Contenu

Introduction

Ce document donne les réponses aux questions fréquemment posées (FAQ) au sujet du système de contrôle d'accès sécurisé Cisco (ACS) versions 5.x et ultérieures.

Questions connexes d'authentification

Q. Quelques utilisateurs/groupes de la base de données interne ACS 5.x peuvent-ils être exclus de la stratégie de mot de passe utilisateur (administration système > utilisateurs > configurations d'authentification) ?

A. Par défaut, chaque utilisateur de base de données interne doit se conformer à la stratégie de mot de passe utilisateur. Actuellement, aucun utilisateur/groupe de la base de données interne ACS 5.x ne peut être exclu.

Q. Quelques administrateurs GUI d'ACS 5.x peuvent-ils être exclus de la stratégie administrative de mot de passe utilisateur (administration système > administrateurs > configurations > authentification) ?

A. Par défaut, chaque utilisateur administratif GUI doit se conformer à la stratégie administrative de mot de passe utilisateur. Actuellement, aucun utilisateur administratif d'ACS 5.x ne peut être exclu.

Q. ACS 5.x fournit-il le support pour des outils de VMware ?

A. Non. Actuellement, les outils de VMWare ne sont pas pris en charge avec la version 5.x ACS. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCtg50048 (enregistrés seulement

Q. Quels sont les protocoles d'authentification EAP pris en charge pour ACS 5.x quand le LDAP est configuré comme mémoire d'identité ?

A. Quand le LDAP est utilisé comme mémoire d'identité, ACS 5.2 prend en charge des protocoles PEAP-GTC, EAP-FAST-GTC, et d'EAP-TLS seulement. Il ne prend en charge pas l'EAP-FAST MSCHAPv2, PEAP EAP-MSCHAPv2, et EAP-MD5. Le pour en savoir plus, se rapportent à l'authentification Protocol et à la compatibilité de base de données utilisateur.

Q. Pourquoi a-t-elle fait l'authentification pour WLC avec le rayon d'utilisation sur l'échouer ACS, et pourquoi ACS n'a-t-il pas affiché des essais ratés ?

A. Une question existe avec l'**Interopérabilité ACS 5.0 et WLC** avant que le correctif 8 de téléchargement du correctif 4., et applique le correctif sur le CLI. N'employez pas le TFTP afin de réparer cette question.

Q. Pourquoi j'incapable de restaurer tar.gz suis- les fichiers qui ont été sauvegardés avec la commande de journal de sauvegarde dans ACS 5.2 ?

A. Vous ne pouvez pas restaurer les fichiers journal qui sont sauvegardés avec la commande de **journal de sauvegarde**. Vous pouvez restaurer seulement ces fichiers sauvegardés pour la configuration ACS et l'ADE-OS. Référez-vous à la **sauvegarde** et aux commandes de **journaux de sauvegarde** dans le guide de référence CLI pour le pour en savoir plus de Cisco Secure Access Control System 5.1.

Q. Est-ce que je peux limiter le nombre de tentatives infructueuses de mot de passe sur ACS 5.2 ?

A. Non. Cette caractéristique n'est pas disponible sur ACS 5.2, mais on s'attend à ce qu'elle soit intégrée dans ACS 5.3. Référez-vous à la section non prise en charge de caractéristiques des notes de mise à jour pour le pour en savoir plus du Système de contrôle d'accès sécurisé Cisco 5.2.

Q. Je ne peux pas utiliser l'option de changer le mot de passe à la prochaine procédure de connexion pour des utilisateurs internes dans ACS 5.0. Comment faire pour résoudre ce problème ?

A. L'option de changer le mot de passe à la prochaine procédure de connexion n'est pas prise en charge dans ACS 5.0. Le soutien de cette caractéristique est disponible dans ACS 5.1 et versions ultérieures.

Q. Que cette alarme sur ACS signifie-t-elle ?

A. Cette erreur signifie que quand la vue ACS atteint une limite de 250,000 sessions, elle jette une alarme pour supprimer 20,000 sessions. La base de données de vue ACS enregistre toutes les sessions précédentes d'authentification et quand il atteint 250,000, elle donne une alarme pour effacer le cache et pour supprimer 20,000 sessions.

Q. Comment fais je résolvez ce message d'erreur : **Échec de l'authentification : L'authentification de l'utilisateur 24407 contre le Répertoire actif a manqué puisque l'utilisateur est requis de changer son mot de passe** ?

A. Ce message d'erreur apparaît quand il y a un problème avec la gestion des mots de passe pendant l'authentification de SDI. ACS 5.x est utilisé pendant qu'un proxy RADIUS et les utilisateurs doivent être authentifiés par un serveur RSA. Le proxy RADIUS à la RSA fonctionnera seulement sans gestion des mots de passe. La raison est que la valeur OTP doit être réparable par le proxy de serveur de rayon la valeur du mot de passe au serveur RSA. Quand la gestion des mots de passe est activée dans le groupe de tunnel, la demande RADIUS est envoyée avec les attributs MS-CHAPv2. La RSA ne prend en charge pas le MS-0CHAPv2 ; il prend en charge seulement le PAP.

Afin de résoudre ce problème, gestion des mots de passe de débronchement. Le pour en savoir

plus, se rapportent à l'ID de bogue Cisco CSCsx47423 (enregistrés seulement

Q. Est-il possible de limiter l'admin ACS pour gérer seulement certains périphériques dans ACS 5.1 ?

A. Non, il n'est pas possible de limiter l'admin ACS pour gérer seulement certains périphériques dans ACS 5.1.

Q. ACS prend en charge-il QoS dans l'authentification de sorte que le RAYON puisse être donné la priorité au-dessus de TACACS ?

A. Non, ACS ne prend en charge pas QoS dans l'authentification. ACS ne donnera pas la priorité à des demandes d'authentification de RAYON au-dessus des demandes TACACS ou TACACS au-dessus du RAYON.

Q. Peuvent-ils le proxy TACACS ACS 5.x et les authentifications de RAYON à d'autres serveurs TACACS ou de RAYON ?

A. Oui, toutes les versions ACS 5.x mettent en boîte le proxy les authentifications de RAYON à d'autres serveurs de RAYON. ACS 5.3 et proxy postérieur de boîte les authentifications TACACS à d'autres serveurs TACACS.

Q. ACS 5.x peut-il vérifier les attributs d'accès distant d'un utilisateur de Répertoire actif afin d'accorder l'accès ?

A. Oui, dans ACS 5.3 et plus tard vous pouvez permettre, refuser, et contrôler l'accès des permissions d'accès commuté entrant d'un utilisateur. Les autorisations sont vérifiées pendant des authentifications ou les requêtes à partir du Répertoire actif. Il est placé sur le dictionnaire dédié par Répertoire actif.

Q. ACS 5.x prend en charge-il le CHAP ou l'authentification MSCHAP tape-elle pour TACACS+ ?

A. Oui, des types d'authentification de CHAP TACACS+ et MSCHAP sont pris en charge dans des versions 5.3 et ultérieures ACS.

Q. Est-ce que je peux placer le type de mot de passe d'un utilisateur interne ACS à une base de données externe ?

A. Oui, dans ACS 5.3 et plus tard vous pouvez placer le type de mot de passe d'un utilisateur interne ACS. Cette caractéristique était disponible dans ACS 4.x.

Q. Le réussite/échec I qu'une authentification a basé le temps à l'où l'utilisateur a été créé dans l'identité interne ACS peut-il enregistrent ?

A. Oui, dans ACS 5.3 et plus tard vous pouvez employer le **nombre d'heures puisqu'**attribut de **création d'utilisateur** afin de créer vos stratégies. Cet attribut contient le nombre d'heures puisque l'utilisateur a été créé dans la mémoire interne d'identité à la période de la demande

d'authentification en cours.

Q. Est-ce que je peux employer des masques afin d'ajouter une nouvelle entrée de hôte dans la base de données interne ACS ?

A. Oui, ACS 5.3 et plus tard te permet pour utiliser des masques quand vous ajoutez de nouveaux hôtes dans la mémoire interne d'identité. Il te permet également pour entrer dans des masques (après que vous présentez les trois premiers octets) afin de spécifier tous les périphériques du fabricant identifié.

Q. Est-ce que je peux configurer des groupes d'adresse IP sur l'ACS 5.x et les assigner d'ACS ?

A. Non, il n'est pas actuellement possible de créer des groupes d'adresse IP sur l'ACS 5.x.

Q. Est-ce que je peux voir l'adresse IP du client d'AAA où la demande a été livré dans l'état d'AUTHENTIFICATION DÉFAILLANTE ?

A. Non, il n'est pas possible de voir l'adresse IP du client d'AAA d'où la demande est entrée.

Q. Quelle est reprise de message de log de vue dans ACS 5.3 ?

A. ACS 5.3 fournit une nouvelle caractéristique pour récupérer tous les logs qui sont manqués quand la vue est en baisse. ACS collecte ces logs manqués et les enregistre dans sa base de données. Utilisant cette caractéristique, vous pouvez récupérer les logs manqués de la base de données ACS à la base de données de vue après que la vue soit sauvegardent. Afin d'utiliser cette caractéristique, vous devez placer la configuration de reprise de message de log à **en fonction**. Pour plus de détails sur configurer la reprise de message de log de vue, référez-vous à la surveillance et aux exploitations du système de visionneuse de rapports.

Q. Est-ce que je peux compresser la base de données ACS 5.x en émettant la commande de base de données-

A. Oui, dans ACS 5.3 et plus tard, la commande de base de données-**compresse** réduit la taille de la base de données ACS avec une option de supprimer les administrateurs de la transaction table.ACS ACS peut émettre cette commande afin de réduire la taille de la base de données. Ceci aide à réduire la taille de la base de données et le moment pris pour des sauvegardes et une pleine synchronisation qui est nécessaire pour la maintenance.

Q. Est-ce que je peux rechercher une entrée de client d'AAA basée sur son adresse IP ?

A. Oui, ACS 5.3 et plus tard te permet pour rechercher un périphérique de réseau utilisant son adresse IP. Vous pouvez également employer les masques et la plage afin de rechercher un ensemble spécifique de périphériques de réseau.

Q. Est-ce que je peux créer une condition basée sur le temps à l'où l'utilisateur a été créé dans la mémoire interne d'identité ACS ?

A. Oui, dans ACS 5.3 et plus tard vous pouvez utiliser le **nombre d'heures puisque l'**attribut de **création d'utilisateur** qui te permet de configurer les conditions de règle de stratégie, basé sur le temps à l'où l'utilisateur a été créé dans la mémoire interne d'identité ACS. Exemple : SI **group=HelpDesk&NumberofHoursSinceUserCreation>48** rejettent alors. Cet attribut contient le nombre d'heures puisque l'utilisateur a été créé dans la mémoire interne d'identité à la période de la demande d'authentification en cours.

Q. Est-ce que je peux signer que la mémoire d'identité l'utilisateur a été authentifié dans la section d'autorisation d'une stratégie de service ?

A. Oui, dans ACS 5.3 et plus tard vous pouvez utiliser l'attribut de **mémoire d'identité d'authentification**, qui te permet de configurer les conditions de règle de stratégie basés sur la mémoire d'identité d'authentification. Exemple : SI **AuthenticationIdentityStore=LDAP_NY** rejettent alors. Cet attribut contient le nom de la mémoire d'identité utilisée et il est mis à jour avec le nom approprié de mémoire d'identité après l'authentification réussie.

Q. Quand l'ACS va-il à la prochaine mémoire d'identité définie dans l'ordre de mémoire d'identité ?

A. L'ACS va à la prochaine mémoire d'identité définie dans l'ordre de mémoire d'identité dans ces scénarios :

- Un utilisateur n'est pas trouvé dans la première mémoire d'identité
- Une mémoire d'identité n'est pas disponible dans l'ordre

Q. Quelle est la stratégie de désactivation de compte dans ACS 5.3 ?

A. La stratégie de désactivation de compte te permet pour désactiver les utilisateurs de la mémoire interne d'identité quand la date configurée a lieu au delà de la date donnée, le nombre configuré de jours ont lieu au delà des jours donnés, ou le nombre de tentatives infructueuses consécutives de procédure de connexion dépasse le seuil. La valeur par défaut pour la date dépasse est à 30 jours de la date du jour. La valeur par défaut pendant des jours ne devrait pas être plus de 60 jours du jour en cours. La valeur par défaut pour des essais ratés est 5.

Q. Est-ce que je peux changer le mot de passe d'un utilisateur de base de données interne d'ACS au-dessus de telnet ?

A. Oui, on te permet pour changer le mot de passe d'un utilisateur de base de données interne utilisant TACACS+ au-dessus de telnet. Vous devez sélectionner le **Change Password de TELNET d'enable** sous le **contrôle de modification de mot de passe** sur ACS 5.x.

Q. Est-ce queexemple primaire ACS 5.x met à jour automatiquement les exemples de sauvegarde périodiquement, ou devrait il seulement se produire quand une configuration a changé ?

A. ACS 5.x répliquera immédiatement vers l'ACS secondaire toutes les fois que vous apportez des modifications sur l'ACS primaire. En outre, si vous n'apportez aucune modification à l'ACS primaire alors, il fera une réplication de force toutes les 15 minutes. En ce moment, il n'y a pas une option de contrôler le temporisateur de sorte qu'ACS puisse répliquer les informations après

une heure précise.

Q. Je peut-il visualise-t-il/exportation un état sur ACS 5.x de tous les utilisateurs qui sont actuellement ouverts une session et authentifiés d'ACS sur différents clients de NAS ?

A. Oui, c'est possible. Il y a deux états distincts pour le RAYON et le TACACS+. Vous pouvez les trouver sous la **surveillance et les états** > les **états** > le **catalogue** > le **répertoire de session** > les **sessions actives de RAYON** et les **sessions actives TACACS**. Les deux états sont basés sur l'information de comptabilité des clients de NAS puisqu'elle te permet de dépister quand l'utilisateur se connecte et se déconnecte. L'historique de session te permet même pour obtenir les informations dès le début et pour arrêter des messages pendant un jour spécifique.

Informations connexes

- Page de support de Système de contrôle d'accès sécurisé Cisco
- Support et documentation techniques - Cisco Systems