Domande frequenti ESA: Quali sono i livelli di accesso amministrativo disponibili per l'ESA?

Sommario

Introduzione

In questo documento vengono descritti i vari livelli di accesso amministrativo, o ruoli utente predefiniti, disponibili in Email Security Appliance (ESA).

Quali sono i livelli di accesso amministrativo disponibili per l'ESA?

Quando si crea un nuovo account utente, si assegna l'utente a un ruolo utente predefinito o personalizzato. Ogni ruolo utente contiene diversi livelli di privilegi all'interno del sistema operativo e dell'accessorio, come indicato di seguito:

Administrators	Gli account utente con ruolo Amministratore hanno accesso completo a tutte le impostazio di configurazione del sistema. Tuttavia, solo l'utente admin ha accesso ai comandi **resetconfig** e **revert**.
Operatori	Gli account utente con ruolo Operatore sono limitati da: • Creazione o modifica di account utente. • Esecuzione del comando **resetconfig**. • Aggiornamento dell'accessorio. • Eseguire il comando **systemsetup** o eseguire la Configurazione guidata sistema. • Esecuzione del comando **adminaccessconfig**. • Esecuzione di alcune funzioni di quarantena (tra cui la creazione, la modifica, l'eliminazione e la centralizzazione delle quarantene). • Modifica delle impostazioni del profilo del server LDAP diverse da nome utente e password, se LDAP è abilitato per l'autenticazione esterna. In caso contrario, dispongono degli stessi privilegi del ruolo Administrator.
Operatori di sola lettura	Gli account utente con ruolo Operatore di sola lettura hanno accesso per visualizzare le informazioni di configurazione. Gli utenti con il ruolo Operatore di sola lettura possono apportare e inviare modifiche per vedere come configurare una funzionalità, ma non posso eseguirne il commit. Gli utenti con questo ruolo possono gestire i messaggi in quarantena, l'accesso è abilitato in quarantena. Gli utenti con questo ruolo non possono accedere a: • File system, FTP o SCP. • Impostazioni per la creazione, la modifica, l'eliminazione o la centralizzazione delle quarantene.
Guest	Gli account utente con ruolo Guest possono visualizzare solo le informazioni sullo stato. G utenti con il ruolo Guest possono anche gestire i messaggi in quarantena, se l'accesso è

	abilitato in quarantena. Gli utenti con il ruolo Guest non possono accedere a Verifica messaggi.
Tecnico	Gli account utente con il ruolo di tecnico possono eseguire aggiornamenti del sistema, riavviare l'accessorio e gestire le chiavi di funzionalità. Per aggiornare l'accessorio, i tecnic possono inoltre eseguire le seguenti operazioni: • Sospendi recapito e ricezione e-mail. • Visualizzare lo stato della coda di lavoro e dei listener. • Salvare i file di configurazione e inviarli per posta elettronica. • Eseguire il backup di elenchi di sicurezza e di blocchi. I tecnici non possono ripristinar questi elenchi. • Scollegare l'accessorio da un cluster. • Abilitare o disabilitare l'accesso al servizio remoto per il supporto tecnico Cisco. • Generare una richiesta di supporto.
Utenti Help Desk	Gli account utente con ruolo di utente Help Desk sono limitati a: • Verifica messaggi. • Gestione dei messaggi in quarantena. Gli utenti con questo ruolo non possono accedere al resto del sistema, inclusa la CLI. È necessario abilitare l'accesso in ogni quarantena prima che un utente con questo ruolo possa gestirli.
Ruolo utente personalizzato	Gli account utente con un ruolo utente personalizzato possono accedere solo alle funzionalità di sicurezza e-mail assegnate al ruolo. Queste funzionalità possono essere costituite da qualsiasi combinazione di criteri di prevenzione della perdita dei dati, criteri di posta elettronica, report, quarantene, registrazione dei messaggi locali, profili di crittografia lo strumento di debug Trace. Gli utenti non possono accedere alle funzionalità di configurazione del sistema. Solo gli amministratori possono definire ruoli utente personalizzati. **Nota**: gli utenti assegnati a ruoli personalizzati non possono accedere alla CLI.

L'account utente predefinito del sistema, admin, dispone di tutti i privilegi amministrativi. L'account utente admin non può essere eliminato, ma è possibile modificare la password e bloccare l'account.

Sebbene non vi siano limiti al numero di account utente che è possibile creare nell'accessorio, non è possibile creare account utente con nomi riservati dal sistema. Ad esempio, non è possibile creare gli account utente denominati "operator" o "root".

Tutti i ruoli definiti in precedenza possono accedere sia alla GUI sia alla CLI, ad eccezione del ruolo utente dell'help desk e dei ruoli utente personalizzati, che possono accedere solo alla GUI.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems