Domande frequenti su Secure Access Control System 5.x e versioni successive

Sommario

Introduzione

Questo documento contiene le risposte alle domande più frequenti (FAQ) relative a Cisco Secure Access Control System (ACS) 5.x e versioni successive.

Problemi correlati all'autenticazione

D. È possibile escludere alcuni utenti/gruppi del database interno ACS 5.x dai criteri password utente (Amministrazione sistema > Utenti > Impostazioni autenticazione)?

R. Per impostazione predefinita, ogni utente interno del database deve rispettare i criteri password utente. Al momento non è possibile escludere utenti/gruppi del database interno di ACS 5.x.

D. È possibile escludere alcuni amministratori GUI di ACS 5.x dai criteri di gestione delle password degli utenti (Amministrazione sistema > Amministratori > Impostazioni > Autenticazione)?

R. Per impostazione predefinita, ogni utente amministrativo della GUI deve rispettare i criteri per la password dell'utente amministrativo. Al momento non è possibile escludere alcun utente amministrativo di ACS 5.x.

D. ACS 5.x fornisce supporto per gli strumenti VMWare?

R. No. Al momento, gli strumenti VMWare non sono supportati con ACS versione 5.x. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtg50048 (solo utenti registrati).

D. Quali sono i protocolli di autenticazione EAP supportati per ACS 5.x quando LDAP è configurato come archivio identità?

R. Quando si usa LDAP come archivio identità, ACS 5.2 supporta solo i protocolli PEAP-GTC, EAP-FAST-GTC e EAP-TLS. Non supporta EAP-FAST MSCHAPv2, PEAP EAP-MSCHAPv2 e EAP-MD5. Per ulteriori informazioni, fare riferimento a Compatibilità protocollo di autenticazione e database utenti.

D. Perché l'autenticazione per il WLC con raggio di utilizzo su ACS non è riuscita e perché ACS non ha mostrato alcun tentativo non riuscito?

R. Esiste un problema di **interoperabilità** con **ACS 5.0 e WLC** prima della patch 4. Scaricare la patch 8 e applicare la patch sulla CLI. Non utilizzare il protocollo TFTP per risolvere il problema.

D. Perché non è possibile ripristinare i file tar.gz di cui è stato eseguito il backup con il comando backup-log in ACS 5.2?

R. Non è possibile ripristinare i file di log di cui è stato eseguito il backup con il comando **backup-log**. È possibile ripristinare solo i file di cui è stato eseguito il backup per la configurazione ACS e ADE-OS. Per ulteriori informazioni, consultare i comandi **backup** e **backup-logs** nella CLI Reference Guide for the Cisco Secure Access Control System 5.1.

D. È possibile limitare il numero di tentativi di password non riusciti in ACS 5.2?

R. No. Questa funzione non è disponibile su ACS 5.2, ma si prevede che venga integrata in ACS 5.3. Per ulteriori informazioni, consultare la sezione Caratteristiche non supportate delle note sulla versione di Cisco Secure Access Control System 5.2.

D. Non è possibile modificare la password al prossimo accesso per gli utenti interni in ACS 5.0. Come risolvere il problema?

R. L'opzione di modifica della password al prossimo accesso non è supportata in ACS 5.0. Il supporto per questa funzione è disponibile in ACS 5.1 e versioni successive.

D. Cosa significa questo allarme su ACS?

```
Cisco Secure ACS - Alarm Notification
Severity: Warning
Alarm Name delete 20000 sessions
Cause/Trigger active sessions are over limit
Alarm Details session is over 250000
```

R. Questo errore indica che quando la visualizzazione ACS raggiunge il limite di 250.000 sessioni, viene generato un avviso che indica l'eliminazione di 20.000 sessioni. Il database di visualizzazione ACS memorizza tutte le sessioni di autenticazione precedenti e, quando raggiunge le 250.000, invia un allarme per cancellare la cache ed eliminare 20.000 sessioni.

D. Come risolvere questo messaggio di errore: `Autenticazione non riuscita: 24407 Autenticazione utente con Active Directory non riuscita. È necessario modificare la password`?

R. Questo messaggio di errore viene visualizzato quando si verifica un problema con la gestione della password durante l'autenticazione SDI. ACS 5.x viene utilizzato come proxy Radius e gli utenti devono essere autenticati da un server RSA. Il proxy Radius per RSA funziona solo senza gestione della password. Il motivo è che il valore OTP deve essere recuperabile dal server Radius per poter inviare il valore della password al server RSA. Quando la gestione delle password è abilitata nel gruppo di tunnel, la richiesta Radius viene inviata con gli attributi MS-CHAPv2. RSA non supporta MS-0CHAPv2; supporta solo PAP.

Per risolvere il problema, disabilitare la gestione delle password. Per ulteriori informazioni, fare

riferimento all'ID bug Cisco CSCsx47423 (solo utenti registrati).

D. È possibile impedire all'amministratore ACS di gestire solo alcuni dispositivi all'interno di ACS 5.1?

R. No, non è possibile impedire all'amministratore ACS di gestire solo alcuni dispositivi all'interno di ACS 5.1.

D. L'ACS supporta la funzionalità QoS nell'autenticazione in modo che sia possibile assegnare una priorità a RADIUS rispetto a TACACS?

R. No, ACS non supporta QoS nell'autenticazione. ACS non assegna priorità alle richieste di autenticazione RADIUS rispetto alle richieste TACACS o TACACS rispetto a RADIUS.

D. ACS 5.x può fungere da proxy per l'autenticazione TACACS e RADIUS ad altri server TACACS o RADIUS?

R. Sì, tutte le versioni ACS 5.x possono inoltrare le autenticazioni RADIUS ad altri server RADIUS. ACS 5.3 e versioni successive possono inoltrare le autenticazioni TACACS ad altri server TACACS.

D. ACS 5.x può controllare gli attributi della connessione remota di un utente di Active Directory per concedere l'accesso?

R. Sì, in ACS 5.3 e versioni successive è possibile consentire, negare e controllare l'accesso alle autorizzazioni della connessione remota di un utente. Le autorizzazioni vengono controllate durante le autenticazioni o le query da Active Directory. È impostato nel dizionario dedicato di Active Directory.

D. ACS 5.x supporta i tipi di autenticazione CHAP o MSCHAP per TACACS+?

R. Sì, i tipi di autenticazione TACACS+ CHAP e MSCHAP sono supportati nelle versioni 5.3 e successive di ACS.

D. È possibile impostare il tipo di password di un utente interno ACS su un database esterno?

R. Sì, in ACS 5.3 e versioni successive è possibile impostare il tipo di password di un utente interno ACS. Questa funzione era disponibile in ACS 4.x.

D. È possibile superare o fallire un'autenticazione in base all'ora di creazione dell'utente nell'archivio di identità interno di ACS?

R. Sì, in ACS 5.3 e versioni successive è possibile utilizzare l'attributo **Numero di ore dalla creazione dell'utente** per creare le regole. Questo attributo contiene il numero di ore dalla creazione dell'utente nell'archivio identità interno fino all'ora della richiesta di autenticazione corrente.

D. È possibile utilizzare i caratteri jolly per aggiungere una nuova voce host nel database interno ACS?

R. Sì, ACS 5.3 e versioni successive consentono di utilizzare i caratteri jolly quando si aggiungono nuovi host all'archivio identità interno. Consente inoltre di immettere caratteri jolly (dopo aver immesso i primi tre ottetti) per specificare tutti i dispositivi del produttore identificato.

D. È possibile configurare pool di indirizzi IP su ACS 5.x e assegnarli da ACS?

R. No, al momento non è possibile creare pool di indirizzi IP su ACS 5.x.

D. È possibile visualizzare l'indirizzo IP del client AAA a cui è stata inoltrata la richiesta nel report FAILED AUTHENTICATION?

R. No, non è possibile visualizzare l'indirizzo IP del client AAA da cui è arrivata la richiesta.

D. Che cos'è View Log Message Recovery in ACS 5.3?

R. ACS 5.3 offre una nuova funzionalità per il recupero di eventuali log mancanti quando la vista non è attiva. ACS raccoglie i registri mancanti e li memorizza nel proprio database. Utilizzando questa funzione, è possibile recuperare i log mancanti dal database ACS al database delle viste dopo il backup della vista. Per utilizzare questa funzionalità, è necessario impostare la configurazione di ripristino dei messaggi **di** log su **on**. Per ulteriori informazioni sulla configurazione del recupero dei messaggi di log, vedere Monitoraggio e operazioni di sistema di Visualizzatore report.

D. È possibile comprimere il database ACS 5.x eseguendo il comando database-compress dalla CLI di Solution Engine? Questa funzione era disponibile in ACS 4.x.

R. Sì, in ACS 5.3 e versioni successive, il comando **database-compress** riduce le dimensioni del database ACS con la possibilità di eliminare la tabella delle transazioni ACS. Gli amministratori ACS possono usare questo comando per ridurre le dimensioni del database. Ciò consente di ridurre le dimensioni del database e il tempo necessario per i backup e la sincronizzazione completa necessaria per la manutenzione.

D. È possibile cercare una voce di un client AAA in base al relativo indirizzo IP?

R. Sì, ACS 5.3 e versioni successive consentono di cercare un dispositivo di rete utilizzando il relativo indirizzo IP. Per cercare un gruppo specifico di dispositivi di rete, è possibile anche utilizzare i caratteri jolly e l'intervallo.

D. È possibile creare una condizione in base all'ora di creazione dell'utente nell'archivio di identità interno di ACS?

R. Sì, in ACS 5.3 e versioni successive è possibile utilizzare l'attributo **Numero di ore dalla creazione dell'utente** che consente di configurare le condizioni delle regole dei criteri in base all'ora di creazione dell'utente nell'archivio identità interno di ACS. Ad esempio: IF **group=HelpDesk&NumberofHoursSinceUserCreation>48,** quindi rifiutare. Questo attributo contiene il numero di ore dalla creazione dell'utente nell'archivio identità interno fino all'ora della

richiesta di autenticazione corrente.

D. È possibile verificare in quale archivio di identità l'utente è stato autenticato nella sezione Autorizzazione di un criterio del servizio?

R. Sì, in ACS 5.3 e versioni successive è possibile utilizzare l'attributo **Authentication Identity Store**, che consente di configurare le condizioni della regola dei criteri in base all'Authentication Identity Store. Ad esempio: IF **AuthenticationIdentityStore=LDAP_NY**, quindi rifiutare. Questo attributo contiene il nome dell'archivio di identità utilizzato e viene aggiornato con il nome dell'archivio di identità pertinente dopo l'autenticazione riuscita.

D. Quando l'ACS passa all'archivio identità successivo definito nella sequenza dell'archivio identità?

R. L'ACS passa all'archivio identità successivo definito nella sequenza di archivi identità nei seguenti scenari:

- Impossibile trovare un utente nel primo archivio identità
- Archivio identità non disponibile nella sequenza

D. In che modo viene applicata la policy di disattivazione dell'account in ACS 5.3?

R. Il criterio di disabilitazione dell'account consente di disabilitare gli utenti dell'archivio identità interno quando la data configurata è successiva alla data consentita, il numero di giorni configurato è superiore ai giorni consentiti o il numero di tentativi di login non riusciti consecutivi supera la soglia. Il valore predefinito per la data supera i 30 giorni dalla data corrente. Il valore predefinito per i giorni non deve essere superiore a 60 giorni dal giorno corrente. Il valore predefinito per i tentativi non riusciti è 5.

D. È possibile modificare la password di un utente del database interno di ACS su telnet?

R. Sì, è possibile modificare la password di un utente del database interno utilizzando TACACS+ su telnet. È necessario selezionare **Enable TELNET Change Password** in **Password Change Control** (Controllo modifica password su ACS 5.x).

D. L'istanza ACS 5.x primaria aggiorna automaticamente le istanze di backup periodicamente o dovrebbe essere eseguita solo quando una configurazione è stata modificata?

R. ACS 5.x verrà immediatamente replicato nell'ACS secondario ogni volta che si apportano modifiche nell'ACS principale. Inoltre, se non si apportano modifiche all'ACS principale, verrà forzata la replica ogni 15 minuti. A questo punto, non è disponibile un'opzione per controllare il timer in modo che ACS possa replicare le informazioni dopo un determinato periodo di tempo.

D. È possibile visualizzare/esportare un report su ACS 5.x di tutti gli utenti attualmente connessi e autenticati da ACS su client NAS diversi?

R. Sì, è possibile. Esistono due rapporti distinti per RADIUS e TACACS+. Sono disponibili in

Monitoraggio e report > Report > Catalogo > **Directory di sessione** > **Sessioni attive RADIUS** e **Sessioni attive TACACS**. Entrambi i report sono basati sulle informazioni di accounting dei client NAS, in quanto consentono di tenere traccia della connessione e della disconnessione dell'utente. La cronologia della sessione consente inoltre di ottenere informazioni dai messaggi di avvio e di arresto durante un giorno specifico.

Informazioni correlate

- Pagina di supporto di Cisco Secure Access Control System
- Documentazione e supporto tecnico – Cisco Systems