーバ (sendmailプログラムなど) を実行するUNIXホストや、Microsoft Exchangeサーバを実行するWindowsサーバなどを使用できます。メールホストは1つでも複数でもかまいません。

AutoSupportに社内のサポート部門またはサポートパートナーのEメールアドレスが指定されている場合、それらのアドレスへのメッセージは常にSMTPで送信されます。たとえば、テクニカルサポートに推奨されるHTTPSプロトコルを使用してメッセージを送信し、同時に社内のサポート部門にもメッセージを送信する場合、それぞれHTTPSとSMTPを使用して送信されます。

AutoSupportのペイロード

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。HTTPS転送のデフォルト設定は、50MB (ONTAP 9以降) または10MB (Data ONTAP 8.3以前) です。SMTPのデフォルト設定は5MBです。AutoSupportメッセージのサイズが設定した制限を超えた場合、メッセージの一部が最大サイズの範囲で配信されます。コアダンプファイルまたはパフォーマンスアーカイブファイルをアップロードするAutoSupportメッセージを生成してNetApp Support Siteまたは指定したURLに送信すると、AutoSupportはHTTPSプロトコルの最大サイズ制限を自動的に上書きします。

Data ONTAPでのAutoSupportのセットアップ

このセクションでは、NetApp AFF、FAS、ASA、CVO、FlexArrayでAutoSupportをセットアップする手順を説明します。およびVシリーズストレージコントローラ

DNSを設定する

DNSは、AutoSupportのHTTPやHTTPSの送信先URL、および (IPアドレスではなくホスト名を使用する場合は) ホスト名を解決するために必要です。

ONTAPの場合

1. クラスタでDNSを有効にします。

```
vserver services name-service dns create -vserver cluster_name -domains domainname -name-servers ip_address -state enabled
```

ファイアウォールでONTAPのIPアドレスを許可する (該当する場合)

1. ONTAP AutoSupportメッセージをHTTPS経由でNetAppに送信するためには、ONTAPクラスタのノード管理とクラスタ管理の論理インターフェイス (LIF) をすべて許可する必要があります。
2. サービスプロセッサのAutoSupportメッセージは、SMTP経由でのみ送信されます。
3. SMTP経由のONTAP AutoSupportメッセージの場合は、ローカルのSMTPゲートウェイに到達し、autosupport@netapp.com への電子メール送信を許可する必要があります。

AutoSupportが有効なことを確認する

AutoSupportメッセージを受信するには、AutoSupportを有効にする必要があります。

ONTAPの場合

1. `-state system node autosupport modify` コマンドのパラメータをenableに設定します。

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

2. テクニカルサポートにAutoSupportメッセージを送信する場合は `- support system node autosupport modify`、コマンドのパラメータをenableに設定します。

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

AutoSupportでAutoSupport On Demandを使用できるようにする場合や、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。これらのコマンドは、クラスタの全ノードで実行する必要があります。新しいノードがクラスタに追加された場合、そのノードのAutoSupportを既存のノードに合わせて設定することが重要です。

メッセージの転送プロトコルを指定する

AutoSupportメッセージの送信に使用する転送プロトコルを指定します。

ONTAPの場合

1. デフォルトのプロトコルはHTTPSです。SMTPは、ネットワーク接続でHTTPSが許可されていない場合にのみ使用してください。-transport パラメータを使用して転送プロトコルを設定します。

```
system node autosupport modify -node nodename -transport protocol
```

2. 転送プロトコルとしてHTTPSを選択し、プロキシを使用する場合は、を -proxy-url プロキシのURLに設定します。

```
system node autosupport modify -node nodename -proxy-url proxyurl
```

これらのコマンドは、クラスタの全ノードで実行する必要があります。新しいノードがクラスタに追加された場合、そのノードのAutoSupportを既存のノードに合わせて設定することが重要です。

HTTPSシステムのプロキシ設定の詳細の指定

-transport パラメータがHTTPSに設定されていて、組織でプロキシを使用している場合。

-proxy-url パラメータを使用して、HTTPまたはHTTPSプロキシを指定します。

形式: [-proxy-url <text>] - Support Proxy URL:Port

例:

```
system node autosupport modify -node nodename -proxy-url proxyurl:8080
```

注:

- URLは、先頭にhttp://またはhttps://を付けずに入力します。
- HTTPはTCPポート80を使用します。
- NetAppでは、**HTTP/1.1** 準拠のプロキシを使用することを推奨しています。HTTP/1.0のプロキシを使用している場合、Transfer-Encodingヘッダに関連する互換性の問題を解決するために、AutoSupport On Demandの機能を有効にする設定が追加で必要になる場合があります。プロキシ認証も必要な場合は、URLにユーザ名とパスワードを含めます。形式:
"[username] : [password]@[host][: [port]]"

```
system node autosupport modify -node nodename -proxy-url user1:mypass@proxyurl:8080
```

- 指定しない場合、デフォルトのパスワードは空の文字列です。疑問符を含むプロキシを指定するには、Escキーを押してから「?」と入力します。
- Data ONTAP 8.3以前では、「autosupport show」と「options autosupport」のどちらの出力にも、パスワードはプレーンテキストで表示されます。
- ONTAP 9.0以降では、パスワードの入力にはセキュアな対話方式（パスワードを2回入力）が使用されています。さらに、各種のクラスタシェルCLIコマンド（autosupport show、autosupport check show）では、URLテキストにパスワードが「*****」と表示されます。
- ONTAP 9.0以降では、ノードシェル / dBlade CLIの「options」の出力から、AutoSupportオプションがすべて削除されています。

例 :

```
Support URL for HTTP/S PUT: support.netapp.com/put/AsupPut
Support Proxy URL: andris:*****@proxy.netapp.com:8080
Support Address: autosupport@netapp.com
```

SMTP転送用メール サーバを設定する

ストレージノードからEメールベースのメッセージをルーティングできるEメールサーバの名前またはIPアドレスを設定します。この設定は、お客様の社内のサポート部門やサポートパートナーにAutoSupportメッセージを届けたり、NetAppへの転送プロトコルにSMTPを使用する場合に必要です。

ONTAPの場合

1. 次のコマンドを使用してメールホストを設定します。各メールホストのポートを設定するには、メールホスト名に続けてコロンとポート番号を入力します。メールホストは5つまで設定できます。

```
system node autosupport modify -node nodename -mail-hosts mailhost:port
```

2. `-from` AutoSupportメッセージを送信する電子メールアドレスを設定します。
3. `-to`、`-noteto`、`-partner-address` の各パラメータを設定して、AutoSupportメッセージを受信するEメールアドレスを設定します。`-noteto` 受信者は、携帯電話やその他のモバイルデバイス用に指定された主要なAutoSupportメッセージの短縮バージョンを受け取ります。Eメールアドレスはパラメータごとに5つまで設定できます。
4. アドレスが正しく設定されていることを確認するには、次のコマンドを使用します。

```
system node autosupport destinations show
```

その他のAutoSupportオプションを設定する

ONTAPの場合

1. メッセージ内の機密データを削除、マスキング、またはエンコードしてプライベートデータを非表示にするには、`-remove-private-data` に設定しtrueます。falseをtrueに変更すると、AutoSupportの履歴と関連するファイルがすべて削除されます。
2. 定期的なパフォーマンスAutoSupportメッセージの送信を停止するには、`set -perf` を false参照してください。

注 :

- すべてのAutoSupportコンテンツはさまざまなNetAppツールによる監視とトラブルシューティングに使用されるため、AutoSupportコンテンツを制限してパフォーマンスデータを無効にすることは推奨されません。
- 「minimal」や「remove-private-data」を有効にすると、パフォーマンス データやSnapshotのAutoSupportで1時間ごとのパフォーマンス データが送信されなくなります。
- 「minimal」や「remove-private-data」を有効にした場合、手動のAutoSupportやAutoSupport On Demandでこの設定を上書きすることはできません。

パフォーマンスアーカイブ : ONTAP 8.3以降でのパフォーマンスの最初の障害データ収集

ONTAP 8.3以降では、パフォーマンスコンテンツがデフォルトで収集され、すべてのシステムに格納（アーカイブ）されます。このコンテンツは、診断目的でData ONTAPノードごとに最大28日間、QoSパフォーマンス統計をボリューム単位で自動的に格納するData ONTAPの新機能をベースに構築されています。

AutoSupportインフラを使用して、パフォーマンス アーカイブを作成してNetAppにアップロードすることができます。

パフォーマンス アーカイブが無効の場合、EMSイベントが次のメッセージをレポートします。

パフォーマンス アーカイブを有効にするには、テクニカル サポートにご連絡ください。

```
::*> event log show -event perf*
Time                Node                Severity            Event
-----
INFORMATIONAL perf.ccma.off: Performance archiver is not enabled.
```

パフォーマンスアーカイブのアップロード

'system node autosupport invoke-performance-archive' 次のオプションを指定してサブコマンドを実行します。

```
-start-date <"MM/DD/YYYY HH:MM:SS">
-duration <[<integer>h][<integer>m][<integer>s]> (or -end-date)
-node *
-case-number <text>
```

1回のデータ収集時間は最大で6時間ですが、推奨されるサンプリング時間は4時間です。パフォーマンスアーカイブは、HTTPまたはHTTPS経由でのみアップロードできます。SMTPは、パフォーマンスアーカイブのアップロード方法として現在サポートされていません。パフォーマンス アーカイブは、AutoSupport On Demandを使用してトラブルシューティング目的でも要求できます。

AutoSupportの設定全体を確認する

ONTAPの場合

次のコマンドを実行して、設定全体を確認します。クラスタ内のすべてのノードで値が同じである必要があります。

```
cluster1::> system node autosupport show -node nodename -instance
Node: node1
State: enable
SMTP Mail Hosts: mailhost
From Address: Postmaster
List of To Addresses: me@itsupport.com
List of Noteto Addresses: alerts@itsupport.com
List of Partner Addresses: -
Send AutoSupport Messages to Vendor Support: enable
Protocol to Contact Support: https
Support URL for HTTP/HTTPS: support.netapp.com/asupprod/post/1.0/postAsup
Support URL for HTTP/S PUT: support.netapp.com/put/AsupPut
Support Proxy URL:
Support Address: autosupport@netapp.com
Hostname Subject: false
NHT Enable: true
Performance Data Enable: true
Retry Interval: 4m
Retry Count: 15
Reminder Enable: true
Last Subject Sent: MANAGEMENT_LOG
Last Time Sent: 9/17/2017 00:25:09
Maximum HTTP Size: 50MB
Maximum SMTP Size: 5MB
Remove Sensitive Data: false
```

AutoSupport設定のテスト

設定が終わったら、AutoSupportをテストして、すべてが適切に動作することを確認します。AutoSupportのテストメッセージをNetAppに送信すると、autosupport.to/-to パラメータで指定した宛先に、メッセージが届いたことを確認するEメールが返信されます。NetAppから確認のEメールが届かない場合、またはNetAppがメッセージを受信しなかった場合は、ブロックされたネットワークポートまたは使用中の転送プロトコル (HTTPSまたはSMTP) に関連するアクセスポリシーのトラブルシューティングタスクを実行して問題を解決します。

ONTAPの場合

1. ONTAP 8.3以降を実行している場合は、を実行し `system node autosupport check show` で AutoSupportの設定を確認します。
2. `system node autosupport invoke -type` パラメータを `test` に設定してコマンドを実行します。

```
system node autosupport invoke -type test -node nodename -message Test
```

3. NetAppがAutoSupportメッセージを受信していることを確認するには、`-to` パラメータで指定したEメールアドレスを確認します。このアドレスには、NetAppメールハンドラからの自動応答が含まれています。さらに、Active IQにログインして受信を確認します。

```
system node autosupport history -node nodename
```

sent- successful 設定されているすべてのプロトコルの宛先で、最新の発信AutoSupportメッセージのステータスが最終的にに変わります。

4. **オプション** : AutoSupportメッセージが社内のサポート部門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するには `-to-noteto`、に設定したアドレスのEメールを確認します。または `-partner-address system node autosupport modify` コマンドのパラメータ。

テストAutoSupport電子メールメッセージの例

```
+++++  
Dear NetApp Customer,  
  
This email is sent to acknowledge the receipt of the AutoSupport email from:  
  
System ID: ##SYSID  
Hostname: ##HOSTNAME  
The AutoSupport had the following subject line:  
##ASUPSUBJECT
```

Active IQで推奨されるAutoSupport構成

AutoSupportに推奨されるプロトコルはHTTPSです。ストレージコントローラのAutoSupportに別のプロトコルが設定されている場合は、Active IQの[健全性チェック]にベストプラクティスと対処手順が表示されません。

この情報は、Active IQの健全性チェック機能を使用して、単一のシステムレベルまたはクラスターレベル、または集約されたレベル (お客様、サイト、グループ) で表示できます。

AutoSupportの運用停止 / 辞退

以下は、使用しなくなったシステムを辞退して運用を終了する際に必要な手順です。

- AutoSupportの運用を終了するまたは辞退するストレージシステムのシリアル番号を確認します。シリアル番号の数が多い場合は、NetAppサポートサイトでテクニカルでないサポートケースをオープンし、番号の一覧を添付してください。
- NetAppサポートサイトにログインします。
- [My Support]タブを選択します。
- [Systems] > [View Installed Products]の順にクリックします。
- システムのシリアル番号を入力します。

AutoSupportを辞退する

- [Manage Product Location & Details]で、設定を変えずにそのまま[Go]をクリックします。
- [Configuration Details]セクションで、[Update Configuration Details]を選択します。
- AutoSupportを辞退する理由をドロップダウンメニューから選択します。
- [Confirm Data Submit Changes]をクリックします。

運用を停止する

- [Manage Product Location & Details]のドロップダウンメニューで[Decommission this system]を選択し、[Go]をクリックします。
- [Decommission]フォームに必要な情報をすべて入力し、[Submit]をクリックします。

EシリーズでのAutoSupportの設定

EシリーズでのAutoSupportの完全なガイドについては、次のドキュメントを参照してください。
https://kb.netapp.com/onprem/E-Series/Management_Apps/How_to_enable_AutoSupport_on_E-Series_Santricity_System_Manager

StorageGRIDでのAutoSupportの設定

StorageGRIDでAutoSupportを設定する方法については、次のドキュメントを参照してください。
<https://docs.netapp.com/us-en/storagegrid-117/admin/configure-autosupport-grid-manager.html>

また、StorageGRIDのAutoSupportについて説明する素敵なブログ記事もあります。
<https://www.netapp.com/blog/enable-autosupport-to-get-more-insights-analytics-for-storagegrid-system/>

NetAppのコミュニティサイトには、次の手順も掲載されています。
<https://community.netapp.com/t5/Tech-ONTAP-Blogs/Enabling-StorageGRID-AutoSupport-and-integrating-with-Active-IQ/ba-p/171339>

SolidFireおよびHCIでのAutoSupportの設定

設定に関するドキュメントについては、https://docs.netapp.com/us-en/hci/docs/task_mnode_enable_activeIQ.htmlのドキュメントを参照してください。

Data ONTAPでのAutoSupportのトラブルシューティング

ここでは、メッセージが受信されない場合、または特定のコンテンツが欠落している場合にAutoSupportをトラブルシューティングする手順について説明します。

メッセージが届かない場合のAutoSupportのトラブルシューティング

システムからAutoSupportメッセージが送信されていない場合は、AutoSupportがメッセージを生成できないことが原因か、メッセージを配信できないことが原因かを確認します。

1. `system node autosupport history show` コマンドを使用して、メッセージの配信ステータスを確認します。
2. ステータスは次のいずれかです。
 - **initializing** : 収集プロセスが開始しています。この状態が一時的なものであれば問題はありません。ただしこの状態が持続する場合は、問題が発生しています。
 - **collection-failed** : AutoSupportが、スプール ディレクトリ内にAutoSupportコンテンツを作成できません。エラーに関する追加情報を表示するには、`system node autosupport history show -detail` コマンドを入力します。
 - **collection-in-progress** : AutoSupportがAutoSupportコンテンツを収集しています。AutoSupportが収集している情報を表示するには、`system node autosupport manifest show` コマンドを入力します。
 - **queued** : AutoSupportメッセージが配信のためにキューに登録されていますが、まだ配信されていません。
 - **transmitting** : AutoSupportが現在メッセージを配信しています。
 - **sent -成功しました**。AutoSupportがメッセージを正常に配信しました。AutoSupportがメッセージを配信した場所を確認するには、`system node autosupport history show -delivery` コマンドを入力します。
 - **無視します**。AutoSupportでメッセージの宛先が指定されていません。配信の詳細を表示するには、`system node autosupport history show -delivery` コマンドを入力します。
 - **再キューに入れられました**。AutoSupportがメッセージの配信を試行しましたが、失敗しました。その結果、再度配信を試行するためにメッセージが配信キューに戻されました。エラーを表示するには、`system node autosupport history show` コマンドを入力します。
 - **トランスミッション-失敗**。AutoSupportが指定された回数メッセージの配信に失敗し、メッセージ配信の試行を停止しました。エラーを表示するには、`system node autosupport history show` コマンドを入力します。
 - **ondemand-ignore** : AutoSupportメッセージは正常に処理されましたが、AutoSupport On Demandサービスによって無視されました。次のいずれかを実行してください。
 - **initializing**または**collection-failed** : AutoSupportがメッセージを生成できません。テクニカル サポートに問い合わせてください。
 - **ignore**、**re-queued**、**transmission failed** : AutoSupportがメッセージを配信できません。SMTP、HTTP、HTTPSの配信先が正しく設定されているかどうかを確認してください。

HTTPS経由のAutoSupportのトラブルシューティング

HTTPSを使用していて、想定されるAutoSupportメッセージが送信されない場合は、いくつかの設定を確認して問題を解決できます。

ONTAPの場合

1. 基本的なネットワーク接続とDNSルックアップを確認します。Data ONTAP 8.3以降を実行している場合は、を実行し `system node autosupport check show` でAutoSupportの設定と接続を確認します。
2. ノード管理LIFのステータスを確認します。

```
network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role
```

`status-oper` `status-admin` フィールドとフィールドに返される必要があります `up`。

3. あとで使用できるように、ノード名、LIF名、LIFのIPアドレスを書き留めておきます。
4. DNSが有効になっており、正しく設定されていることを確認します。

```
vserver services name-service dns show
```

5. AutoSupportメッセージで返されたエラーに対処します。

```
system node autosupport history show -node * -fields node,seq-num,destination,last-update,status,error
```

デジタル証明書に問題があることを示すエラーの場合は、テクニカルサポートにお問い合わせください。

6. クラスタがNetAppのAutoSupportサーバに正常にアクセスできることを確認します。

```
network traceroute -node local -destination default_router
network traceroute -node local -destination support.netapp.com
system node autosupport show -fields proxy-url
network traceroute -node local -destination proxy_url
```

アクセスできないデスティネーションがある場合は、「`traceroute`」ユーティリティまたは「`tracert`」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください（この2つのユーティリティは、ほとんどのサードパーティ製ネットワーククライアントに搭載されています）。この方法により、ネットワーク設定とクラスタ構成のどちらに問題があるかを判断できます。

7. AutoSupportの転送プロトコルにHTTPSを使用している場合は、HTTPSトラフィックを社内ネットワーク外に送信可能であることを確認します。
 - a. クラスタ管理LIFと同じサブネットにWebクライアントを設定します。プロキシサーバ、ユーザ名、パスワード、ポートを含む、すべての設定パラメータの値がAutoSupportの設定と同じであることを確認します。
 - b. Webクライアントを使用して `https://support.netapp.com` にアクセスします。

アクセスに成功する必要があります。成功しない場合は、HTTPSトラフィックとDNSトラフィックを許可するようにすべてのファイアウォールが正しく設定されていること、プロキシサーバが正しく設定されていることを確認します。

SMTPを使用しているAutoSupportのトラブルシューティング

AutoSupportメッセージが送信されず、SMTPを使用している場合は、いくつかの設定を確認して問題を解決できます。

ONTAPの場合

1. 基本的なネットワーク接続とDNSルックアップを確認します。Data ONTAP 8.3以降を実行している場合は、を実行し `system node autosupport check show` でAutoSupportの設定と接続を確認します。
2. ノード管理LIFのステータスを確認します。

```
network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role
```

`status-oper` フィールドと `status-admin` フィールドの値が `up` になっていることを確認します。

3. あとで使用できるように、ノード名、LIF名、LIFのIPアドレスを書き留めておきます。

4. メールホストの送信先にホスト名を使用している場合は、DNSが有効になっていて正しく設定されていることを確認します。

```
vserver services name-service dns show
```

5. AutoSupportで使用するよう設定されているすべてのメールホストを表示します。

```
system node autosupport show -fields mail-hosts
```

表示されたメールホストをすべて書き留めます。

6. 前の手順で表示されたメールホストごとに、ノードからホストにアクセスできることを確認します。

```
network traceroute -node local -destination mailhost
```

アクセスできないデスティネーションがある場合は、「traceroute」ユーティリティまたは「tracert」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください（この2つのユーティリティは、ほとんどのサードパーティ製ネットワーククライアントに搭載されています）。この方法により、ネットワーク設定とクラスタ構成のどちらに問題があるかを判断できます。

7. メールホストとして指定したホストにログインし、このホストがSMTP要求を処理できることを確認します。

```
netstat -aAn|grep 25
```

25は、リスナーSMTPのポート番号です。次のようなメッセージが表示されます。

```
ff64878c tcp          0          0 *.25      *.*       LISTEN.
```

8. 他のホストで、メールホストのSMTPポートを使用したTelnetセッションを開きます。

```
telnet mailhost 25
```

次のようなメッセージが表示されます。

```
220 smtp.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2015 10:49:04 PST
```

9. Telnetのプロンプトで、メールホストからメッセージをリレーできることを確認します。

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

domain_name は、ネットワークのドメイン名です。

リレーが拒否されたというエラーが返された場合は、メールホストでリレーが有効になっていません。システム管理者にお問い合わせください。

10. Telnetのプロンプトで、テストメッセージを送信します。

```
SUBJECT: TESTING
```

```
THIS IS A TEST
```

```
.
```

注：

- 必ず最後の行にピリオド(.)を単独で入力してください。このピリオドで、メッセージの完了をメールホストに示します。
- エラーが返された場合は、メールホストが正しく設定されていません。システム管理者にお問い合わせください。

11. Data ONTAP CLIから、アクセス可能な信頼できる電子メールアドレスにAutoSupportテストメッセージを送信します。

```
system node autosupport invoke -node local -type test
```

12. 送信したテストメッセージのシーケンス番号を確認します。

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

タイムスタンプを基に探してください。おそらく、最後に送信されたメッセージです。

13. テストメッセージのエラーを表示します。

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

Login deniedというエラーが表示された場合は、SMTPサーバが、ノード/クラスタ管理LIF、または「from」に指定されたEメール アドレスからの送信要求を受け入れていません。転送プロトコルをHTTPSに変更できない場合は、SMTPゲートウェイの設定をサイトのネットワーク管理者に依頼し、この問題に対処してください。

このテストに成功しても、mailto : autosupport@netapp.comに同じメッセージが送信されない場合は、すべてのSMTPメールホストでautosupport@netapp.comデスティネーションに対してSMTPリレーが有効になっていることを確認するか、転送プロトコルとしてHTTPSを使用してください。

ローカルで管理されている電子メールアカウントへのメッセージが失敗した場合は、次の両方の特性を持つ添付ファイルを転送するようにSMTPサーバが設定されていることを確認します。

- サフィックスが「7z」
- MIMEタイプが「application/x-7x-compressed」

AutoSupportのコンテンツの切り捨て（AutoSupport予算）

Data ONTAPストレージオペレーティングシステムの機能が拡張するにつれて、AutoSupportメッセージで収集および配信されるコンテンツの量も増加しています。一部のメールサーバは添付ファイルのサイズが大きすぎる（5MB以上）Eメールメッセージを削除し、また一部のWebサーバではアップロードできるファイルのサイズに制限があります。

ONTAPには、AutoSupportの収集と提供の予算があり、データ提供ワークフローへの影響を最小限に抑え、必要な帯域幅を最小限に抑えながら、AutoSupportデータを迅速に生成できます。

AutoSupportコレクションフレームワークでは、すべてのコンテンツがサブシステムによって所有されません。AutoSupportは、コンテンツの収集についてサブシステムに時間とサイズの制限を適用することで、すべてのサブシステムに情報収集の機会を公平に付与します。あるサブシステムが割り当てられた時間やサイズを超えてデータを収集しようとするすると、AutoSupportはそのサブシステムでの収集を停止し、次のサブシステムでの収集へと進みます。

AutoSupportの配信割当量は、AutoSupportの圧縮されたペイロードアーカイブの最大サイズを制限します。配信サイズには、SMTP用とHTTPS用の2つの制限があります。AutoSupportアーカイブのサイズが上限を超えると、一部のコンテンツは切り捨てられます。配信の際は、アーカイブの上限に達するまで、マニフェストに指定された優先順でコンテンツが追加されます。

割当制限が原因で特定のコンテンツが失われているかどうかは、次の手順で確認できます。

1. manifest.xml AutoSupportメッセージに含まれているファイルを確認します。問題のコンテンツには次のいずれかのステータスが表示されます。

```
collection-truncated-size-limit  
collection-skipped-size-limit  
collection-truncated-time-limit  
collection-skipped-time-limit  
delivery-skipped-size-limit
```

または、次のいずれかのコマンドを実行して出力を確認します。

```
system node autosupport manifest show  
system node autosupport manifest show -seq-num SequenceNumber
```

（後者のコマンドでは、特定のメッセージのエントリだけが表示されます）。

問題のコンテンツには上記のいずれかのステータスが表示されるはずですが。

2. 収集サイズの制限は、個々のファイルではなく、ノードのサブシステム全体に適用されます。たとえば、あるサブシステムがマニフェスト内の6つの異なるエントリ（ファイル）の収集を

担当していて、サブシステム全体のサイズ制限のために4つ目のエントリを収集できなかった場合、5つ目と6つ目のエントリも収集されません。

これらのエントリが収集される順序は **prio-num**、マニフェストのフィールドによって指定されます。マニフェスト内での各エントリの収集順序を確認するには、次のコマンドを実行します。

```
system node autosupport manifest show -node local -seq-num SequenceNumber -fields prio-num,body-file,subsys,status,error,size-collected
system node autosupport manifest show -status *-limit -fields subsys,status,error
```

特定のサブシステムのエントリのみを表示するには、フラグを追加し **-subsys**、続けてサブシステム名を追加します (例: **log_files**)。

注: 一部のファイル(ログファイルなど)には、**AutoSupport**収集のための個別のサイズ割当があります。ファイル固有の制限のためにファイル収集が切り捨てられた場合、マニフェストステータスにはなります **collection-truncated-file-size-limit**。この切り捨ては想定される動作なので、無視してかまいません。これらのファイルの割当量は変更できません。

特定の**AutoSupport**メッセージについてサブシステムの収集サイズの上限に実際に達している場合、エラーになっている最初のマニフェストエントリにはという **collection-truncated-size-limit** ステータスが表示され、サブシステム内の後続のすべてのエントリにはというステータス **collection-skipped-size-limit** が表示されることがあります。

次の出力例を考えてみましょう。

```
Cluster1::system node autosupport*> manifest show -node local -seq-num 14 -fields prio-num,body-file,subsys,status,error,size-collected -subsys mhost
node      seq-num prio-num subsys body-file      size-collected
status                                         error
-----
node-01 14      39      mhost  rdb_dump.txt 1KB collection-truncated-size-limit ""
node-01 14      40      mhost  cluster_ha.xml
                                         730B collection-truncated-size-limit ""
node-01 14      41      mhost  cluster_ring.xml
                                         - collection-skipped-size-limit ""
node-01 14      42      mhost  dns.xml      - collection-skipped-size-limit ""
node-01 14      43      mhost  hosts.xml    - collection-skipped-size-limit ""
node-01 14      44      mhost  jm_sched.xml - collection-skipped-size-limit ""
node-01 14      45      mhost  jm_history_table_errors.xml
                                         - collection-skipped-size-limit ""
node-01 14      46      mhost  contact_info_view.xml
                                         - collection-skipped-size-limit ""
node-01 14      47      mhost  clusterPeer_itable.xml
                                         - collection-skipped-size-limit ""
node-01 14      48      mhost  foreign_cluster_addrs.xml
                                         - collection-skipped-size-limit ""
node-01 14      49      mhost  foreign_cluster_authority.xml
                                         - collection-skipped-size-limit ""
node-01 14      50      mhost  health_monitor_cache.xml
                                         - collection-skipped-size-limit ""
node-01 14      51      mhost  smdb_smf_metrics.xml
                                         - collection-skipped-size-limit ""
node-01 14      52      mhost  node_root_mounts.xml
                                         - collection-skipped-size-limit ""
```

上記の例では、**mhost**サブシステムの2番目の項目を収集しようとする **cluster_ha.xml**、障害に関連しています。(この例では、サブシステムのサイズ制限が**1KB**というきわめて低い値に設定されています)。

サブシステムのサイズ制限を超えた場合も、すべてのファイルが切り捨てられるわけではありません。サブシステムの制限を超えるバイナリファイルは切り捨てられず、AutoSupportメッセージから完全に除外されます。問題なく切り捨てることができるのはASCII（テキスト）ファイルのみです。

AutoSupportデータが切り捨てられている場合は、次の手順を実行してAutoSupport設定を変更し、切り捨てるを軽減します。

1. HTTPSが使用中のAutoSupport転送であることを確認します。SMTP（Eメール）を使用するようにAutoSupportが設定されている場合は、`-transport` パラメータ（サポートに連絡するプロトコル）をSMTPではなくHTTPSを使用するように変更します。HTTPS転送プロトコルを使用すると、格段に大容量のAutoSupportメッセージを送信できるだけでなく、暗号化されたセキュアな方法でNetAppと通信できます。各ノードのノード管理LIFからのアウトバウンド通信が、ホスト `support.netapp.com` のTCPポート443に接続できることを確認します。HTTPプロキシを使用している環境の場合は、プロキシに到達できることを確認してください。

注：

- AutoSupportの切り捨てを解決するには、AutoSupport転送でHTTPSを有効にする必要があります。SMTPを使用する必要がある場合は、切り捨てが増加する可能性があるため、以降の手順は実行しないでください。
- AutoSupport転送プロトコルを変更しても、`-to`、`-noteto`、`-partner-address`のEメール宛先へのSMTPベースのAutoSupportメッセージの送信には影響しません。

```
::> system node autosupport modify -node * -transport https
```

2. ONTAP 8.3.2P3以降にアップグレードする

または

次のコマンドを実行して、AutoSupport設定を手動で変更します。

```
::> set -privilege diagnostic
::*> system node autosupport modify -node * -max-http-size 50MB
::*> system node autosupport budget modify -node * -subsystem performance_asup -size-limit 350MB -time-limit 10m
::*> system node autosupport budget modify -node * -subsystem performance -size-limit 150MB -time-limit 10m
::*> system node autosupport budget modify -node * -subsystem mhost -size-limit 17MB -time-limit 4m
::*> system node autosupport budget modify -node * -subsystem storage -size-limit 26MB -time-limit 6m
::*> system node autosupport budget modify -node * -subsystem asup_ems -size-limit 4MB -time-limit 2m
::*> system node autosupport budget modify -node * -subsystem kernel -size-limit 6MB -time-limit 2m
::*> system node autosupport budget modify -node * -subsystem waf1 -size-limit 30MB -time-limit 10m
```

3. 必要な宛先（Eメール、syslog、SNMP）にEMSイベント通知が届くよう設定することを推奨します。Data ONTAPからのEMSイベント通知は、クラスタで発生したイベントのアラートを受け取る方法として推奨されています。クラスタからのEMSイベント通知の設定については、『EMS Configuration Express Guide』を参照してください。

証明書の検証が有効な場合にHTTPS経由で送信されたAutoSupportメッセージがNetAppに届かない

AutoSupportメッセージは、転送プロトコルとしてSMTPを使用してNetAppに正常に配信されますが、証明書の検証が有効な状態でHTTPSを使用すると失敗します。

この問題には2種類あることがわかっています。AutoSupportサブシステムによってログに記録されたエラーを表示することで、シグネチャを特定できます。/mroot/etc/log/mlog/notifyd.log:

- 最初のシグネチャは、error setting certificate verify locations次のように強調表示されたエラーメッセージです。

```
00000008.0004cbb8 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message: Connected
to support.netapp.com(216.240.21.18) port 443)
00000008.0004cbb9 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message: error setting
certificate verify locations:
00000008.0004cbb8 069e8daa Thu Mar 28 2013 10:33:04 -04:00
[kern_notifyd:info:711] CAfile: /mroot/etc/keymgr/root/cacert.pem
00000008.0004cbbb 069e8daa Thu Mar 28 2013 10:33:04 -04:00
[kern_notifyd:info:711] CApath: none)
00000008.0004cbbc 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message: Closing
connection #0)
00000008.0004cbbd 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message:
deliver_http_asup: HTTP PUT response error, status code 60.)
```

または

2番目のシグネチャは、SSL certificate problem: self signed certificate in certificate chain次のように強調表示された「」エラーメッセージです。

```
00000017.00975b3d 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: Connected
tosupport.netapp.com (216.240.21.18) port 443 (#0))
00000017.00975b3e 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: successfully
set certificate verify locations:)
00000017.00975b3f 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: CAfile:
/mroot/etc/keymgr/root/cacert.pem
00000017.00975b40 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00
[kern_notifyd:info:43017] CApath: none)
00000017.00975b41 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
handshake, Client hello (1):)
00000017.00975b42 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
handshake, Server hello (2):)
00000017.00975b43 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
handshake, CERT (11):)
00000017.00975b44 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
alert, Server hello (2):)
00000017.00975b45 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSL certificate
problem: self signed certificate in certificate chain)
00000017.00975b46 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: Closing
connection #0)
```

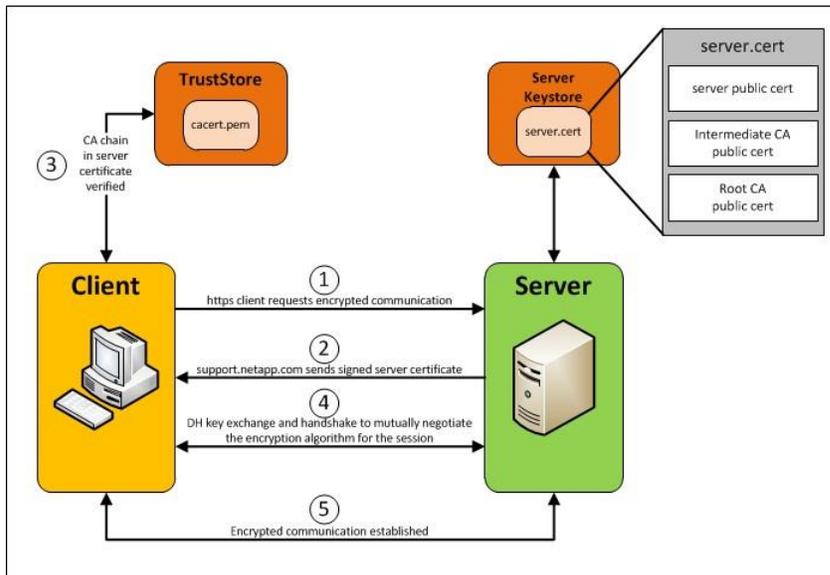
```

00000017.00975b47 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message:
deliver_http_asup: HTTP PUT response error, status code 60.)
00000017.00975b48 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: asup_job HTTP
attempt failed '/mroot/etc/log/autosupport/201603011107.0')
00000017.00975b49 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: Failed to
deliver http with subject: HA Group Notification from ho-0001-cn-as50t-01
(USER_TRIGGERED (ALL:debuglevel)) INFO)

```

Data ONTAPコントローラは、HTTPSプロトコル経由でAutoSupportメッセージを送信する場合、HTTPSクライアントとして機能します。次の図に、HTTPSクライアントがサーバと暗号化された通信を確立するときの基本的な手順を示します。

図3) HTTPS暗号化通信図



主要なコンポーネントは次のとおりです。

- クライアントは、通信を開始し、暗号化された通信チャンネルを必要とするシステムです。ここでは、ONTAPのAutoSupportサブシステムがクライアントにあたります。
- サーバーは、暗号化された通信チャンネルを介して通信できるサービスを提供するシステムです。<https://support.netapp.com/put/AsupPut>および<https://support.netapp.com/asupprod/post/1.0/postASUP>のAutoSupportサービス
- サーバのキーストア：サーバ上にあり、CA署名済みのサーバパブリック証明書ファイルと秘密鍵ファイルのコピーが格納されています。サーバパブリック証明書のみが提供されます。
- サーバパブリック証明書には、サーバの公開鍵、サーバ証明書に署名した認証局（CA）の公開鍵チェーンが含まれています。
- 信頼ストアはクライアント上にあり、クライアントが信頼するすべてのCAの公開鍵のリストが格納されています。cacert.pemファイルは、Data ONTAPがAutoSupport HTTPSクライアントによって信頼され、証明書の検証時に使用されるすべてのCAの公開鍵を格納する場所です。

次に、暗号化されたチャネルの確立方法を記載します。

1. HTTPSクライアントがサーバ (<https://support.netapp.com/put/AsupPut>) に接続し、暗号化された通信チャネルを要求します。
2. サーバが、CA署名済みのサーバ証明書で応答します。この署名済み証明書には、サーバの公開鍵、証明書に署名したCAの公開鍵チェーンが含まれています。
3. クライアントは受け取ったサーバ証明書のCAチェーンを確認し、次に、クライアントの信頼ストアを確認してCAが信頼できることを検証します。Data ONTAPでは、設定によってこの手順をスキップすることができます。
 - a) CAが信頼されている場合、証明書交換は手順4に進みます。
 - b) CAが信頼されていない場合、クライアントは証明書を拒否して接続を終了します。
4. Diffie-Hellman (DH; Diffie-Hellman) キー交換と暗号化ハンドシェイクが行われ、セッションに使用される暗号化アルゴリズムが相互に決定されます。
5. 暗号化ハンドシェイクが完了したら、クライアントとサーバの間で暗号化通信が開始されます。

error setting certificate verify locationsエラーメッセージが表示された場合、cacert.pemファイルが作成中に破損する可能性があるため、Data ONTAPはこのファイルを使用して受信した証明書を検証できません。

というSSL certificate problem: self signed certificate in certificate chainエラーメッセージが表示された場合、ストレージコントローラが受け取っている証明書には、HTTPSクライアントで検証できないCAチェーンが含まれています。この問題は、ファイアウォールや透過型プロキシなどのネットワークデバイスがsupport.netapp.comとストレージコントローラ間の通信パスの途中にある場合に発生する可能性があります。また、証明書交換ハンドシェイクを処理し、support.netapp.comが直接提供するものとは異なるCA証明書チェーンをsupport.netapp.comサーバ証明書に指定するHTTPSパケットを代行受信します。ファイアウォールまたは透過型プロキシによって挿入されたCA証明書チェーンは、support.netapp.comから提供されているように見えますが、チェーン内のCA公開鍵はData ONTAP cacert.pem信頼ストアにはありません。その結果、Data ONTAPは受け取ったサーバ証明書を拒否し、AutoSupportは配信に失敗します。

この問題を解決するには、サポート パートナーまたはNetAppテクニカル サポートにお問い合わせください。解決するためには、Data ONTAPシステムのファイルとサービスの変更が必要です。

追加情報

AutoSupportの詳細については、以下を参照してください。

NetApp Support SiteのAutoSupportドキュメント

https://docs.netapp.com/us-en/active-ig/concept_autosupport.html

TR-4688 : 『Security and privacy of NetApp telemetry data』

<https://www.netapp.com/media/10439-tr4688.pdf>

バージョン履歴

バージョン	日付	ドキュメントバージョン履歴
バージョン1.0	2015年8月	初版リリース

バージョン	日付	ドキュメントバージョン履歴
バージョン1.1	2016年2月	「AutoSupport On Demand」の内容を若干変更
バージョン1.2	2017年9月	My ASUPの名称をActive IQに変更。その他、内容を若干変更
バージョン1.3	2023年8月	用語を更新、古いコンテンツを更新、7-Modeの手順を削除、リンクを更新、Eシリーズを追加「StorageGRID」、「SolidFire」、「HCI」を追加し、ONTAP固有のセクションを明確にしました。

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで [Interoperability Matrix Tool \(IMT\)](#) を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

Copyright © 2024 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。

NetApp 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、NetApp によって「現状のまま」提供されています。NetApp 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。NetApp 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。

NetApp は、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。NetApp 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、NetApp は責任を負いません。この製品の使用または購入は、NetApp 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り保護されている場合があります。

本書に含まれるデータは市販の製品および/またはサービス（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。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、<https://www.netapp.com/company/legal/trademarks/> 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。