Pianificare

ONTAP 9

NetApp
February 03, 2026

Sommario

Pianificare

Preparare l’uso di ONTAP AutoSupport

È possibile configurare un cluster ONTAP per inviare messaggi AutoSupport a NetApp. Inoltre, è possibile inviare una copia dei messaggi agli indirizzi e-mail locali, in genere all’interno dell’organizzazione. È necessario prepararsi a configurare AutoSupport esaminando le opzioni disponibili.

Consegna dei messaggi AutoSupport a NetApp

I messaggi AutoSupport possono essere recapitati a NetApp utilizzando i protocolli HTTPS o SMTP. A partire da ONTAP 9.15.1, è anche possibile utilizzare TLS con SMTP.

Utilizzare HTTPS quando possibile per la comunicazione con AutoSupport OnDemand e per il caricamento di file di grandi dimensioni.

Notare anche quanto segue:

- Per i messaggi AutoSupport è possibile configurare un solo canale di recapito per NetApp. Non è possibile utilizzare due protocolli per inviare i messaggi AutoSupport a NetApp.
- AutoSupport limita le dimensioni massime dei file per ciascun protocollo. Se le dimensioni di un messaggio AutoSupport superano il limite configurato, AutoSupport recapita la maggior parte del messaggio possibile, ma si verifica il troncamento.
- Se necessario, è possibile modificare la dimensione massima del file. Ulteriori informazioni su `system node autosupport modify` nella "Riferimento al comando ONTAP".
- Entrambi i protocolli possono essere trasportati su IPv4 o IPv6 in base alla famiglia di indirizzi a cui il nome risolve.
- La connessione TCP stabilita da ONTAP per l’invio di messaggi AutoSupport è temporanea e di breve durata.

HTTPS

Ciò fornisce le funzioni più robuste. Tenere presente quanto segue:

- AutoSupport OnDemand e il trasferimento di file di grandi dimensioni sono supportati.
- Viene tentata prima una richiesta HTTPS PUT. Se la richiesta non riesce durante la trasmissione, la richiesta viene riavviata nel punto in cui è stata arrestata.
- Se il server non supporta PUT, viene utilizzato il metodo HTTPS POST.
- Il limite predefinito per i trasferimenti HTTPS è di 50 MB.
- Il protocollo HTTPS utilizza la porta 443.

SMTP

Come regola generale, è necessario utilizzare SMTP solo se HTTPS non è consentito o non è supportato. Tenere presente quanto segue:

- AutoSupport OnDemand e i trasferimenti di file di grandi dimensioni non sono supportati.
- Se le credenziali di accesso SMTP sono configurate, vengono inviate in modo non crittografato e in chiaro.
- Il limite predefinito per i trasferimenti è di 5 MB.
- Il protocollo SMTP non protetto utilizza la porta 25.

Migliorare la sicurezza SMTP con TLS

Quando si utilizza SMTP, tutto il traffico non è crittografato e può essere facilmente intercettato e letto. A partire da ONTAP 9.15.1 è possibile utilizzare TLS anche con SMTP (SMTPS). In questo caso, viene utilizzato *Explicit TLS* che attiva il canale protetto dopo che è stata stabilita la connessione TCP.

La seguente porta viene generalmente utilizzata per SMTPS: Porta 587

Ulteriori considerazioni sulla configurazione

Durante la configurazione di AutoSupport, è necessario tenere in considerazione alcune considerazioni aggiuntive.

Per ulteriori informazioni sui comandi pertinenti a queste considerazioni, fare riferimento a "Configurare AutoSupport".

Inviare una copia locale tramite e-mail

Indipendentemente dal protocollo utilizzato per inviare i messaggi AutoSupport a NetApp, è anche possibile inviare una copia di ciascun messaggio a uno o più indirizzi e-mail locali. Ad esempio, è possibile inviare messaggi all'organizzazione di assistenza interna o a un'organizzazione partner.

Se si recapitano messaggi a NetApp utilizzando SMTP (o SMTPS) e si inviano copie locali di tali messaggi e-mail, viene utilizzata la stessa configurazione del server di posta elettronica.

Proxy HTTP

A seconda della configurazione di rete, il protocollo HTTPS potrebbe richiedere una configurazione aggiuntiva di un URL proxy. Se HTTPS viene utilizzato per inviare messaggi AutoSupport al supporto tecnico e si dispone di un proxy, è necessario identificare l'URL del proxy. Se il proxy utilizza una porta diversa da quella predefinita (porta 3128), è possibile specificare la porta per tale proxy. Facoltativamente, è anche possibile specificare un nome utente e una password per l'autenticazione proxy.

Installare il certificato del server

Con TLS (HTTPS o SMTPS), il certificato scaricato dal server viene convalidato da ONTAP in base al certificato della CA principale. Prima di utilizzare HTTPS o SMTPS, è necessario assicurarsi che il certificato di origine sia installato in ONTAP e che ONTAP possa convalidare il certificato del server. Questa convalida viene eseguita in base alla CA che ha firmato il certificato del server.

ONTAP include un gran numero di certificati CA principali preinstallati. In molti casi, il certificato per il server verrà immediatamente riconosciuto da ONTAP senza ulteriori configurazioni. A seconda di come è stato firmato il certificato del server, potrebbe essere necessario installare un certificato della CA principale ed eventuali certificati intermedi.

Utilizzare la seguente procedura per installare il certificato, se necessario. È necessario installare tutti i certificati richiesti a livello di cluster.

Esempio 1. Fasi

System Manager

1. In System Manager, selezionare **Cluster** > **Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Selezionare → accanto a **certificati**.
4. Nella scheda **autorità di certificazione attendibili** fare clic su **Aggiungi**.
5. Fare clic su **Importa** e selezionare il file del certificato.
6. Completare i parametri di configurazione dell'ambiente.
7. Fare clic su **Aggiungi**.

CLI

1. Avviare l'installazione:

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

   Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

2. Cercare il seguente messaggio della console:

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

3. Aprire il file del certificato con un editor di testo.
4. Copiare l'intero certificato, incluse le seguenti righe:

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

5. Incollare il certificato nel terminale dopo il prompt dei comandi.
6. Premere **Invio** per completare l'installazione.
7. Verificare che il certificato sia installato eseguendo uno dei seguenti comandi:

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

   ```
   security certificate show
   ```

   Ulteriori informazioni su `security certificate show` nella "Riferimento al comando ONTAP".

Informazioni correlate

- "Configurare AutoSupport"
- "Riferimento al comando ONTAP"

Impostare ONTAP AutoSupport

Puoi configurare un cluster ONTAP per inviare messaggi AutoSupport al supporto tecnico NetApp e inviare copie e-mail alla tua organizzazione di supporto interna. Come parte di questo, è anche possibile testare la configurazione prima di utilizzarla in un ambiente di produzione.

A proposito di questa attività

A partire da ONTAP 9,5, puoi abilitare e configurare contemporaneamente AutoSupport per tutti i nodi di un cluster. Quando un nuovo nodo si unisce al cluster, il nodo eredita automaticamente la stessa configurazione AutoSupport. A supporto di questo, l'ambito del comando CLI `system node autosupport modify` è a livello di cluster. Il `-node` l'opzione comando viene mantenuta per la compatibilità con le versioni precedenti, ma viene ignorata.

> In ONTAP 9,4 e versioni precedenti, il comando `system node autosupport modify` è specifico per ogni nodo. Se nel cluster è in esecuzione ONTAP 9,4 o versione precedente, è necessario abilitare e configurare AutoSupport su ciascun nodo del cluster.

Prima di iniziare

La configurazione di trasporto consigliata per la distribuzione dei messaggi AutoSupport a NetApp è HTTPS (HTTP con TLS). Questa opzione fornisce le funzioni più robuste e la massima protezione.

Revisione "Preparare l'uso di AutoSupport" Per ulteriori informazioni prima di configurare il cluster ONTAP.

Fasi

1. Assicurarsi che AutoSupport sia attivato:

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

2. Se si desidera che il supporto tecnico NetApp riceva messaggi AutoSupport, utilizzare il seguente comando:

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

   È necessario attivare questa opzione se si desidera attivare AutoSupport per lavorare con AutoSupport OnDemand o se si desidera caricare file di grandi dimensioni, come i file di archiviazione delle performance e dei core dump, sul supporto tecnico o su un URL specificato.

   > AutoSupport OnDemand è abilitato per impostazione predefinita e funzionale quando è configurato per inviare messaggi al supporto tecnico utilizzando il protocollo di trasporto HTTPS.

3. Se l'assistenza tecnica NetApp è stata attivata per la ricezione di messaggi AutoSupport, specificare il

protocollo di trasporto da utilizzare per questi messaggi.

È possibile scegliere tra le seguenti opzioni:

Se si desidera…	Quindi, impostare i seguenti parametri di `system node autosupport modify` comando…
Utilizzare il protocollo HTTPS predefinito	a. Impostare `-transport` a. `https`. b. Se si utilizza un proxy, impostare `-proxy-url` All'URL del proxy. Questa configurazione supporta la comunicazione con AutoSupport OnDemand e il caricamento di file di grandi dimensioni.
USA SMTP	Impostare `-transport` a. `smtp`. Questa configurazione non supporta AutoSupport OnDemand o upload di file di grandi dimensioni.

4. Se si desidera che l'organizzazione di supporto interna o un partner di supporto riceva messaggi AutoSupport, eseguire le seguenti operazioni:
   a. Identificare i destinatari dell'organizzazione impostando i seguenti parametri di `system node autosupport modify` comando:

Imposta questo parametro…	A questo…
`-to`	Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione di supporto interna che riceveranno messaggi AutoSupport chiave
`-noteto`	Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione di supporto interna che riceveranno una versione abbreviata dei messaggi AutoSupport chiave progettati per telefoni cellulari e altri dispositivi mobili
`-partner-address`	Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione del partner di supporto che riceveranno tutti i messaggi AutoSupport

   b. Verificare che gli indirizzi siano configurati correttamente elencando le destinazioni utilizzando `system node autosupport destinations show` comando.
5. Se nel passaggio precedente sono stati configurati gli indirizzi dei destinatari per l'organizzazione di supporto interno o è stato scelto il trasporto SMTP per i messaggi al supporto tecnico, configurare SMTP impostando i seguenti parametri del `system node autosupport modify` comando:

- Impostare `-mail-hosts` a uno o più mail host, separati da virgole.

  È possibile impostare un massimo di cinque.

È possibile configurare un valore di porta per ciascun host di posta specificando i due punti e il numero di porta dopo il nome host della posta: Ad esempio, `mymailhost.example.com:5678`, dove 5678 è la porta per l'host di posta.

- Impostare `-from` All'indirizzo e-mail che invia il messaggio AutoSupport.

6. Configurare il DNS.
7. Se si desidera modificare impostazioni specifiche, aggiungere opzioni di comando:

Se si desidera eseguire questa operazione…	Quindi, impostare i seguenti parametri di `system node autosupport modify` comando…
Nascondere i dati privati rimuovendo, mascherando o codificando i dati sensibili nei messaggi	Impostare `-remove-private-data` a. `true`. Se si cambia da `false` a. `true`, Vengono cancellati tutti i file della cronologia AutoSupport e tutti i file associati.
Interrompere l'invio dei dati relativi alle prestazioni nei messaggi AutoSupport periodici	Impostare `-perf` a. `false`.

8. Se si utilizza SMTP per inviare messaggi AutoSupport a NetApp, è possibile attivare TLS per una maggiore protezione.
   a. Visualizzare i valori disponibili per il nuovo parametro:

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

   b. Abilita TLS per la consegna dei messaggi SMTP:

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

   c. Visualizza la configurazione corrente:

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

9. Controllare la configurazione generale utilizzando `system node autosupport show` con il `-node` parametro.
10. Verificare il funzionamento di AutoSupport utilizzando `system node autosupport check show` comando.

    Se vengono segnalati problemi, utilizzare `system node autosupport check show-details` per visualizzare ulteriori informazioni.

11. Verifica dell'invio e della ricezione dei messaggi AutoSupport:

    a. Utilizzare `system node autosupport invoke` con il `-type` parametro impostato su `test`:

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

    b. Conferma che NetApp sta ricevendo i tuoi messaggi AutoSupport:

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

    Lo stato dell'ultimo messaggio AutoSupport in uscita dovrebbe cambiare in `sent-successful` per tutte le destinazioni del protocollo appropriate.

    c. Se si desidera, verificare che i messaggi AutoSupport vengano inviati all'organizzazione di supporto interna o al partner di supporto controllando l'indirizzo e-mail configurato per `-to`, `-noteto`, o. `-partner-address` parametri di `system node autosupport modify` comando.

Informazioni correlate

- "Preparare l'uso di AutoSupport"
- "Riferimento al comando ONTAP"