Gestire i servizi Web

ONTAP 9

NetApp
February 12, 2026

Sommario

Gestire i servizi Web

Panoramica sulla gestione dei servizi Web

È possibile attivare o disattivare un servizio Web per il cluster o una macchina virtuale di storage (SVM), visualizzare le impostazioni per i servizi Web e controllare se gli utenti di un ruolo possono accedere a un servizio Web.

È possibile gestire i servizi Web per il cluster o una SVM nei seguenti modi:

- Attivazione o disattivazione di un servizio Web specifico
- Specifica se l'accesso a un servizio Web è limitato solo a HTTP (SSL) crittografato
- Visualizzazione della disponibilità dei servizi Web
- Consentire o negare agli utenti di un ruolo di accedere a un servizio Web
- Visualizzazione dei ruoli autorizzati ad accedere a un servizio Web

Affinché un utente possa accedere a un servizio Web, devono essere soddisfatte tutte le seguenti condizioni:

- L'utente deve essere autenticato.

  Ad esempio, un servizio Web potrebbe richiedere un nome utente e una password. La risposta dell'utente deve corrispondere a un account valido.

- L'utente deve essere configurato con il metodo di accesso corretto.

  L'autenticazione ha successo solo per gli utenti con il metodo di accesso corretto per il servizio Web specificato. Per il servizio Web API di ONTAP `ontapi`), gli utenti devono disporre di `ontapi` metodo di accesso. Per tutti gli altri servizi Web, gli utenti devono disporre di `http` metodo di accesso.

  > Si utilizza `security login` comandi per gestire i metodi di accesso e di autenticazione degli utenti.

- Il servizio Web deve essere configurato in modo da consentire il ruolo di controllo degli accessi dell'utente.

  > Si utilizza `vserver services web access` comandi per controllare l'accesso di un ruolo a un servizio web.

Se un firewall è attivato, il criterio firewall per l'utilizzo della LIF per i servizi Web deve essere impostato in modo da consentire HTTP o HTTPS.

Se si utilizza HTTPS per l'accesso al servizio Web, è necessario attivare anche SSL per il cluster o SVM che offre il servizio Web e fornire un certificato digitale per il cluster o SVM.

Gestire l'accesso ai servizi web ONTAP

Un servizio Web è un'applicazione a cui gli utenti possono accedere utilizzando HTTP o HTTPS. L'amministratore del cluster può configurare il motore del protocollo Web, configurare SSL, abilitare un servizio Web e consentire agli utenti di un ruolo di accedere

a un servizio Web.

A partire da ONTAP 9.6, sono supportati i seguenti servizi Web:

- Infrastruttura del Service Processor (`spi`)

  Questo servizio rende disponibili i file di log, core dump e MIB di un nodo per l'accesso HTTP o HTTPS attraverso la LIF di gestione del cluster o una LIF di gestione dei nodi. L'impostazione predefinita è `enabled`.

  Su richiesta di accesso ai file di registro o ai file di dump del core di un nodo, `spi` Il servizio web crea automaticamente un punto di montaggio da un nodo al volume radice di un altro nodo, dove risiedono i file. Non è necessario creare manualmente il punto di montaggio.

- API ONTAP (`ontapi`)

  Questo servizio consente di eseguire API ONTAP per eseguire funzioni amministrative con un programma remoto. L'impostazione predefinita è `enabled`.

  Questo servizio potrebbe essere richiesto per alcuni strumenti di gestione esterni. Ad esempio, se si utilizza System Manager, lasciare attivato questo servizio.

- Rilevamento Data ONTAP (`disco`)

  Questo servizio consente alle applicazioni di gestione off-box di rilevare il cluster nella rete. L'impostazione predefinita è `enabled`.

- Diagnostica di supporto (`supdiag`)

  Questo servizio controlla l'accesso a un ambiente privilegiato sul sistema per facilitare l'analisi e la risoluzione dei problemi. L'impostazione predefinita è `disabled`. Attivare questo servizio solo se richiesto dal supporto tecnico.

- System Manager (`sysmgr`)

  Questo servizio controlla la disponibilità di Gestore di sistema, incluso in ONTAP. L'impostazione predefinita è `enabled`. Questo servizio è supportato solo sul cluster.

- Aggiornamento del firmware Baseboard Management Controller (BMC) (`FW_BMC`)

  Questo servizio consente di scaricare i file del firmware BMC. L'impostazione predefinita è `enabled`.

- Documentazione ONTAP (`docs`)

  Questo servizio consente di accedere alla documentazione di ONTAP. L'impostazione predefinita è `enabled`.

- API RESTful di ONTAP (`docs_api`)

  Questo servizio fornisce l'accesso alla documentazione dell'API RESTful di ONTAP. L'impostazione predefinita è `enabled`.

- Caricamento e download del file (`fud`)

Questo servizio offre il caricamento e il download dei file. L'impostazione predefinita è `enabled`.

- Messaggi ONTAP (`ontapmsg`)

  Questo servizio supporta un'interfaccia di pubblicazione e sottoscrizione che consente di iscriversi agli eventi. L'impostazione predefinita è `enabled`.

- Portale ONTAP (`portal`)

  Questo servizio implementa il gateway in un server virtuale. L'impostazione predefinita è `enabled`.

- Interfaccia RESTful di ONTAP (`rest`)

  Questo servizio supporta un'interfaccia RESTful utilizzata per gestire in remoto tutti gli elementi dell'infrastruttura cluster. L'impostazione predefinita è `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

  Questo servizio fornisce risorse per supportare il provider di servizi SAML. L'impostazione predefinita è `enabled`.

- Provider di servizi SAML (`saml-sp`)

  Questo servizio offre servizi come i metadati SP e il servizio di asserzione per i clienti al provider di servizi. L'impostazione predefinita è `enabled`.

A partire da ONTAP 9.7, sono supportati i seguenti servizi aggiuntivi:

- File di backup della configurazione (`backups`)

  Questo servizio consente di scaricare i file di backup della configurazione. L'impostazione predefinita è `enabled`.

- Sicurezza ONTAP (`security`)

  Questo servizio supporta la gestione dei token CSRF per un'autenticazione avanzata. L'impostazione predefinita è `enabled`.

Gestire il motore dei protocolli Web in ONTAP

È possibile configurare il motore dei protocolli Web sul cluster per controllare se l'accesso Web è consentito e quali versioni SSL possono essere utilizzate. È inoltre possibile visualizzare le impostazioni di configurazione del motore dei protocolli Web.

È possibile gestire il motore dei protocolli Web a livello di cluster nei seguenti modi:

- È possibile specificare se i client remoti possono utilizzare HTTP o HTTPS per accedere al contenuto del servizio Web utilizzando `system services web modify` con il `-external` parametro.
- È possibile specificare se utilizzare SSLv3 per un accesso web sicuro utilizzando `security config modify` con il `-supported-protocol` parametro. Per impostazione predefinita, SSLv3 è disattivato.

Transport Layer Security 1.0 (TLSv1.0) è attivato e può essere disattivato se necessario.

Ulteriori informazioni su `security config modify` nella "Riferimento al comando ONTAP".

- È possibile attivare la modalità di conformità FIPS (Federal Information Processing Standard) 140-2 per le interfacce dei servizi Web del piano di controllo a livello di cluster.

  Per impostazione predefinita, la modalità di conformità FIPS 140-2 è disattivata.

  - **Quando la modalità di compliance FIPS 140-2 è disattivata**, è possibile attivare la modalità di compliance FIPS 140-2 impostando `is-fips-enabled` parametro a. `true` per `security config modify` e quindi utilizzando il comando `security config show` per confermare lo stato online.
  - **Quando è attivata la modalità di conformità FIPS 140-2**
    - A partire da ONTAP 9.11.1, TLSv1, TLSv1,1 e SSLv3 sono disattivati e solo TSLv1,2 e TSLv1,3 rimangono abilitati. Riguarda altri sistemi e comunicazioni interni ed esterni a ONTAP 9. Se si attiva la modalità di conformità FIPS 140-2 e successivamente si disattiva, TLSv1, TLSv1.1 e SSLv3 rimangono disattivati. TLSv1.2 o TLSv1.3 resteranno abilitati a seconda della configurazione precedente.
    - Per le versioni di ONTAP precedenti alla 9.11.1, TLSv1 e SSLv3 sono disattivati e solo TLSv1.1 e TLSv1.2 rimangono attivati. ONTAP impedisce di abilitare sia TLSv1 che SSLv3 quando è attivata la modalità di conformità FIPS 140-2. Se si attiva la modalità di conformità FIPS 140-2 e successivamente la si disattiva, TLSv1 e SSLv3 rimangono disattivati, ma TLSv1.2 o TLSv1.1 e TLSv1.2 vengono attivati a seconda della configurazione precedente.
- È possibile visualizzare la configurazione della sicurezza a livello di cluster utilizzando `system security config show` comando.

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

Se il firewall è attivato, il criterio firewall per l'interfaccia logica (LIF) da utilizzare per i servizi Web deve essere impostato in modo da consentire l'accesso HTTP o HTTPS.

Se si utilizza HTTPS per l'accesso al servizio Web, è necessario attivare anche SSL per il cluster o la macchina virtuale di storage (SVM) che offre il servizio Web e fornire un certificato digitale per il cluster o la SVM.

Nelle configurazioni MetroCluster, le modifiche apportate alle impostazioni per il motore del protocollo Web su un cluster non vengono replicate sul cluster partner.

Comandi ONTAP per la gestione del motore del protocollo web

Si utilizza `system services web` comandi per gestire il motore dei protocolli web. Si utilizza `system services firewall policy create` e. `network interface modify` comandi per consentire alle richieste di accesso web di passare attraverso il firewall.

Se si desidera…	Utilizzare questo comando…
Configurare il motore del protocollo Web a livello di cluster: • Attivare o disattivare il motore dei protocolli Web per il cluster • Attivare o disattivare SSLv3 per il cluster • Attivazione o disattivazione della conformità FIPS 140-2 per servizi Web sicuri (HTTPS)	`system services web modify`
Visualizzare la configurazione del motore dei protocolli Web a livello di cluster, determinare se i protocolli Web sono funzionanti in tutto il cluster e visualizzare se la conformità FIPS 140-2 è attivata e online	`system services web show`
Visualizzare la configurazione del motore dei protocolli Web a livello di nodo e l'attività di gestione dei servizi Web per i nodi nel cluster	`system services web node show`
Creare una policy firewall o aggiungere il servizio del protocollo HTTP o HTTPS a una policy firewall esistente per consentire alle richieste di accesso Web di passare attraverso il firewall	`system services firewall policy create` Impostazione di `-service` parametro a. `http` oppure `https` consente alle richieste di accesso web di passare attraverso il firewall.
Associare una policy firewall a una LIF	`network interface modify` È possibile utilizzare `-firewall-policy` Parametro per modificare la policy firewall di una LIF.

Informazioni correlate

- "modifica dell'interfaccia di rete"

Configurare l'accesso ai servizi web ONTAP

La configurazione dell'accesso ai servizi Web consente agli utenti autorizzati di utilizzare HTTP o HTTPS per accedere al contenuto del servizio sul cluster o su una macchina virtuale di storage (SVM).

Fasi

1. Se è attivato un firewall, assicurarsi che l'accesso HTTP o HTTPS sia impostato nel criterio del firewall per la LIF che verrà utilizzata per i servizi Web:

   È possibile verificare se un firewall è attivato utilizzando `system services firewall show` comando.

a. Per verificare che HTTP o HTTPS sia impostato nel criterio firewall, utilizzare `system services firewall policy show` comando.

   Impostare `-service` del parametro `system services firewall policy create` comando a. `http` oppure `https` per consentire al criterio di supportare l'accesso web.

b. Per verificare che il criterio firewall che supporta HTTP o HTTPS sia associato al LIF che fornisce servizi Web, utilizzare `network interface show` con il `-firewall-policy` parametro.

   Ulteriori informazioni su `network interface show` nella "Riferimento al comando ONTAP".

   Si utilizza `network interface modify` con il `-firewall-policy` Parametro per attivare la policy firewall per una LIF.

Ulteriori informazioni su `network interface modify` nella "Riferimento al comando ONTAP".

2. Per configurare il motore del protocollo Web a livello di cluster e rendere accessibile il contenuto del servizio Web, utilizzare `system services web modify` comando.
3. Se si prevede di utilizzare servizi web sicuri (HTTPS), abilitare SSL e fornire informazioni sul certificato digitale per il cluster o SVM utilizzando `security ssl modify` comando.

   Ulteriori informazioni su `security ssl modify` nella "Riferimento al comando ONTAP".

4. Per attivare un servizio Web per il cluster o SVM, utilizzare `vserver services web modify` comando.

   Ripetere questo passaggio per ogni servizio che si desidera attivare per il cluster o SVM.

5. Per autorizzare un ruolo ad accedere ai servizi Web sul cluster o SVM, utilizzare `vserver services web access create` comando.

   Il ruolo a cui si concede l'accesso deve già esistere. È possibile visualizzare i ruoli esistenti utilizzando `security login role show` o creare nuovi ruoli utilizzando `security login role create` comando.

   Ulteriori informazioni su `security login role show` e `security login role create` nella "Riferimento al comando ONTAP".

6. Per un ruolo autorizzato ad accedere a un servizio Web, verificare che anche i relativi utenti siano configurati con il metodo di accesso corretto controllando l'output di `security login show` comando.

   Per accedere al servizio Web API di ONTAP `ontapi`), un utente deve essere configurato con `ontapi` metodo di accesso. Per accedere a tutti gli altri servizi Web, è necessario configurare un utente con `http` metodo di accesso.

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

   > Il `security login create` comando consente di aggiungere un metodo di accesso per un utente. Ulteriori informazioni su `security login create` nella "Riferimento al comando ONTAP".

Comandi ONTAP per la gestione dei servizi web

Si utilizza `vserver services web` Comandi per gestire la disponibilità dei servizi Web per il cluster o una macchina virtuale di storage (SVM). Si utilizza `vserver services web access` comandi per controllare l'accesso di un ruolo a un servizio web.

Se si desidera…	Utilizzare questo comando…
Configurare un servizio Web per il cluster o anSVM: • Attivare o disattivare un servizio Web • Specificare se è possibile utilizzare solo HTTPS per accedere a un servizio Web	`vserver services web modify`
Visualizzare la configurazione e la disponibilità dei servizi Web per il cluster o anSVM	`vserver services web show`
Autorizzare un ruolo ad accedere a un servizio Web sul cluster o su una SVM	`vserver services web access create`
Visualizzare i ruoli autorizzati ad accedere ai servizi Web sul cluster o su una SVM	`vserver services web access show`
Impedire a un ruolo di accedere a un servizio Web sul cluster o su una SVM	`vserver services web access delete`

Informazioni correlate

"Riferimento al comando ONTAP"

Comandi per la gestione dei punti di montaggio sui nodi ONTAP

Il `spi` il servizio web crea automaticamente un punto di montaggio da un nodo al volume root di un altro nodo su richiesta di accesso ai file di log o ai file core del nodo. Sebbene non sia necessario gestire manualmente i punti di montaggio, è possibile farlo utilizzando `system node root-mount` comandi.

Se si desidera…	Utilizzare questo comando…
Creare manualmente un punto di montaggio da un nodo al volume root di un altro nodo	`system node root-mount create` Può esistere un solo punto di montaggio da un nodo all'altro.
Visualizzare i punti di montaggio esistenti sui nodi del cluster, incluso l'ora in cui è stato creato un punto di montaggio e il relativo stato corrente	`system node root-mount show`

Se si desidera…	Utilizzare questo comando…
Eliminare un punto di montaggio da un nodo al volume root di un altro nodo e forzare la chiusura delle connessioni al punto di montaggio	`system node root-mount delete`

Informazioni correlate

"Riferimento al comando ONTAP"

Gestire SSL in ONTAP

Utilizzare `security ssl` Comandi per gestire il protocollo SSL per il cluster o una Storage Virtual Machine (SVM). Il protocollo SSL migliora la sicurezza dell'accesso Web utilizzando un certificato digitale per stabilire una connessione crittografata tra un server Web e un browser.

È possibile gestire SSL per il cluster o una macchina virtuale di storage (SVM) nei seguenti modi:

- Abilitazione di SSL
- Generazione e installazione di un certificato digitale e associazione con il cluster o SVM
- Visualizzazione della configurazione SSL per verificare se SSL è stato attivato e, se disponibile, il nome del certificato SSL
- Impostazione di policy firewall per il cluster o SVM, in modo che le richieste di accesso Web possano essere inoltrate
- Definizione delle versioni SSL utilizzabili
- Limitazione dell'accesso solo alle richieste HTTPS per un servizio Web

Comandi per la gestione di SSL

Si utilizza `security ssl` Comandi per gestire il protocollo SSL per il cluster o una Storage Virtual Machine (SVM).

Se si desidera…	Utilizzare questo comando…
Abilitare SSL per il cluster o una SVM e associare un certificato digitale	`security ssl modify`
Visualizzare la configurazione SSL e il nome del certificato per il cluster o una SVM	`security ssl show`

Ulteriori informazioni su `security ssl modify` e `security ssl show` nella "Riferimento al comando ONTAP".

Utilizzare HSTS per i servizi Web ONTAP

HTTP Strict Transport Security (HSTS) è un meccanismo di policy di sicurezza web che aiuta a proteggere i siti web da attacchi man-in-the-middle, come gli attacchi di

downgrade del protocollo e il dirottamento dei cookie. Imponendo l'uso di HTTPS, HSTS garantisce che tutte le comunicazioni tra il browser dell'utente e il server siano crittografate. A partire da ONTAP 9.17.1, ONTAP può imporre connessioni HTTPS per i servizi web ONTAP .

> HSTS viene applicato dal browser web solo dopo aver stabilito una connessione HTTPS sicura iniziale con ONTAP. Se il browser non stabilisce una connessione sicura iniziale, HSTS non verrà applicato. Consultare la documentazione del browser per informazioni sulla gestione di HSTS.

A proposito di questa attività

- Per la versione 9.17.1 e successive, HSTS è abilitato per impostazione predefinita per i cluster ONTAP appena installati. Quando si esegue l'aggiornamento alla versione 9.17.1, HSTS non è abilitato per impostazione predefinita. È necessario abilitare HSTS dopo l'aggiornamento.
- HSTS è supportato per tutti "Servizi web ONTAP" .

Prima di iniziare

- Per le seguenti attività sono richiesti privilegi avanzati.

Mostra la configurazione HSTS

È possibile visualizzare la configurazione HSTS corrente per verificare se è abilitata e visualizzare l'impostazione dell'età massima.

Fasi

1. Utilizzare il `system services web show` comando per mostrare la configurazione corrente dei servizi web, incluse le impostazioni HSTS:

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                        Per Address Limit: 80
                      Wait Queue Capacity: 192
                             HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                             HSTS Enabled: true
                   HSTS max age (Seconds): 63072000
```

Abilita HSTS e imposta l'età massima

A partire da ONTAP 9.17.1, HSTS è abilitato per impostazione predefinita sui nuovi cluster ONTAP . Se si aggiorna un cluster esistente alla versione 9.17.1 o successiva, è necessario abilitare manualmente HSTS sul cluster per imporre l'utilizzo di HTTPS. È possibile abilitare HSTS e impostare l'età massima. È possibile modificare l'età massima in qualsiasi momento se HSTS è abilitato. Una volta abilitato HSTS, i browser inizieranno a imporre connessioni sicure solo dopo aver stabilito una connessione sicura iniziale.

Fasi

1. Utilizzare il `system services web modify` comando per abilitare HSTS o modificare l'età massima:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` Specifica la durata in secondi per cui il browser ricorderà di attivare HTTPS. Il valore predefinito è 63072000 secondi (due anni).

Disabilitare HSTS

I browser salvano l'impostazione relativa all'età massima di HSTS a ogni connessione e continuano ad applicare HSTS per l'intera durata, anche se HSTS è disabilitato su ONTAP. Dopo la disabilitazione, il browser dovrà attendere il raggiungimento della durata massima configurata per interrompere l'applicazione di HSTS. Se durante questo periodo di tempo diventa impossibile stabilire una connessione sicura, i browser che applicano HSTS non consentiranno l'accesso ai servizi web ONTAP fino alla risoluzione del problema o alla scadenza dell'età massima del browser.

Fasi

1. Disabilitare HSTS utilizzando `system services web modify` comando:

```
system services web modify -hsts-enabled false
```

Informazioni correlate

"RFC 6797 - Sicurezza del trasporto HTTP rigorosa (HSTS)"

Risoluzione dei problemi di accesso al servizio Web ONTAP

Gli errori di configurazione causano problemi di accesso al servizio Web. È possibile risolvere gli errori assicurandosi che LIF, policy firewall, motore del protocollo web, servizi web, certificati digitali, e l'autorizzazione all'accesso dell'utente sono tutte configurate correttamente.

La seguente tabella consente di identificare e risolvere gli errori di configurazione del servizio Web:

Questo problema di accesso…	Si verifica a causa di questo errore di configurazione…	Per risolvere l'errore…
Il browser Web restituisce un `unable to connect` oppure `failure to establish a connection` errore quando si tenta di accedere a un servizio web.	La LIF potrebbe non essere configurata correttamente.	Assicurarsi di poter eseguire il ping della LIF che fornisce il servizio Web. Puoi usare `network ping` il comando per eseguire il ping di una LIF.
Il firewall potrebbe non essere configurato correttamente.	Assicurarsi che un criterio firewall sia impostato per supportare HTTP o HTTPS e che il criterio sia assegnato alla LIF che fornisce il servizio Web. Si utilizza `system services firewall policy` comandi per gestire le policy firewall. Si utilizza `network interface modify` con il `-firewall -policy` Parametro per associare un criterio a un LIF.	Il motore del protocollo Web potrebbe essere disattivato.
Assicurarsi che il motore dei protocolli Web sia abilitato in modo da poter accedere ai servizi Web. Si utilizza `system services web` comandi per gestire il motore del protocollo web per il cluster.	Il browser Web restituisce un `not found` errore quando si tenta di accedere a un servizio web.	Il servizio Web potrebbe essere disattivato.

Questo problema di accesso…	Si verifica a causa di questo errore di configurazione…	Per risolvere l'errore…
Assicurarsi che ogni servizio Web a cui si desidera consentire l'accesso sia attivato singolarmente. Si utilizza `vserver services web modify` per abilitare un servizio web per l'accesso.	Il browser Web non riesce ad accedere a un servizio Web con il nome account e la password dell'utente.	L'utente non può essere autenticato, il metodo di accesso non è corretto o non è autorizzato ad accedere al servizio Web.
Assicurarsi che l'account utente esista e sia configurato con il metodo di accesso e di autenticazione corretti. Inoltre, assicurarsi che il ruolo dell'utente sia autorizzato ad accedere al servizio Web. Si utilizza `security login` comandi per gestire gli account utente, i relativi metodi di accesso e i metodi di autenticazione. L'accesso al servizio Web API di ONTAP richiede `ontapi` metodo di accesso. L'accesso a tutti gli altri servizi Web richiede `http` metodo di accesso. Si utilizza `vserver services web access` comandi per gestire l'accesso di un ruolo a un servizio web.	Si effettua la connessione al servizio Web con HTTPS e il browser Web indica che la connessione è stata interrotta.	È possibile che SSL non sia abilitato sul cluster o sulla SVM (Storage Virtual Machine) che fornisce il servizio Web.

Questo problema di accesso…	Si verifica a causa di questo errore di configurazione…	Per risolvere l'errore…
Assicurarsi che il cluster o la SVM abbia abilitato SSL e che il certificato digitale sia valido. Si utilizza `security ssl` Comandi per gestire la configurazione SSL per i server HTTP e il `security certificate show` per visualizzare le informazioni del certificato digitale.	La connessione al servizio Web viene stabilita con HTTPS e il browser Web indica che la connessione non è attendibile.	È possibile che si stia utilizzando un certificato digitale autofirmato.

Informazioni correlate

- "Quali sono le migliori pratiche per la configurazione di rete per ONTAP?"
- "ping di rete"
- "modifica dell'interfaccia di rete"
- "certificato di sicurezza generate-csr"
- "installazione del certificato di sicurezza"
- "mostra certificato di sicurezza"
- "sicurezza ssl"