Planen

ONTAP 9

NetApp
February 03, 2026

Inhalt

Planen

Bereiten Sie die Verwendung von ONTAP AutoSupport vor

Sie können ein ONTAP-Cluster konfigurieren, um AutoSupport-Meldungen an NetApp zu übermitteln. In diesem Zusammenhang können Sie auch eine Kopie der Nachrichten an lokale E-Mail-Adressen senden, normalerweise innerhalb Ihres Unternehmens. Sie sollten die Konfiguration von AutoSupport vorbereiten, indem Sie die verfügbaren Optionen überprüfen.

AutoSupport-Nachrichten an NetApp senden

AutoSupport-Meldungen können entweder über HTTPS- oder SMTP-Protokolle an NetApp gesendet werden. Ab ONTAP 9.15.1 können Sie TLS auch mit SMTP verwenden.

Verwenden Sie nach Möglichkeit HTTPS zur Kommunikation mit AutoSupport OnDemand und zum Hochladen großer Dateien.

Beachten Sie auch Folgendes:

- Für die AutoSupport-Meldungen kann nur ein Ausgabekanal an NetApp konfiguriert werden. Sie können nicht zwei Protokolle verwenden, um AutoSupport Meldungen an NetApp zu übermitteln.
- AutoSupport begrenzt die maximale Dateigröße für jedes Protokoll. Wenn die Größe einer AutoSupport Meldung das konfigurierte Limit überschreitet, liefert AutoSupport so viele Meldungen wie möglich, doch wird ein Trunking durchgeführt.
- Sie können die maximale Dateigröße bei Bedarf ändern. Erfahren Sie mehr über `system node autosupport modify` in der "ONTAP-Befehlsreferenz".
- Beide Protokolle können basierend auf der Adressenfamilie, in die der Name aufgelöst wird, über IPv4 oder IPv6 übertragen werden.
- Die TCP-Verbindung, die von ONTAP zum Senden von AutoSupport-Nachrichten eingerichtet wurde, ist vorübergehend und nur von kurzer Dauer.

HTTPS

Dies bietet die robustesten Funktionen. Beachten Sie Folgendes:

- AutoSupport OnDemand und die Übertragung großer Dateien werden unterstützt.
- Es wird zuerst versucht, eine HTTPS-PUT-Anforderung zu stellen. Wenn die Anforderung während der Übertragung fehlschlägt, wird die Anforderung an der Stelle neu gestartet, an der sie angehalten wurde.
- Wenn der Server PUT nicht unterstützt, wird stattdessen die HTTPS-POST-Methode verwendet.
- Die Standardeinstellung für HTTPS-Übertragungen ist 50 MB.
- Das HTTPS-Protokoll verwendet Port 443.

SMTP

Als allgemeine Regel sollten Sie SMTP nur verwenden, wenn HTTPS nicht zulässig ist oder nicht unterstützt wird. Beachten Sie Folgendes:

- AutoSupport OnDemand und Übertragungen großer Dateien werden nicht unterstützt.
- Wenn SMTP-Anmeldeinformationen konfiguriert sind, werden sie unverschlüsselt und im Klaren gesendet.
- Die Standardgrenze für Übertragungen beträgt 5 MB.
- Das ungesicherte SMTP-Protokoll verwendet Port 25.

Verbessern Sie die SMTP-Sicherheit mit TLS

Bei Verwendung von SMTP ist der gesamte Datenverkehr unverschlüsselt und kann leicht abgefangen und gelesen werden. Ab ONTAP 9.15.1 können Sie TLS auch mit SMTP (SMTPS) verwenden. In diesem Fall wird *Explicit TLS* verwendet, der den sicheren Kanal aktiviert, nachdem die TCP-Verbindung hergestellt wurde.

Der folgende Port wird normalerweise für SMTPS verwendet: Port 587

Weitere Überlegungen zur Konfiguration

Bei der Konfiguration von AutoSupport müssen zusätzlich einige Überlegungen angestellt werden.

Weitere Informationen zu den Befehlen, die für diese Überlegungen relevant sind, finden Sie unter "AutoSupport einrichten".

Senden Sie eine lokale Kopie per E-Mail

Unabhängig vom Protokoll, das zum Senden von AutoSupport-Nachrichten an NetApp verwendet wird, können Sie auch eine Kopie jeder Nachricht an eine oder mehrere lokale E-Mail-Adressen senden. Beispielsweise können Sie Meldungen an Ihre interne Support-Organisation oder an eine Partnerorganisation senden.

Wenn Sie Nachrichten über SMTP (oder SMTPS) an NetApp senden und gleichzeitig lokale E-Mail-Kopien dieser Nachrichten senden, wird dieselbe E-Mail-Server-Konfiguration verwendet.

HTTP-Proxy

Je nach Netzwerkkonfiguration erfordert das HTTPS-Protokoll möglicherweise eine zusätzliche Konfiguration einer Proxy-URL. Wenn HTTPS zum Senden von AutoSupport-Nachrichten an den technischen Support verwendet wird und Sie über einen Proxy verfügen, müssen Sie die URL für den Proxy angeben. Wenn der Proxy einen anderen Port als den Standardport (Port 3128) verwendet, können Sie den Port für diesen Proxy angeben. Optional können Sie auch einen Benutzernamen und ein Passwort für die Proxy-Authentifizierung angeben.

Installieren Sie das Serverzertifikat

Mit TLS (HTTPS oder SMTPS) wird das vom Server heruntergeladene Zertifikat anhand des Stammzertifizierungszertifikats von ONTAP validiert. Bevor Sie HTTPS oder SMTPS verwenden, müssen Sie sicherstellen, dass das Stammzertifikat in ONTAP installiert ist und dass ONTAP das Serverzertifikat validieren kann. Diese Validierung erfolgt auf der Grundlage der Zertifizierungsstelle, die das Serverzertifikat signiert hat.

ONTAP enthält eine große Anzahl vorinstallierter Stammzertifizierungsstellen-Zertifikate. In vielen Fällen wird das Zertifikat für Ihren Server ohne zusätzliche Konfiguration sofort von ONTAP erkannt. Je nachdem, wie das Serverzertifikat signiert wurde, müssen Sie möglicherweise ein Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate installieren.

Gehen Sie wie folgt vor, um das Zertifikat bei Bedarf zu installieren. Installieren Sie alle erforderlichen Zertifikate auf Cluster-Ebene.

Beispiel 1. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Wählen Sie → neben **Certificates** aus.
4. Klicken Sie auf der Registerkarte **Vertrauenswürdige Zertifizierungsstellen** auf **Hinzufügen**.
5. Klicken Sie auf **Import** und wählen Sie die Zertifikatdatei aus.
6. Vervollständigen Sie die Konfigurationsparameter für Ihre Umgebung.
7. Klicken Sie Auf **Hinzufügen**.

CLI

1. Starten Sie die Installation:

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

   Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

2. Suchen Sie nach der folgenden Konsolenmeldung:

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

3. Öffnen Sie die Zertifikatdatei mit einem Texteditor.
4. Kopieren Sie das gesamte Zertifikat einschließlich der folgenden Zeilen:

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

5. Fügen Sie das Zertifikat nach der Eingabeaufforderung in das Terminal ein.
6. Drücken Sie **Enter**, um die Installation abzuschließen.
7. Überprüfen Sie, ob das Zertifikat installiert ist, indem Sie einen der folgenden Befehle ausführen:

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

   ```
   security certificate show
   ```

   Erfahren Sie mehr über `security certificate show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "AutoSupport einrichten"
- "ONTAP-Befehlsreferenz"

Richten Sie ONTAP AutoSupport ein

Sie können einen ONTAP Cluster so konfigurieren, dass AutoSupport-Nachrichten an den technischen Support von NetApp gesendet werden, und E-Mail-Kopien an den internen Support senden. Im Rahmen dieser Funktion können Sie die Konfiguration auch testen, bevor Sie sie in einer Produktionsumgebung verwenden.

Über diese Aufgabe

Ab ONTAP 9.5 können Sie AutoSupport für alle Nodes eines Clusters gleichzeitig aktivieren und konfigurieren. Wenn ein neuer Node dem Cluster Beitritt, übernimmt der Node automatisch die gleiche AutoSupport-Konfiguration. Zur Unterstützung dieses Befehls `system node autosupport modify` dient der CLI-Befehl als Cluster-Ebene. Die `-node` Befehlsoption wird aus Gründen der Abwärtskompatibilität beibehalten, wird jedoch ignoriert.

> In ONTAP 9.4 und früheren Versionen `system node autosupport modify` ist der Befehl für jeden Knoten spezifisch. Wenn auf dem Cluster ONTAP 9.4 oder eine frühere Version ausgeführt wird, müssen Sie auf jedem Node im Cluster AutoSupport aktivieren und konfigurieren.

Bevor Sie beginnen

Die empfohlene Transportkonfiguration für die Übertragung von AutoSupport Meldungen an NetApp ist HTTPS (HTTP mit TLS). Diese Option bietet die robustesten Funktionen und die beste Sicherheit.

Überprüfen "Bereiten Sie die Verwendung von AutoSupport vor" Sie vor der Konfiguration des ONTAP-Clusters, ob weitere Informationen vorhanden sind.

Schritte

1. Vergewissern Sie sich, dass AutoSupport aktiviert ist:

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

2. Wenn der technische Support von NetApp AutoSupport Meldungen erhalten soll, verwenden Sie den folgenden Befehl:

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

   Sie müssen diese Option aktivieren, wenn Sie AutoSupport aktivieren möchten, um mit AutoSupport OnDemand zu arbeiten, oder wenn Sie große Dateien wie Core Dump- und Performance-Archivdateien auf technischen Support oder eine angegebene URL hochladen möchten.

   > AutoSupport OnDemand ist standardmäßig aktiviert und funktioniert, wenn es so konfiguriert ist, dass über das HTTPS-Transportprotokoll Meldungen an den technischen Support gesendet werden.

3. Wenn Sie den technischen Support von NetApp zum Empfang von AutoSupport Meldungen aktiviert haben, geben Sie das für diese Meldungen zu verwendende Transportprotokoll an.

   Sie können aus folgenden Optionen wählen:

Ihr Ziel ist	Legen Sie dann die folgenden Parameter des `system node autosupport modify` Befehls fest…
Verwenden Sie das HTTPS-Standardprotokoll	a. Setzen Sie `-transport` auf `https`. b. Wenn Sie einen Proxy verwenden, legen Sie `-proxy-url` die URL Ihres Proxys fest. Diese Konfiguration unterstützt die Kommunikation mit AutoSupport OnDemand und das Hochladen großer Dateien.
Verwenden Sie SMTP	Setzen Sie `-transport` auf `smtp`. Diese Konfiguration unterstützt weder AutoSupport OnDemand noch Uploads großer Dateien.

4. Wenn Sie möchten, dass Ihre interne Support-Abteilung oder ein Support-Partner AutoSupport-Meldungen erhalten, führen Sie die folgenden Aktionen durch:
   a. Identifizieren Sie die Empfänger in Ihrem Unternehmen, indem Sie die folgenden Parameter des `system node autosupport modify` Befehls festlegen:

Diesen Parameter festlegen…	Künftige Situation
`-to`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer internen Support-Organisation, die wichtige AutoSupport-Nachrichten empfangen
`-noteto`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer internen Support-Organisation, die eine verkürzte Version von wichtigen AutoSupport-Nachrichten erhalten, die für Mobiltelefone und andere mobile Geräte entwickelt wurden
`-partner-address`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer Support-Partnerorganisation, die alle AutoSupport Meldungen erhalten

   b. Überprüfen Sie, ob Adressen richtig konfiguriert `system node autosupport destinations show` sind, indem Sie die Ziele mit dem Befehl auflisten.
5. Wenn Sie im vorherigen Schritt die Empfängeradressen für Ihre interne Supportorganisation konfiguriert haben oder SMTP-Übertragung für Meldungen an den technischen Support gewählt haben, konfigurieren

Sie SMTP, indem Sie die folgenden Parameter des Befehls festlegen `system node autosupport modify`:

- Legen Sie `-mail-hosts` einen oder mehrere E-Mail-Hosts fest, die durch Kommas getrennt sind.

  Sie können maximal fünf festlegen.

Sie können einen Portwert für jeden Mail-Host konfigurieren, indem Sie einen Doppelpunkt und eine Portnummer nach dem Mail-Hostnamen angeben: Z. B. `mymailhost.example.com:5678` , wobei 5678 der Port für den Mail-Host ist.

- Legen Sie `-from` die E-Mail-Adresse fest, an die die AutoSupport-Nachricht gesendet wird.

6. Konfigurieren Sie DNS.
7. Optional können Sie Befehlsoptionen hinzufügen, wenn Sie bestimmte Einstellungen ändern möchten:

Wenn Sie das wollen…	Legen Sie dann die folgenden Parameter des `system node autosupport modify` Befehls fest…
Verbergen Sie private Daten, indem Sie sensible Daten in den Nachrichten entfernen, maskieren oder kodieren	Setzen Sie `-remove-private-data` auf `true`. Wenn Sie von `false` in wechseln `true`, werden alle AutoSupport-Historie und alle zugehörigen Dateien gelöscht.
Beenden Sie das Senden von Performance-Daten in regelmäßigen AutoSupport Meldungen	Setzen Sie `-perf` auf `false`.

8. Wenn Sie SMTP verwenden, um AutoSupport-Nachrichten an NetApp zu senden, können Sie TLS optional aktivieren, um die Sicherheit zu verbessern.
   a. Zeigt die für den neuen Parameter verfügbaren Werte an:

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

   b. TLS für SMTP-Nachrichtenversand aktivieren:

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

   c. Aktuelle Konfiguration anzeigen:

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

9. Überprüfen Sie die Gesamtkonfiguration mit dem `system node autosupport show` Befehl mit dem `-node` Parameter.
10. Überprüfen Sie die AutoSupport-Operation mit dem `system node autosupport check show` Befehl.

Wenn Probleme gemeldet werden, verwenden Sie den `system node autosupport check show-details` Befehl, um weitere Informationen anzuzeigen.

11. Testen, ob AutoSupport Meldungen gesendet und empfangen werden:
    a. Verwenden Sie den `system node autosupport invoke` Befehl mit dem `-type` Parameter auf `test`:

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

    b. Bestätigen Sie, dass NetApp Ihre AutoSupport Mitteilungen erhält:

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

    Der Status der letzten ausgehenden AutoSupport-Nachricht sollte sich schließlich `sent-successful` für alle geeigneten Protokollziele in ändern.

    c. Bestätigen Sie optional, dass AutoSupport-Nachrichten an Ihre interne Support-Organisation oder an Ihren Support-Partner gesendet werden, indem Sie die E-Mail-Adresse einer Adresse überprüfen, die Sie für die `-to`, `-noteto` oder- `-partner-address`Parameter des `system node autosupport modify` Befehls konfiguriert haben.

Verwandte Informationen

- "Bereiten Sie die Verwendung von AutoSupport vor"
- "ONTAP-Befehlsreferenz"