Configurazione di un tunnel SSH di supporto tecnico su richiesta per le appliance virtuali Umbrella

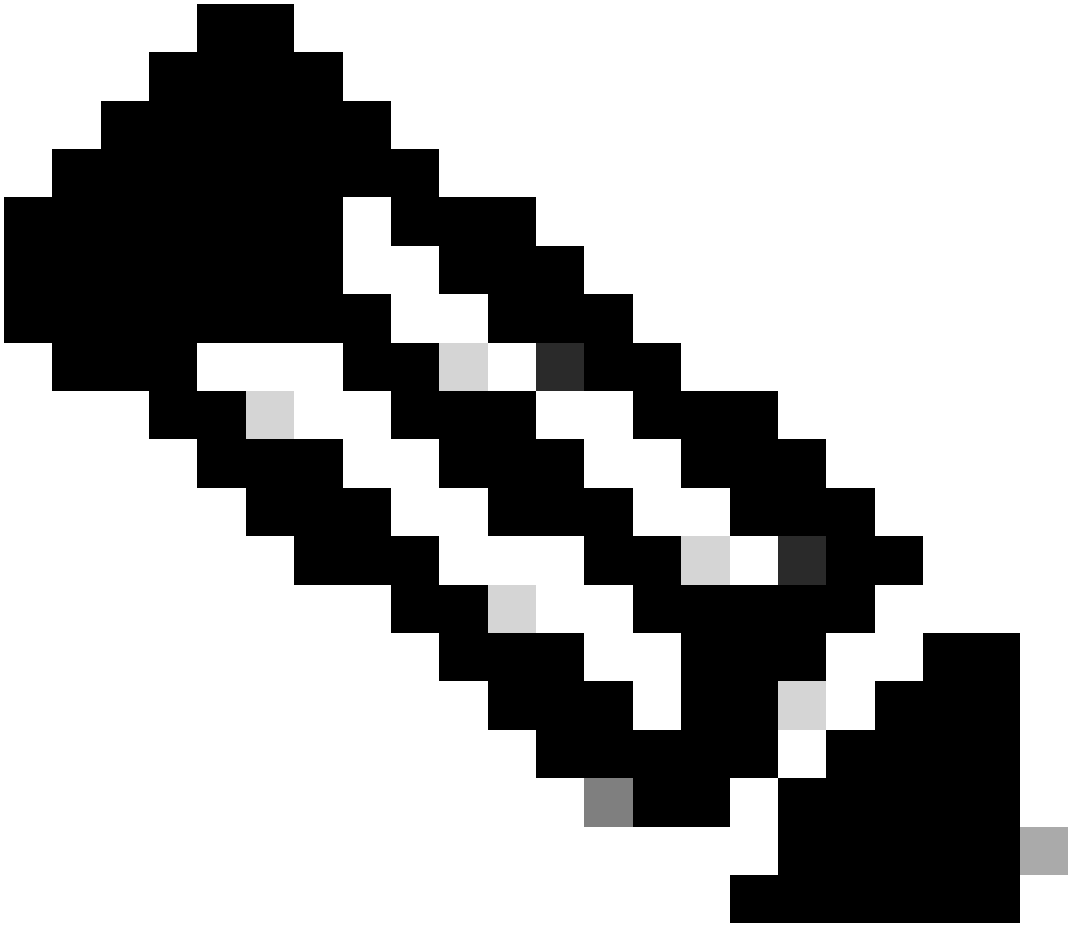
Sommario

Introduzione

Questo documento descrive la configurazione di un tunnel SSH di supporto tecnico on-demand per le appliance virtuali Umbrella.

Tunnel SSH del supporto tecnico on-demand

Un tecnico dell'assistenza può richiedere l'accesso remoto all'appliance virtuale (VA) per diagnosticare ulteriormente una richiesta di assistenza ed eventualmente rivedere o aggiornare le impostazioni per migliorare la disponibilità VA. Affinché un tecnico dell'assistenza Umbrella possa accedere a un VA Umbrella presso la sede del cliente, è necessario attenersi alle presenti linee guida.



Nota: Queste informazioni sono valide solo per VA con versione 2.1.0 o successiva.

Prerequisiti

- Devono essere soddisfatti tutti i requisiti per la configurazione di un VA su VMWare o Hyper-V indicati nella documentazione di installazione.
- Per consentire le connessioni in uscita a s.tunnel.ironport.com, è necessario configurare qualsiasi firewall.
- Il VA tenta di connettersi sulle porte TCP 22, 25, 53, 80, 443 o 4766 in successione.

Per verificare la connettività, è possibile connettersi al tunnel di supporto in modalità telnet:

telnet s.tunnels.ironport.com 25

Prova 63.251.108.107...

Connesso a s.tunnels.ironport.com.

Il carattere di escape è '^]'.

SSH-2.0-OpenSSH_6.2 Tunnel Cisco1

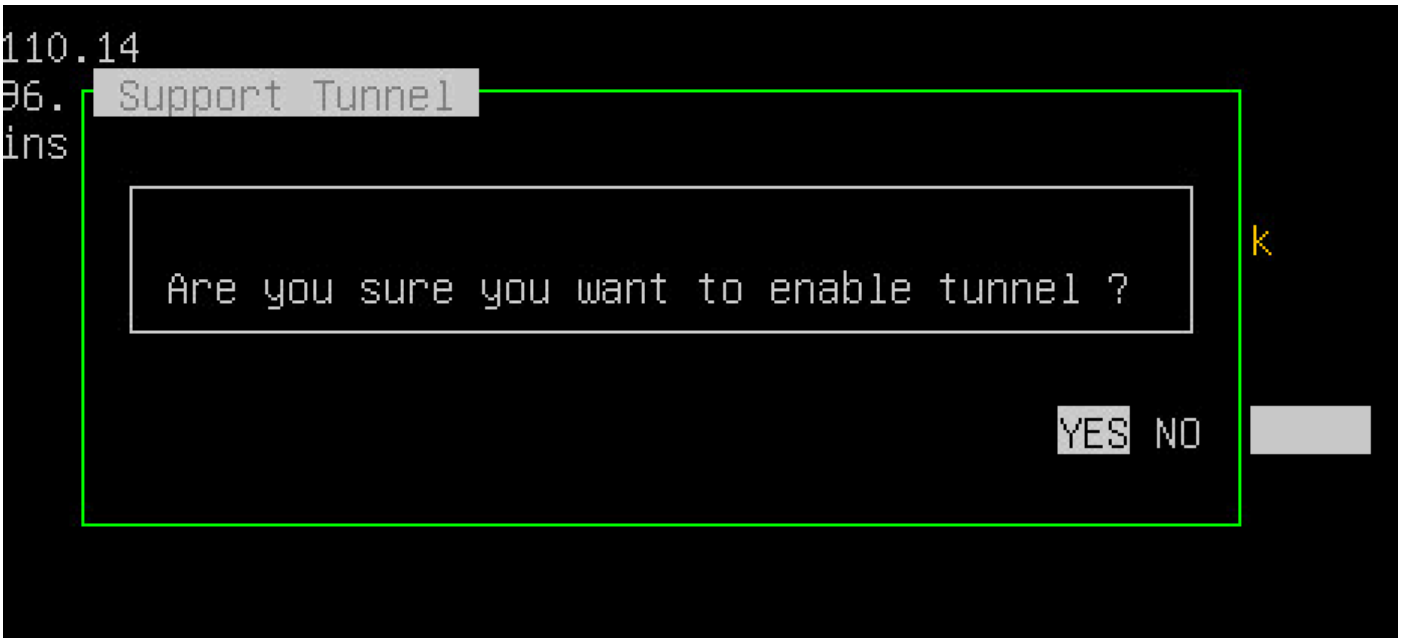
Abilitazione del tunnel

Il tunnel SSH si connette a s.tunnels.ironport.com. La durata della connessione è configurabile, con un valore predefinito di 72 ore.

Abilitazione del tunnel sulle appliance virtuali ospitate in VMware e Hyper-V

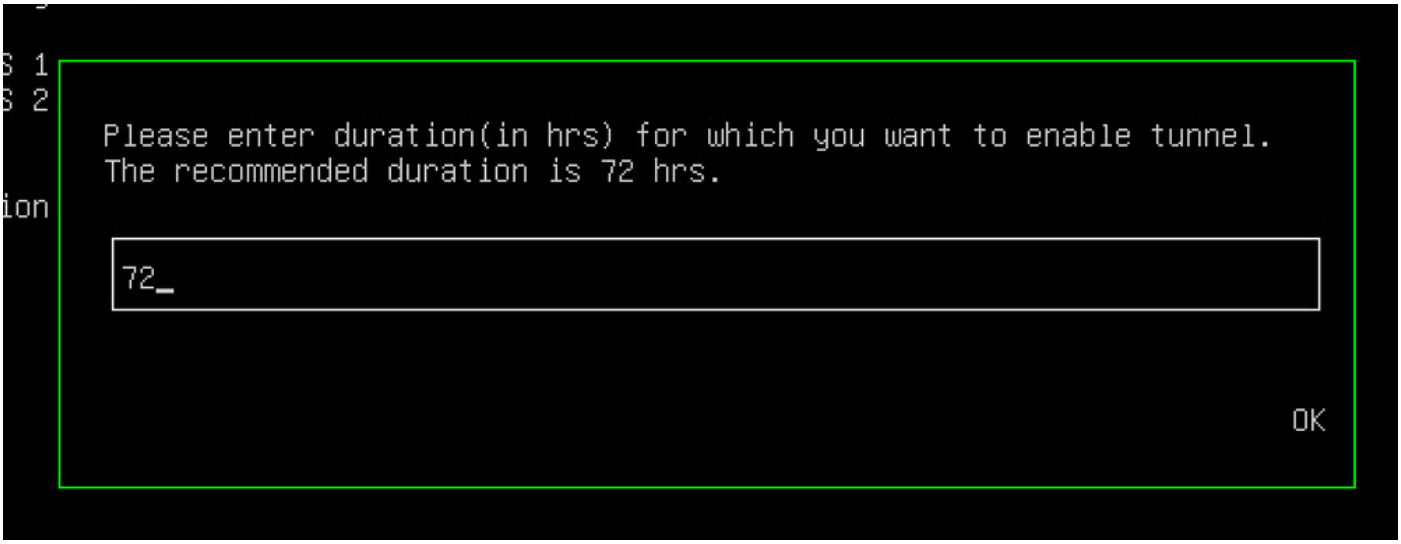
I tunnel possono essere attivati dalla console di VA utilizzando il comando di tastiera "CTRL+T".

Selezionare Yes quando richiesto:



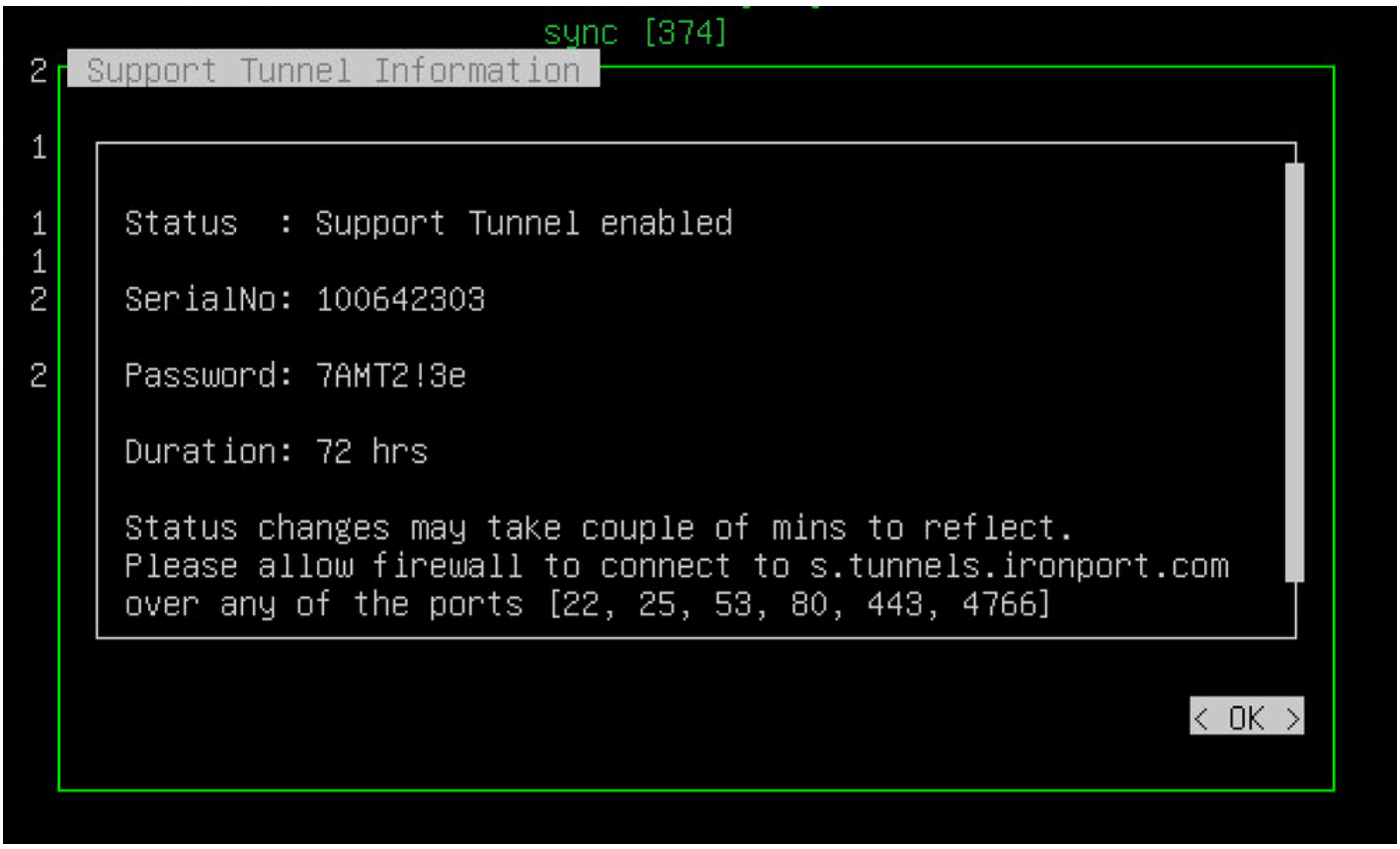
115013855903

Innanzitutto, viene chiesto di definire la durata della sessione del tunnel:



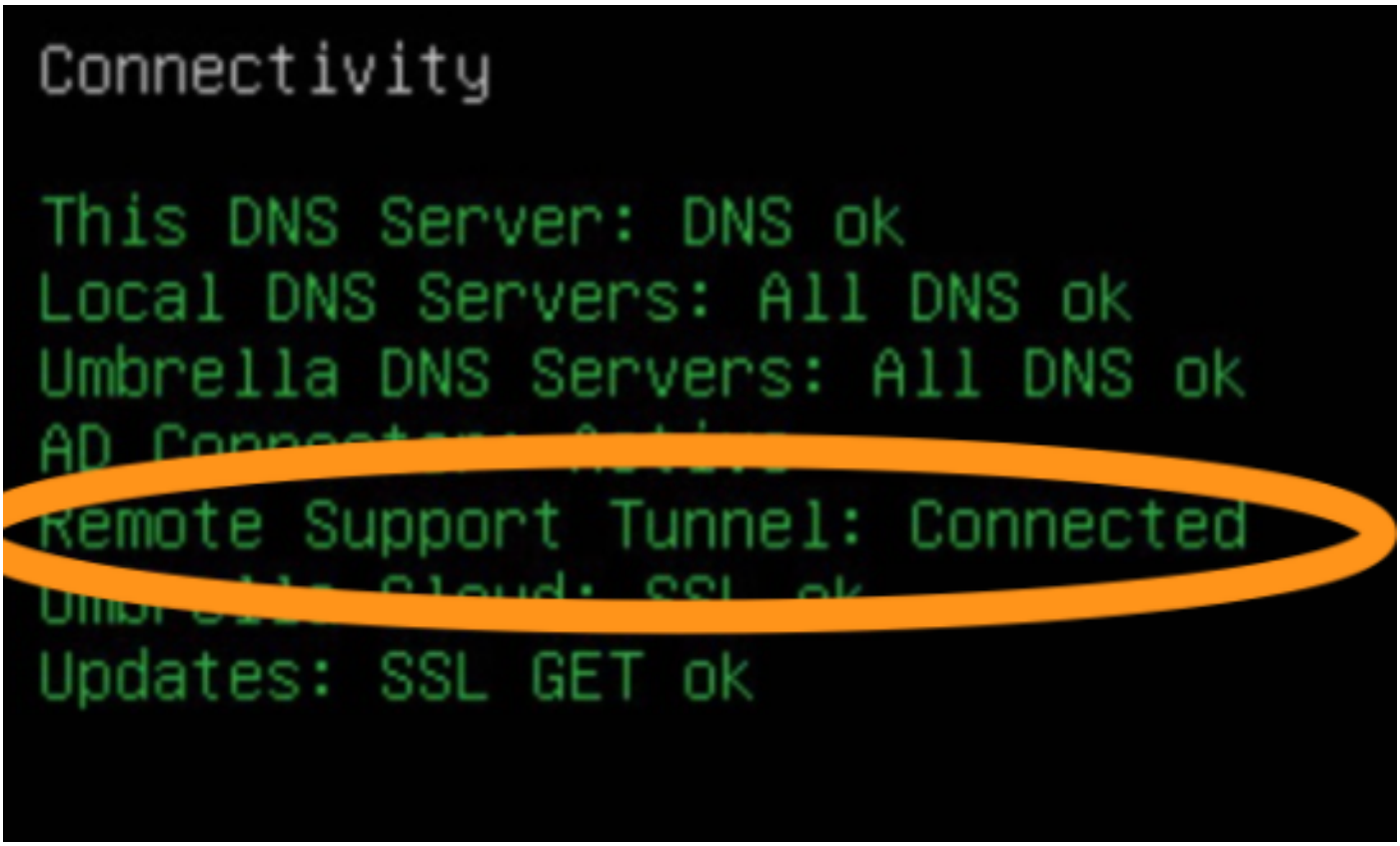
115013856003

Selezionare OK e viene visualizzata una finestra che mostra il numero di serie e la password per il tunnel di supporto. Queste informazioni devono essere trasmesse al tecnico di assistenza. Dopo aver selezionato OK, VA tenta di stabilire una connessione con il server del tunnel di supporto:



115013853243

Fare clic su OK per chiudere la finestra. Verificare che nella console VA sia visualizzato il messaggio "Remote Support Tunnel: Connected" (Connesso).



360000820923

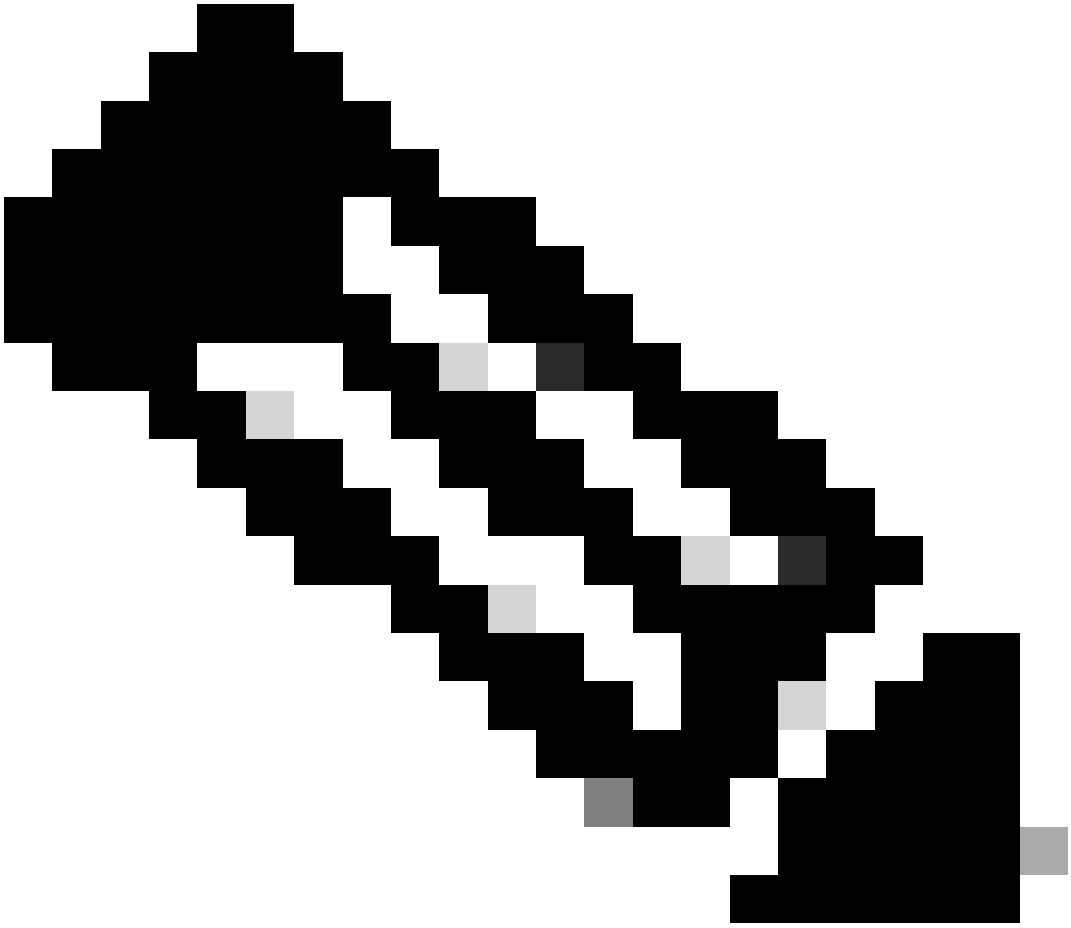
Abilitazione del tunnel su appliance virtuali ospitate su altre piattaforme

Collegarsi a VA over SSH e usare il comando config come indicato di seguito:

- Per abilitare il tunnel di supporto, immettere config tunnel enable <durata in ore>.
- Per disabilitare il tunnel di supporto, immettere config tunnel disable.
- Per controllare lo stato del tunnel di supporto, immettere config tunnel status.
- Per visualizzare queste opzioni, immettere config tunnel help.

Recupero delle credenziali da condividere con il supporto

Il numero di serie e la password visualizzati nella console VSA o quando si utilizza il comando config tunnel status devono essere forniti al tecnico di assistenza.

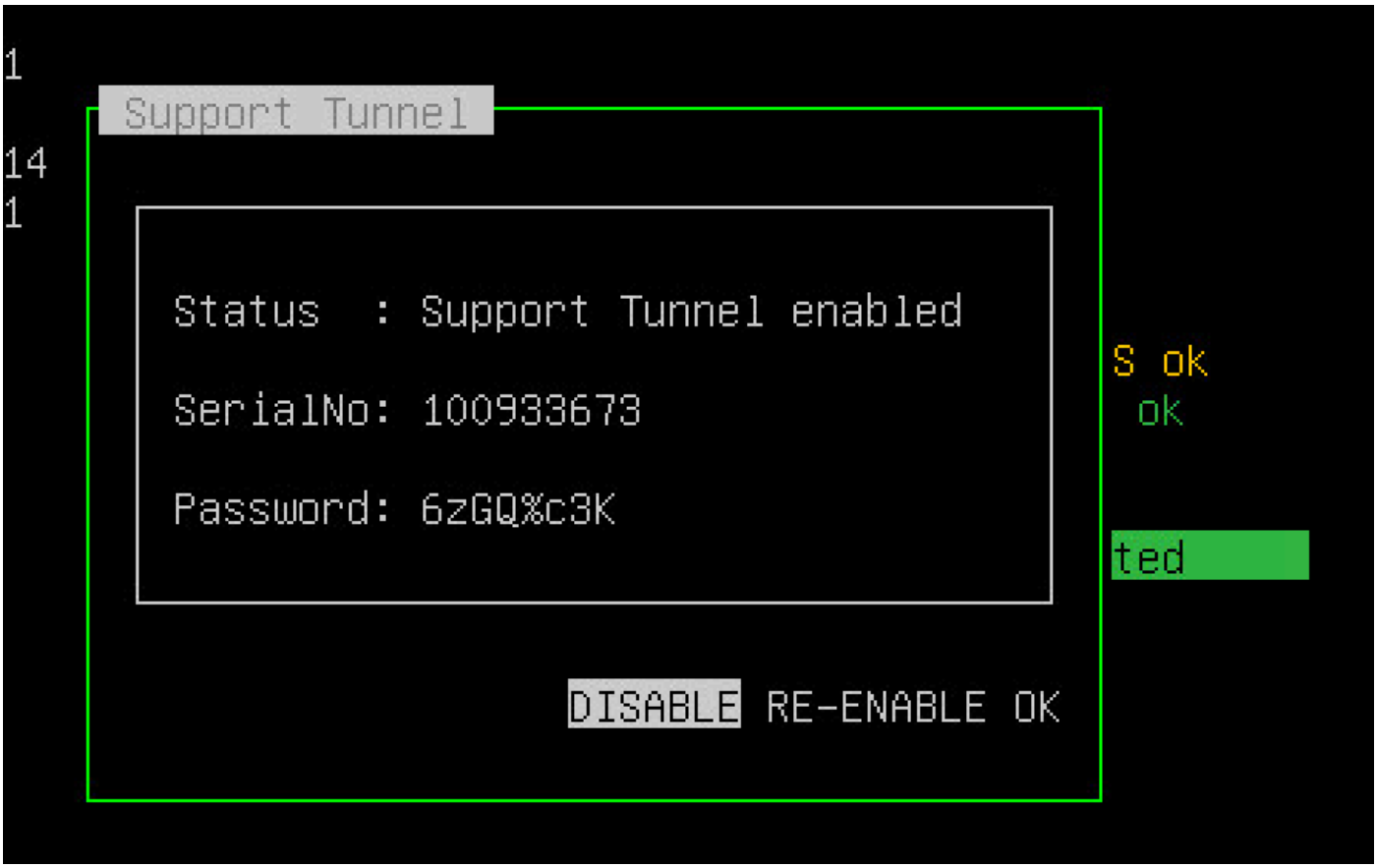


Nota: La password recuperata e condivisa con il supporto non può essere utilizzata direttamente per accedere a VA. Per motivi di sicurezza, la password reale è derivata in modo crittografico dalla password visualizzata. Per ottenere il numero di serie e la password dalla console VA, scatta una schermata dopo aver abilitato il tunnel con Ctrl+T. Assicuratevi che lo screenshot sia leggibile.

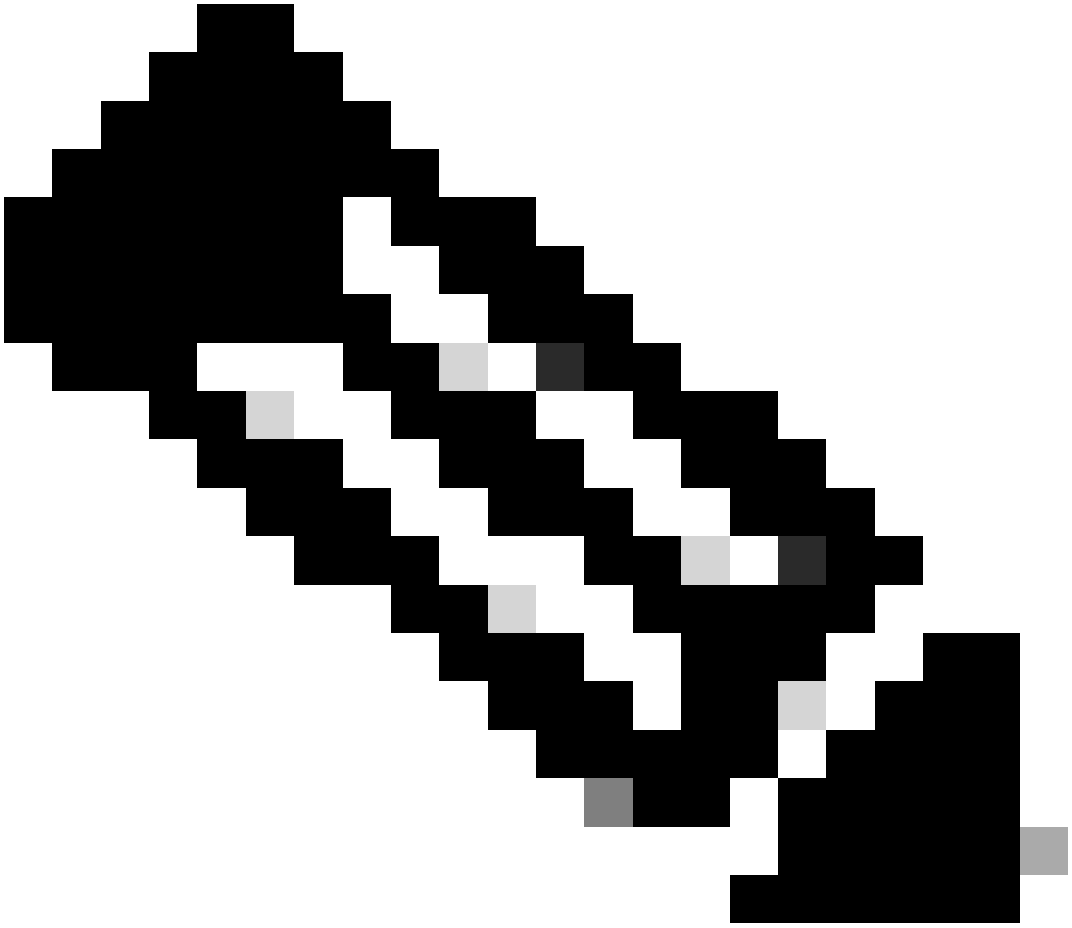
Disabilitazione/Riattivazione del tunnel

Per impostazione predefinita, il tunnel rimane attivo per 72 ore, ma è possibile estenderne la durata utilizzando l'opzione Riattiva (Re-enable).

Su VMware e Hyper-V, il tunnel può essere disabilitato o riabilitato in qualsiasi momento con il comando della tastiera CTRL-T:



115013688906



Nota: La modifica dello stato del tunnel da Connesso a Disabilitato può richiedere fino a un minuto, sia nell'interfaccia utente sia nel back-end, poiché il tunnel viene terminato normalmente.

Su altre piattaforme, è possibile utilizzare questo comando:

- config tunnel reenable <durata in ore>

Se si tenta di riattivare il tunnel subito dopo averlo disabilitato, potrebbero verificarsi delle condizioni anomale e un messaggio di errore perché il tunnel non è completamente disabilitato in questa fase.

La riattivazione del tunnel non comporta la modifica della password per la sessione tunnel esistente del VA. Per impostazione predefinita, selezionando l'opzione Riattiva viene aggiunta 72 ore di durata del tunnel rispetto all'ora corrente.

Stati tunnel

Connesso

Lo stato passa da Disabilitato a Connesso non appena il tunnel viene abilitato. Se la connessione ha esito positivo, notare che lo stato rimane in modalità Connessione per circa un minuto, quando l'amministratore di sistema tenta di stabilire il proprio tunnel con il server.

Disabled

Se il tunnel non è stato abilitato in modo esplicito, viene visualizzato lo stato Disabilitato. Dopo aver disabilitato esplicitamente il tunnel, occorrerà circa un minuto prima che lo stato del tunnel passi da Connesso a Disabilitato.

Collegamento

In stato di connessione, il VSA sta tentando di stabilire il tunnel (provando le porte 22, 25, 53, 80, 443 e 4766 in sequenza) con un ritardo di 5 minuti tra ogni tentativo. Il VA rimane in questo stato fino a quando non viene stabilita una connessione, oppure sono trascorsi 30 minuti senza che sia stata stabilita una connessione.

La connessione può non riuscire a causa di problemi di rete, ad esempio porte bloccate.

Timeout

Se la VA non è in grado di stabilire una connessione con il server remoto, lo stato passa a Timeout. Il timeout si verifica circa 30 minuti dopo che l'amministratore di sistema ha tentato di stabilire un tunnel con il server remoto.

Continuità del tunnel

Una volta abilitato un tunnel di supporto, il VA rispetta il valore immesso per la durata anche se il VA viene riavviato o aggiornato. Non sono necessarie ulteriori azioni. Se il VLAN si riavvia o si aggiorna e il tempo rimane entro la durata specificata, il VAR tenta di riconnettersi automaticamente al server del tunnel SSH.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).