Contenu

Introduction

Ce document décrit les divers niveaux d'accès administratif, ou a prédéfini les rôles de l'utilisateur, qui sont disponibles sur l'appliance de sécurité du courrier électronique (ESA).

Quels sont les niveaux de l'accès administratif disponibles sur l'ESA ?

Quand vous créez un nouveau compte utilisateur, vous affectez l'utilisateur à des prédéfinis ou à un rôle de l'utilisateur fait sur commande. Chaque rôle de l'utilisateur contient des différents niveaux des privilèges dans l'accès de SYSTÈME D'EXPLOITATION et d'appareils, comme suit :

Administrateurs	Les comptes utilisateurs avec le rôle administrateur ont l'accès complet à tous les paramètres de configuration du système. Cependant, seulement l'utilisateur d'admin a accès au **resetconfig** et **retourne des** commandes.
Opérateurs	Des comptes utilisateurs avec le rôle d'opérateur sont limités de : • Créant ou éditant des comptes utilisateurs. • Émettre la commande de **resetconfig**. • Évolution de l'appliance. • En émettant le **systemsetup** commandez ou exécuter l'assistant de configuration de système. • Émettre la commande d'**adminaccessconfig**. • Exécuter quelques fonctions de quarantaine (création y compris, éditer, supprimer, e quarantaines de centralisation). • Modifiant des paramètres de profil de serveur LDAP autres que le nom d'utilisateur e mot de passe, si le LDAP est activé pour l'authentification externe. Autrement, ils ont les mêmes privilèges que le rôle administrateur.
Opérateurs en lecture seule	Les comptes utilisateurs avec le rôle en lecture seule d'opérateur ont accès pour visualis les informations de configuration. Les utilisateurs avec le rôle en lecture seule d'opérateu peuvent apporter et soumettre des modifications pour voir comment configurer une caractéristique, mais ils ne peuvent pas les commettre. Les utilisateurs avec ce rôle peuvent gérer des messages dans les quarantaines, si l'accès est activé dans une quarantaine. Les utilisateurs avec ce rôle ne peuvent pas accéder à ce qui suit : • Système de fichiers, FTP, ou SCP. • Configurations pour la création, éditer, supprimer, ou les quarantaines de centralisation.
Invités	Les comptes d'utilisateurs avec le rôle d'invité peuvent seulement visualiser les informations d'état. Les utilisateurs avec le rôle d'invité peuvent également gérer des messages dans les quarantaines, si l'accès est activé dans une quarantaine. Les utilisateurs avec le rôle d'invité ne peuvent pas accéder au cheminement de message.
Technicien	Les comptes utilisateurs avec le rôle de technicien peuvent exécuter des mises à jour de système, redémarrer l'appliance, et gérer des touches de fonction. Les techniciens

Utilisateurs de centre d'assistance	peuvent également exécuter les actions suivantes afin d'améliorer l'appliance : • Interrompez la livraison et la réception d'email. • État de vue de workqueue et d'auditeurs. • Sauvegardez et envoyez les fichiers de configuration. • Sauvegardez les safelists et les blocklists. Les techniciens ne peuvent pas restaurer ces listes. • Démontez l'appliance d'une batterie. • Activez ou désactivez l'accès de service distant pour le support technique de Cisco. • Soulevez une demande de support. Des comptes utilisateurs avec le rôle de l'utilisateur de centre d'assistance sont limités à • Cheminement de message. • Gérer des messages dans les quarantaines. Les utilisateurs avec ce rôle ne peuvent pas accès au reste du système, y compris le CL Vous devez activer l'accès dans chaque quarantaine avant qu'un utilisateur avec ce rôle puisse les gérer.
Rôle de l'utilisateur fait sur commande	Les comptes utilisateurs avec un rôle de l'utilisateur fait sur commande peuvent seuleme accéder à des caractéristiques de sécurité du courrier électronique assignées au rôle. Ce caractéristiques peuvent être n'importe quelle combinaison des stratégies DLP, envoient des stratégies, des états, des quarantaines, le cheminement local de message, des profi de cryptage, et l'outil de débogage de suivi. Les utilisateurs ne peuvent pas accéder à de caractéristiques de configuration de système. Seulement les administrateurs peuvent définir des rôles de l'utilisateur faits sur commande. Remarque: Les utilisateurs assignés aux rôles faits sur commande ne peuvent pas accéder au CLI.

L'utilisateur par défaut expliquent le système, admin, a tous les privilèges d'administrateur. Le compte utilisateur d'admin ne peut pas être supprimé, mais vous pouvez changer le mot de passe et verrouiller le compte.

Bien qu'il n'y ait aucune limite au nombre de comptes utilisateurs que vous pouvez créer sur l'appliance, vous ne pouvez pas créer des comptes utilisateurs avec les noms qui sont réservés par le système. Par exemple, vous ne pouvez pas créer les comptes utilisateurs nommés « opérateur » ou « racine. »

Tous les rôles définis par ci-dessus peuvent accéder au GUI et le CLI, excepté les rôles de l'utilisateur de rôle de l'utilisateur et de coutume de centre d'assistance, qui peuvent seulement accéder au GUI.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems