Risoluzione dei problemi relativi a Host e aggiunta di errori di certificato

Sommario

Introduzione

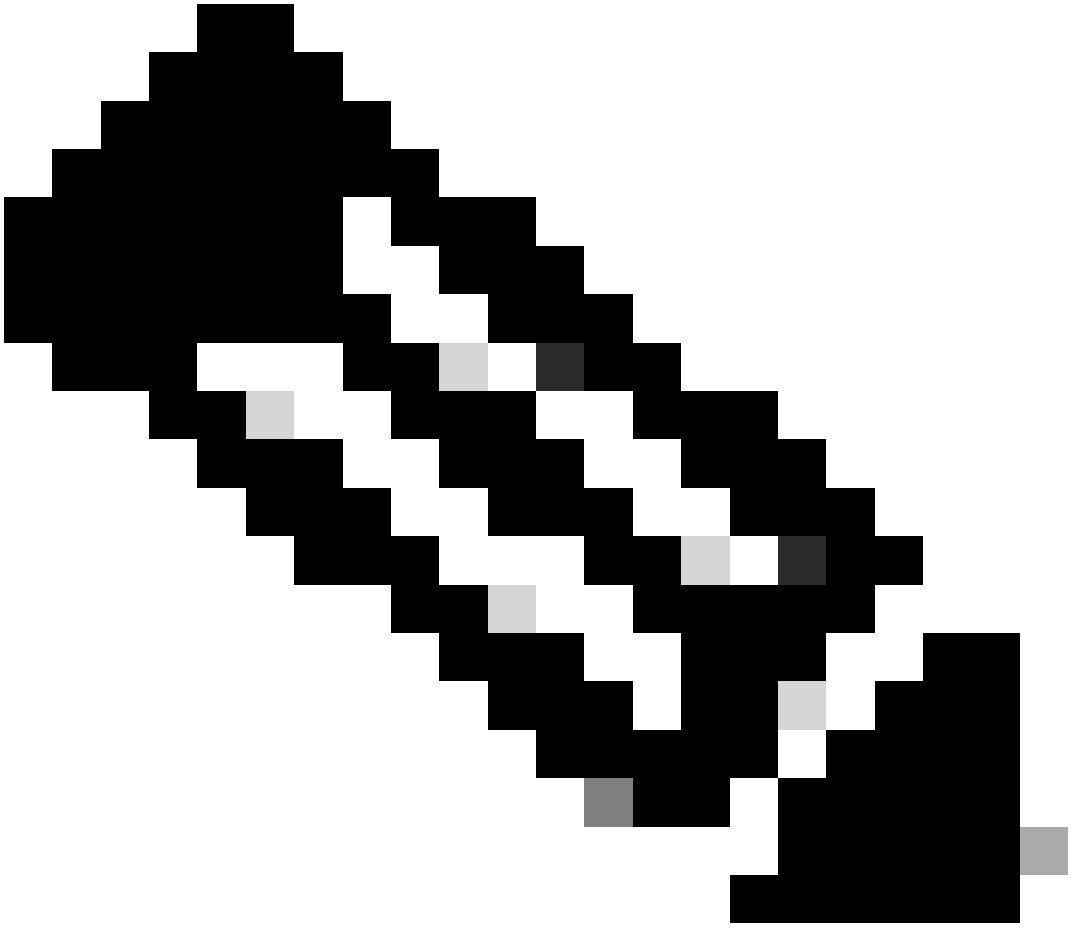
In questo documento viene descritto come cancellare un errore di certificato "La connessione è non attendibile/non privata" che non può essere ignorato.

Errore certificato

Quando viene visualizzato un errore di certificato per `*.opendns.com` o `*.cisco.com` che non può essere ignorato aggiungendo un'eccezione di certificato come indicato nella documentazione di Cisco Umbrella Gestione del certificato radice Cisco Umbrella, attenersi alla seguente procedura per consentire la cancellazione dell'errore di certificato.

Quando non è possibile ignorare l'errore del certificato aggiungendo un'eccezione, ciò è dovuto all'implementazione di HTTP Strict Transport Security (HSTS) o al Pinning del certificato precaricato nei browser moderni. La comunicazione tra determinati browser e determinati siti Web viene effettuata in modo da includere l'obbligo di utilizzare HTTPS e non è possibile ignorare o escludere eccezioni. Questa sicurezza aggiuntiva per le pagine HTTPS impedisce il funzionamento del meccanismo di blocco delle pagine Umbrella e bypass quando HSTS è attivo per un sito Web.

Di conseguenza, la pagina in questione non è accessibile tramite BPB (Block Page Bypass) (in realtà, la schermata Bypass potrebbe non apparire). Questi metodi possono consentire l'accesso a BPB, ma dopo l'accesso, l'errore del certificato riappare e nega l'accesso. Rivedere il resto di questo articolo se si sta vedendo un errore di certificato in Google Chrome, Mozilla Firefox, Safari che non può essere ignorato e si sta cercando di accedere al bypass login.



Nota: Per questo problema è ora disponibile una soluzione più semplice da gestire e persistente per tutti i siti.

Di conseguenza, queste informazioni sono ancora valide ma possono ora essere risolte con una soluzione permanente. Provare a installare la CA radice Cisco utilizzando la documentazione di Cisco Umbrella: Gestisci certificato radice Cisco Umbrella

---

IMPORTANTE: Se il dominio è incluso nell'elenco dei domini bloccati HSTS, non è possibile aggiungere un'eccezione poiché l'elenco non può essere ignorato se si esegue Chrome, Safari o Firefox (Internet Explorer) non è interessato). L'opzione Blocca bypass pagina non funziona per siti di questo tipo. Per un elenco completo dei servizi che utilizzano HSTS da questi tre browser, si prega di rivedere la Ricerca del Codice Chromium di Google. Tra i servizi di rilievo inclusi in questo elenco sono inclusi:

- Google (e le risorse di Google, come Gmail, Youtube o Google Docs)
- Dropbox
- Twitter

- Facebook

Se questo causa un problema per te o per i tuoi utenti e desideri vedere le modifiche al Blocca bypass pagina per risolvere il problema, invia un'e-mail a umbrella-support@cisco.com o al tuo Account Manager per inviare una richiesta di funzionalità. I nostri team di gestione dei prodotti e di progettazione sono consapevoli delle difficoltà con i certificati e il blocco del bypass delle pagine e stanno testando riprogettazioni alternative di questa funzione.

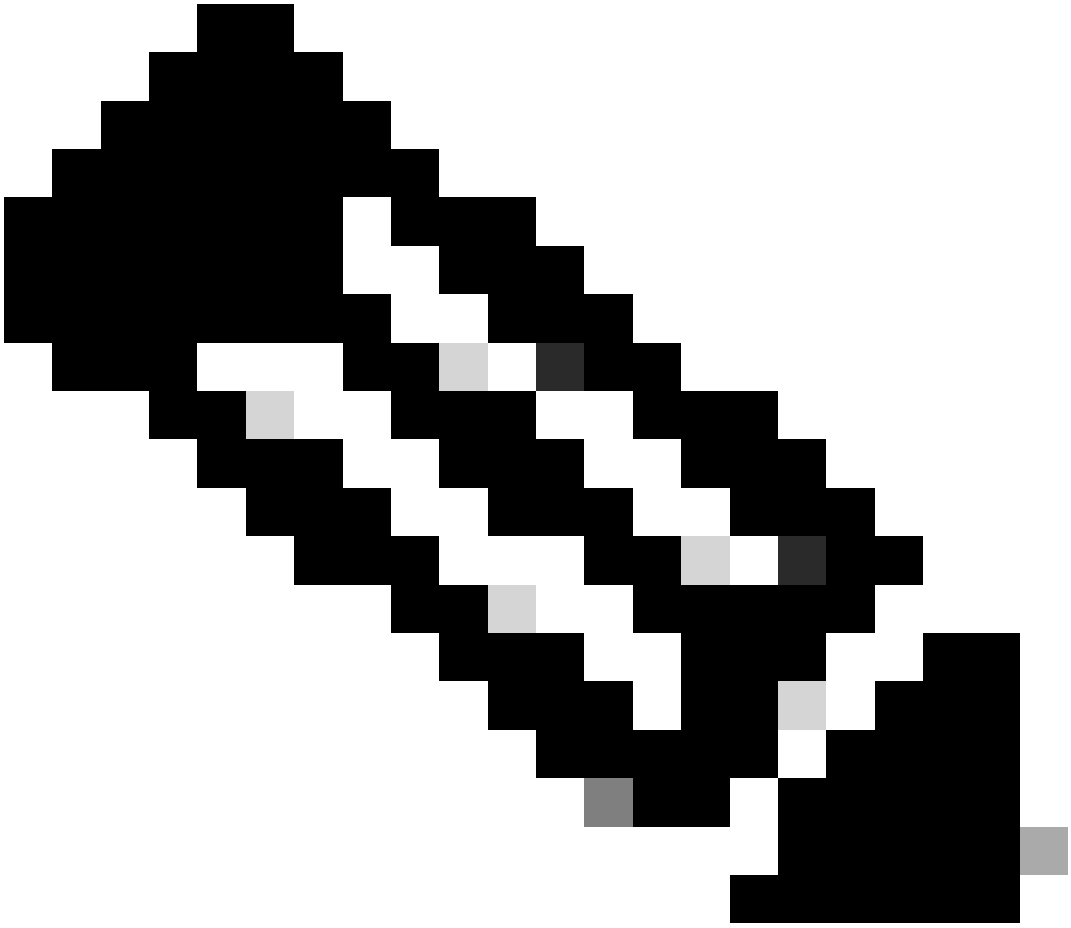
Soluzioni possibili

Ci sono alcuni modi per risolvere questi problemi. In primo luogo, queste sezioni dimostrano come utilizzare criteri più granulari per risolvere il problema. In secondo luogo, è possibile utilizzare le configurazioni dei browser, che tuttavia sono isolate in un sottoinsieme dei browser interessati da questo problema.

Gestione dei criteri e client mobile

Potrebbero verificarsi problemi con la configurazione della rete o con i criteri di utilizzo accettabile (HR) che impediscono la risoluzione di questo problema. La gestione delle policy non è una soluzione efficace se gli utenti sono autorizzati a visitare questi domini solo in determinati momenti (ad esempio durante la pausa pranzo). Umbrella non può fornire un'applicazione di criteri basata sul tempo con il nostro servizio, quindi consentire semplicemente a un utente di accedere al sito in ogni momento potrebbe essere problematico. In un computer condiviso, ad esempio un terminale pubblico, il client di roaming Umbrella non è in grado di distinguere tra gli utenti e non può facilmente consentire i domini corretti per le persone giuste.

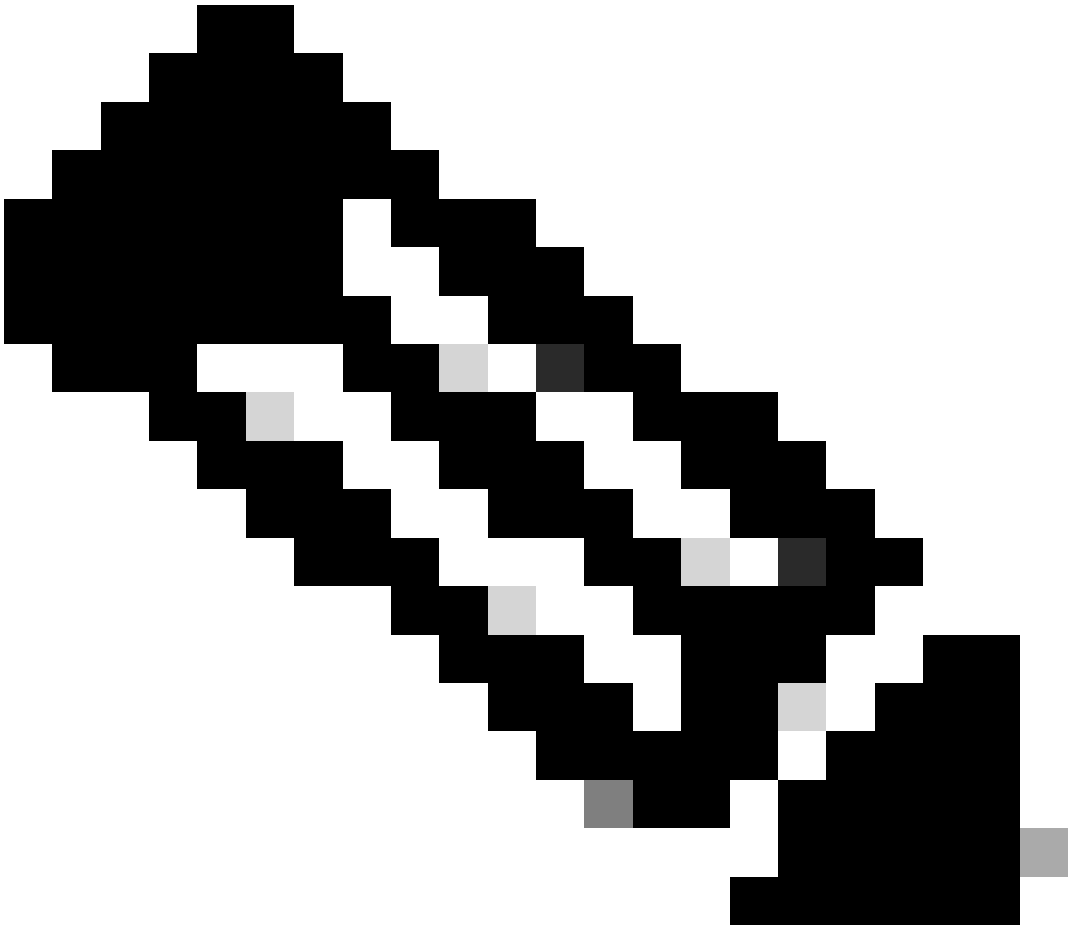
La gestione delle policy non è altrettanto efficace quando si considerano le identità non granulari, come i siti o le reti, a meno che l'amministratore non abbia familiarità nel concedere lo stesso accesso a tutti gli utenti della rete. La gestione dei criteri offre risultati migliori se applicata a un sottoinsieme di utenti a cui è consentito l'accesso ai siti mentre il resto della rete non è in grado di accedervi, individuando tali utenti installando il client di roaming nei computer e applicando la gerarchia dei criteri appropriata.



Nota: Cisco ha annunciato la fine del ciclo di vita per Umbrella Roaming Client il 2 aprile 2024. L'ultima data di supporto per Umbrella Roaming Client è il 2 aprile 2025. Tutte le funzionalità di Umbrella Roaming Client sono attualmente disponibili in Cisco Secure Client. Cisco offre innovazioni future solo in Cisco Secure Client. È consigliabile che i clienti inizino a pianificare e pianificare la migrazione. Fare riferimento a questo articolo della Knowledge Base per istruzioni su come eseguire la migrazione da Umbrella Roaming Client a Cisco Secure Client.

Una corretta gestione dei criteri è la soluzione migliore per questo problema, in quanto il browser non riceve una risposta di convalida non riuscita. Se ad alcuni utenti è consentito l'accesso a siti a cui normalmente dovrebbero accedere mediante l'opzione Blocca esclusione pagine, è possibile configurare un criterio distinto per tali utenti e aggiungere i domini che possono essere utilizzati all'elenco degli utenti autorizzati. Poiché le richieste degli utenti non vengono mai bloccate, il browser non riceve mai una richiesta da un dominio con un certificato non corrispondente. È possibile utilizzare il client di roaming Umbrella per implementare questi criteri specifici. Ciò significa che si stanno inserendo determinati domini in un elenco Consenti ad alcuni utenti in qualsiasi momento della

giornata di risolvere questi errori.



Nota: Il client di roaming Umbrella rappresenta un modo efficace per distribuire criteri particolari a più utenti, ma se è stata abilitata l'integrazione con Active Directory (AD), è possibile applicare questi criteri consentiti anche a determinati utenti AD.

Ignorare gli errori relativi alle eccezioni dei certificati (solo Chrome per Windows)

Solo Chrome per Windows può essere configurato per ignorare gli errori di Eccezione certificato, che riduce questo errore. Al browser viene detto di ignorare l'errore e viene invece visualizzata la normale pagina di blocco Umbrella.

IMPORTANTE: Questo metodo è più rischioso rispetto alla regolazione della gestione dei criteri perché il browser è configurato per ignorare gli errori del certificato. È possibile che, di conseguenza, il browser possa essere soggetto ad attacchi man-in-the-middle (MiTM). Di

conseguenza, non possiamo raccomandare questo come approccio sicuro per la gestione di questo errore, ma si tratta di una soluzione.

Queste modifiche alla configurazione devono essere apportate per singoli computer, il che lo rende difficile per gli ambienti su larga scala, ma funziona.

Firefox, Safari e Chrome per Mac OS X

Firefox, Safari e Chrome per Mac OS X non possono essere configurati per ignorare gli errori delle eccezioni dei certificati per i domini bloccati e rispetta sempre l'elenco HSTS. Per questi errori non sono disponibili soluzioni alternative.

Internet Explorer

Internet Explorer (IE) non implementa le restrizioni HSTS. Di conseguenza, IE non deve essere configurato e non visualizza questo errore. Questa opzione è soggetta a modifiche nelle versioni future di IE se Microsoft sceglie di implementare HSTS nel browser.

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).