Méthodes CallManager approuvées pour l'accès au support technique distant Cisco

Contenu

Introduction

En plus des procédures d'Accès à distance répertoriées dans installer le système d'exploitation sur le serveur d'applications de Téléphonie sur IP de Cisco, ce document répertorie les méthodes utilisées par le support technique de Cisco pour accéder à des systèmes à distance. Ceci améliore considérablement la capacité de l'ingénieur de diagnostiquer et résoudre des problèmes de système. Bien qu'on ne l'exige pas, des clients sont fortement encouragés à fournir un certain genre d'accès pour dépannage des buts.

Il est de la responsabilité du client d'assurer n'importe quel logiciel exigé.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco CallManager 3.x(x) et plus tard
- Virtual Network Computing (VNC)
- Service de terminaux de Windows (WTS) (également appelé le bureau distant)
- Cisco MeetingPlace

WTS n'est pas fourni par Cisco.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Méthodes approuvées d'Accès à distance

Cisco CallManager

Pour des informations supplémentaires sur l'Accès à distance de Cisco CallManager, référez-vous à mai où j'utilise des services de terminaux, à VNC, ou à OIT sur ce serveur pendant le chapitre de mise à jour d'*installer le système d'exploitation sur le serveur d'applications de Téléphonie sur IP de Cisco, version 2000.2.6*.

VNC

Le VNC se transporte maintenant avec le Cisco CallManager installent le CD et sont pris en charge pour l'Accès à distance au Cisco CallManager. Pour plus d'informations sur le VNC, référez-vous au site de RealVNC .

Le VNC est la seule méthode prise en charge d'Accès à distance pour des installations et des mises à jour de logiciel.

Si vous voulez employer Virtual Network Computing (VNC) pour promouvoir à distance un serveur Cisco CallManager, référez-vous à la page de documentation de Système d'exploitation de téléphonie IP de Cisco pour obtenir la dernière version du document VNC.

Le pour en savoir plus, se rapportent à améliorer la version 4.1.2 de Cisco CallManager.

Attention : Si vous avez installé le VNC mais ne prévoyez pas de l'employer pour exécuter la mise à jour, désactivez-la pour empêcher l'Accès à distance au serveur. Si vous ne désactivez pas le VNC et un utilisateur/accès administrateur le serveur au moment de la mise à jour, la mise à jour échoue.

WTS (bureau distant)

Cisco installe des services de terminaux. Par conséquent, le support technique de Cisco peut effectuer des tâches d'administration à distance et de dépannage. Des services de terminaux de

Windows est pris en charge et préférés pour la gestion et l'accès de serveur distant pour le support technique de Cisco.

Limites WTS

L'installation ou les mises à jour du logiciel n'est pas prise en charge sur le Cisco CallManager.

Attention : Avant que la mise à jour, Cisco recommande que vous désactiviez des services de terminaux et redémarrez immédiatement le serveur pour empêcher l'Accès à distance au serveur. Si vous accédez au serveur par des services de terminaux, il fait parfois échouer la mise à jour.

Après que vous promouviez le serveur, vous devez activer des services de terminaux.

Pour plus d'informations sur WTS, référez-vous au site WTS de Microsoft .

Lumières intégrées (l'OIT)

N'employez pas l'OIT pour effectuer des tâches de mise à jour ou d'installation. Cisco prend en charge l'OIT pour des tâches de gestion à distance et de configuration seulement.

Pour plus d'informations sur l'OIT, référez-vous au sujet de l'OIT.

Cisco MeetingPlace

Le Cisco MeetingPlace est un seul outil utilisé par le Soutien technique pour des Conférences Web. Il permet l'accès aux systèmes par le HTTP. Tant que il y a d'accès Internet du serveur Cisco CallManager, c'est la méthode préférée.

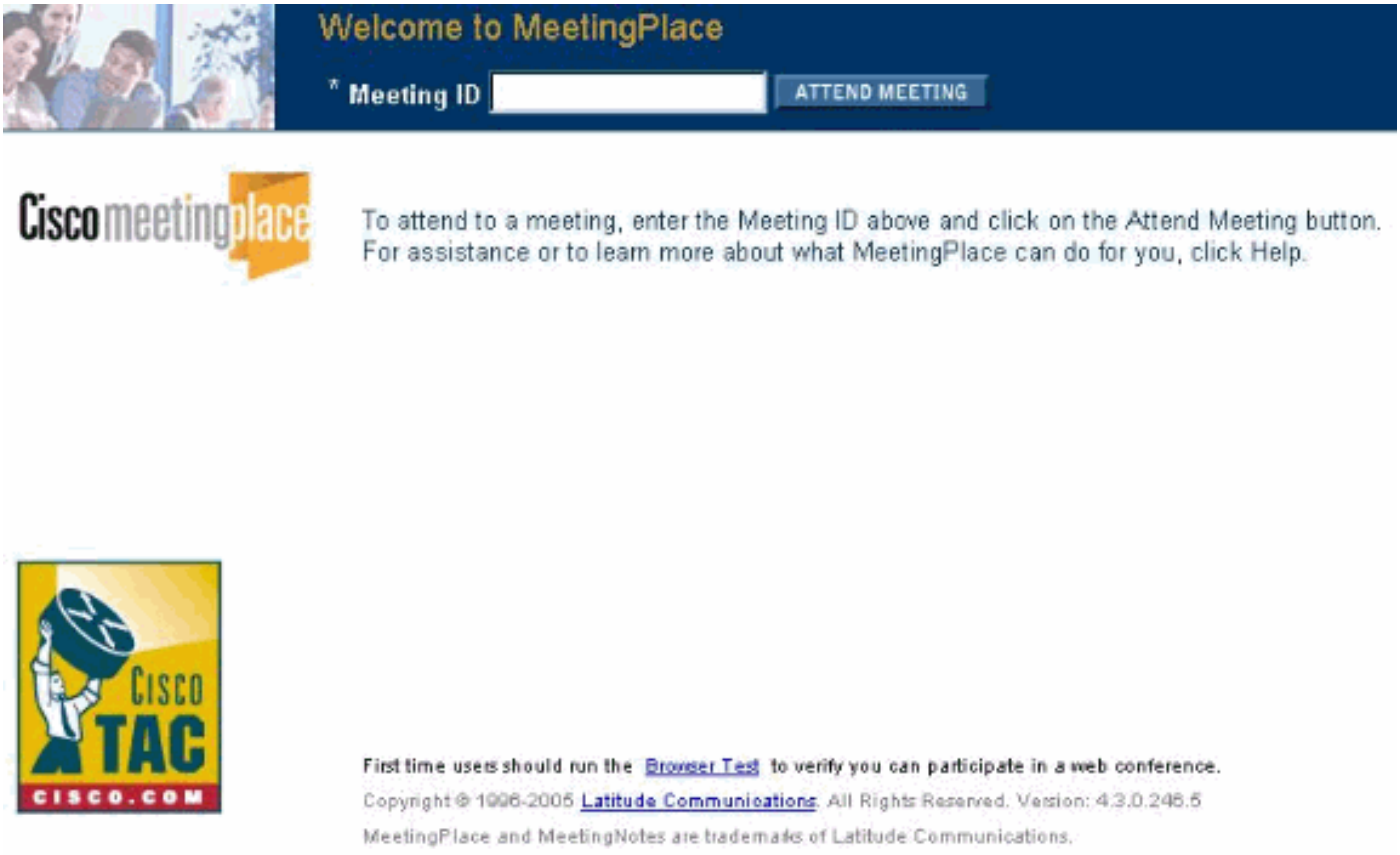
Remarque: Par défaut, l'Internet Explorer ouvre de nouveaux liens dans les fenêtres existantes. Par conséquent, vous pouvez facilement perdre votre téléconférence Web quand vous cliquez sur en fonction un lien. Pour empêcher ce comportement d'Internet Explorer, sélectionner des **outils > des options Internet > a avancé** et décoche des **fenêtres de réutilisation pour lancer des raccourcis**.

Ouvrez le port TCP 1627 afin de partager l'appareil de bureau. Si le port TCP 1627 est bloqué par le Pare-feu, des messages sont percés un tunnel par le port TCP 80. Le Cisco MeetingPlace prend en charge également le Tunnellisation utilisant HTTPS (SSL). Le SSL exige un certificat ssl. Pour activer le soutien du SSL, le port 443 doit être ouvert sur le réseau. Pour l'application de Conférences de l'information sur le Web, référez-vous à la téléconférence Web Cisco MeetingPlace.

Remarque: Quand vous initiez une session de service de terminaux au serveur Cisco CallManager, lancez un navigateur de là au Cisco MeetingPlace, partagez l'appareil de bureau, et puis réduisez cette session de service de terminaux, la téléconférence Web avec des gels de Soutien technique. Cisco recommande que vous partagiez l'appareil de bureau de votre ordinateur local, connexion au Cisco MeetingPlace de la console de serveur directement, ou ne réduisiez pas votre session de service de terminaux au Cisco CallManager.

Pour les informations produit supplémentaires, référez-vous au Cisco MeetingPlace.

Si vous devez installer une session avec un ingénieur de Soutien technique, allez à la page TAC MeetingPlace.



De cette page, introduisez le seul numéro d'ID se réunissant que l'ingénieur de Soutien technique assigne pour cette téléconférence. Si vous êtes un utilisateur de première fois, sélectionnez le lien de test de navigateur pour assurer la compatibilité. Si vous ne les avez pas déjà, la page de navigateur de test vous incite à installer des composants de quelques Javas. C'est un processus d'une fois. On ne l'exige pas la prochaine fois que vous vous connectez au Cisco MeetingPlace.

Une fois que vous vous connectez en tant qu'invité, vous pouvez partager n'importe quelle application avec l'ingénieur de Soutien technique et permettre le contrôle d'ingénieur.

Remarque: Quand vous utilisez le Cisco MeetingPlace pour des Conférences Web, le processus de navigateur Internet utilise une partie de ressources CPU. C'est comportement prévu.

Connexions de réseau sécurisé

Les clients sont responsables de la Connectivité de réseau sécurisé pour l'accès. Les connexions du réseau privé virtuel de Cisco (VPN) sont la méthode préférée.

Comment utiliser un VPN

Un VPN est un réseau privé qui utilise des lignes téléphoniques publiques (ou dans certains cas un modem câble). L'intimité est mise à jour par le cryptage et l'utilisation des protocoles sécurisés. Quand vous employez un VPN pour accéder au Cisco CallManager par un Pare-feu, vous pouvez utiliser le Cisco CallManager comme si vous étiez à l'intérieur du réseau.

Le VPN est exigé dans ces circonstances :

- Quand vous avez besoin de l'accès au site Web de Cisco CallManager (serveur CallManager name>/ccmadmin de <Cisco de http://) à partir d'un ordinateur distant en dehors de votre

pare-feu réseau.

Remarque: Si vous n'utilisez pas le VPN pour l'Accès à distance, référez-vous au site Web de Microsoft pour les informations sur configurer le modèle objet composant distribué (DCOM) par un Pare-feu.

Discutez l'installation d'un VPN avec votre administrateur de RÉSEAU LOCAL.

Informations connexes

- Assistance technique concernant la technologie vocale
- Support produit pour Voix et Communications IP
- Dépannage des problèmes de téléphonie IP Cisco
- Support technique - Cisco Systems