

Installation sur site de MeetingPlace Web avec DMZ

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Éléments à vérifier avant que vous alliez sur le site](#)

[Vérifiez la Connectivité](#)

[Cliquez sur pour assister à des considérations](#)

[Éléments à vérifier avant que vous commenciez le travail sur le site](#)

[Vérifiez la Connectivité](#)

[Valeur par défaut du groupe réglée dans MeetingTime](#)

[Installation de MeetingPlace Web](#)

[Éléments à vérifier après travail sur le site](#)

[Rassemblements publics de test](#)

[Téléconférences de test](#)

[Téléconférences magistrales de test](#)

[Vérification de Conférences Web et de notification](#)

[Informations connexes](#)

[Introduction](#)

Ce document trace les grandes lignes des procédures de vérification pour l'usage avant que vous alliez sur le site, ou avant que vous commencez le travail sur le site, et après que vous vous êtes terminé n'importe quel Cisco MeetingPlace Web avec le travail sur le site démilitarisé de la zone (DMZ).

[Conditions préalables](#)

[Conditions requises](#)

Confirmez-vous ont lu la [version 5.3 de notes en version de Cisco MeetingPlace Web](#) et les exigences sont répondues. Différentes conditions requises de modèle de déploiement, segmentées rencontrant le serveur Access-1 (SMA-1S) et segmentées rencontrant le serveur d'Access 2 (SMA-2S) sont trouvées aux pages six et sept du document de notes de mise à jour thr.

[Composants utilisés](#)

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

- Version 5.3 de Cisco MeetingPlace Web
- Architecture DMZ (DMZ-B et DMZ-C) — (ceux-ci désigné sous le nom de SMA-1S et de SMA-2S du [guide d'administrateur pour la version 5.3 de téléconférence Web Cisco MeetingPlace](#) — installation et configuration.)

[Conventions](#)

Pour plus d'informations sur les conventions de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

[Éléments à vérifier avant que vous alliez sur le site](#)

Cette section trace les grandes lignes des étapes de vérification nécessaires avant que vous alliez sur le site.

[Vérifiez la Connectivité](#)

Procédez comme suit :

1. Passez en revue le chapitre 5 du [guide d'administrateur pour la version 5.3 de téléconférence Web Cisco MeetingPlace](#) concernant la façon configurer des Conférences de Web externe, avec l'installation de Protocole SSL (Secure Socket Layer).
2. Vérifiez que le port 80 ou le port 443 (protocole SSL) est ouvert de l'Internet et de serveur DMZ.
3. Vérifiez que le port 80 est ouvert de l'intranet et d'Internet.
4. Vérifiez que le port 5003 est ouvert entre le serveur DMZ et le serveur Cisco MeetingPlace (le module d'intégrité de système de passerelle de Cisco MeetingPlace [GWSIM] utilise ceci).Initié du serveur DMZ à l'intranet
5. Pour WebShare, veillez-vous pour avoir le port 1627 ouvert de l'Internet et de serveur DMZ si vous voulez éviter le perçage d'un tunnel.Initié de l'Internet au serveur DMZSi ce port n'est pas ouvert, alors le Tunnellisation par le port 80 ou 443 est utilisé, qui est dix pour cent plus lent.
6. Pour WebShare, assurez-vous que vous avez le port 1627 ouvert de l'intranet et de serveur DMZ si vous voulez éviter le perçage d'un tunnel.Initié de l'intranet au serveur DMZSi ce port n'est pas ouvert, alors le Tunnellisation par le port 80 ou 443 est utilisé, qui est dix pour cent plus lent.
7. Pour NetMeeting seulement, vérifiez que vous avez le port 1503 ouvert de l'Internet et de serveur DMZ.Initié de l'Internet au serveur DMZ
8. Pour NetMeeting seulement, vérifiez que vous avez le port 1503 ouvert de l'intranet et de serveur DMZ.Initié de l'intranet au serveur DMZ

[Cliquez sur pour assister à des considérations](#)

Considérez ces facteurs :

1. (Ou séparer) un Système de noms de domaine (DNS) segmenté peut-il être utilisé ? Ceci te permet pour utiliser un URL simple dans vos notifications.
2. Sinon, vous devez décider comment modifier les modèles de notification :Prévoyez-vous d'utiliser deux URLs ?Prévoyez-vous d'utiliser un autre URL basé en fonction si la téléconférence est publique ou privée ?
3. Confirmez si vous avez un pilote des utilisateurs finaux pour tester la fonctionnalité après l'installer ou la mise à jour.
4. Est-ce que vous utilisez ou prévoyez d'utiliser le NT Authentication ?

Éléments à vérifier avant que vous commenciez le travail sur le site

Vérifiez la Connectivité

Procédez comme suit :

1. Ping et NSLOOKUP (si ouvert) le nom de domaine complet (FQDN) ou adresse IP du serveur Web interne d'un autre PC interne.Ping meetingplace.company.com (remplacez par l'adresse Internet correcte du serveur)NSLOOKUP meetingplace.company.com (remplacez par l'adresse Internet correcte du serveur)**Remarque:** Pour utiliser NSLOOKUP, ouvrir une invite DOS (allez au **Start > Run**, écrivez le **cmd** et cliquez sur OK), puis pour écrire **NSLOOKUP meetingplace.company.com** (remplacez par l'adresse Internet correcte du serveur).
2. Ping et NSLOOKUP (si ouvert) le FQDN ou l'adresse IP du serveur Web DMZ d'un PC externe.
3. Ping et NSLOOKUP (si ouvert) le FQDN ou l'adresse IP du serveur Web DMZ d'un autre PC interne.
4. Ping et NSLOOKUP (si ouvert) le FQDN ou l'adresse IP du MeetingPlace Server du serveur Web DMZ.
5. Telnet sur le port 5003 du serveur Web DMZ au serveur Cisco MeetingPlace. Suivez ces étapes pour confirmer que le port est ouvert :Allez au **Start > Run** et sélectionnez la commande du *servername* **5003 de telnet**, où le *servername* est le nom ou l'adresse IP du MeetingPlace Server, et cliquez sur OK.Si vous voyez une gamme de caractères absurdes (par exemple, ☺♥, ☹/v(\ ? ¶ (\ ? le ÿϕ), le port 5003 est ouvert.Entrez dans le **Ctrl-]** (contrôle, crochet de droite) pour quitter.Si vous obtenez une connexion défectueuse, comme affiché ici, alors le port 5003 n'est pas ouvert :`Could not open connection to the host, on port 5003: Connection failed`

Valeur par défaut du groupe réglée dans MeetingTime

Quels sont les types les plus communs de téléconférences réservées ?

Remarque: Si les téléconférences réservées sont en grande partie internes, placez l'affichage de valeur par défaut du groupe rencontrant à chacun la caractéristique à **non**. S'ils sont en grande partie des rassemblements publics, alors placez l'affichage se réunissant à chacun à **oui**.

Installation de MeetingPlace Web

Terminez-vous ces étapes (ces étapes varient basé en fonction si elles s'appliquent à un déploiement un ou de deux-serveur) :

1. Vérifiez le matériel et les logiciels nécessaires pour les serveurs. Veillez que le matériel sur l'ordinateur de passerelle répond à toutes les exigences appropriées. L'ordinateur qui héberge plus de conférences doit avoir le matériel plus rapide et meilleur.
2. Pour le déploiement SMA-1S, suivez les étapes pour l'implémentation dans le tableau 5-1, et pour l'accès segmenté de téléconférence pour le déploiement de serveur 2, se rapportent au tableau 5-2 du [guide d'administrateur pour la version 5.3 de téléconférence Web Cisco MeetingPlace](#).

Éléments à vérifier après travail sur le site

Rassemblements publics de test

Vérifiez ces éléments :

1. Vérifiez ces capacités : Employez le site Web interne pour ouvrir une session en tant qu'utilisateur à profil. Pour prévoir un rassemblement public, utilisez le site Web interne. Pour prévoir un rassemblement public avec une connexion, utilisez le site Web interne. Vous pouvez visualiser des connexions d'un PC interne. Vous recevez les notifications pour la téléconférence ci-dessus. Le clic pour assister à des travaux de lien intérieurement. Le clic pour assister à des travaux de lien d'un PC d'Internet. Interne et les visualiseurs externes peut joindre la téléconférence Web, aussi bien que le partage et collaborer à la même téléconférence Web.
2. Confirmez ces capacités et restrictions sur le site externe : Vous êtes ouvert une session en tant que votre profil quand vous vous occupez du site interne. Vous pouvez accéder aux connexions et le diaporama du serveur externe. Les invités ne peuvent pas ajouter des connexions ou changer des autorisations ou des options d'affichage d'utilisateur.

Remarque: Si la salle de téléconférence semble être gelée à un pour cent ou si les caractéristiques de salle de téléconférence sont grisées, l'adresse Internet peut être entrée inexactement ou le modèle DMZ n'est pas actuellement utilisé pour la téléconférence externe réorientent.

Téléconférences de test

Terminez-vous ces étapes de vérification.

1. Vérifiez ces capacités : Vous pouvez prévoir une téléconférence privée du site Web interne. Vous pouvez visualiser cette téléconférence privée d'un PC interne. Vous pouvez prévoir une téléconférence privée avec une connexion du site Web interne. Vous pouvez visualiser des connexions d'un PC interne. Vous recevez les notifications pour la téléconférence ci-dessus. Le clic pour assister à des travaux de lien intérieurement. Les visualiseurs internes peuvent joindre la téléconférence Web.
2. Vérifiez ces restrictions : Vous ne pouvez pas assister à une téléconférence privée du site Web DMZ. Vous n'êtes pas réorienté au site Web DMZ quand vous joignez la téléconférence

Web.

Téléconférences magistrales de test

Terminez-vous ces étapes de vérification.

1. Vérifiez ces capacités :Vous pouvez prévoir une téléconférence magistrale publique et privée de l'intranet.Un utilisateur à profil peut héberger une téléconférence magistrale de l'intranet et de l'Internet.On permet à un un utilisateur à profil pour collaborer de l'intranet et de l'Internet.
2. Vérifiez ces restrictions d'invité :Un invité ne peut pas héberger une téléconférence magistrale de l'intranet.Un invité ne peut pas héberger une téléconférence magistrale de l'Internet.On ne permet pas à un un invité pour collaborer de l'intranet.On ne permet pas à un un invité pour collaborer de l'Internet.

Vérification de Conférences Web et de notification

Terminez-vous ces étapes de vérification.

1. Pour vérifier le Tunnellisation si le port 1627 n'est pas ouvert :Procédure de connexion à l'interface utilisateur d'admin de Web (UI).Procédure de connexion au **Cisco MeetingPlace Web**.Le lien d'**admin** est à l'en haut à droite de l'écran de bienvenue.Cliquez sur le lien de **serveur de téléconférences de données**.Cliquez sur le lien **avancé**.Cochez le **HTTP de force perçant un tunnel** la case.Cliquez sur le bouton de **téléconférence Web de joindre**.Si le client de WebShare s'ouvre (le « accueil à l'application de MeetingPlace Sharing."), perçant un tunnel est fonctionnel.Si le client de WebShare ne s'ouvre pas, le perçage d'un tunnel n'est pas fonctionnel. Vous devriez [entrer en contact avec le support technique de Cisco](#).
2. Vérifiez que la notification est envoyée correctement et que le clic pour assister à des travaux de lien.

Informations connexes

- [Le guide du gestionnaire de système de téléconférence Web Cisco MeetingPlace](#)
- [Assistance technique concernant la technologie vocale](#)
- [Assistance concernant les produits vocaux et de communications unifiées](#)
- [Dépannage des problèmes de téléphonie IP Cisco](#)
- [Support et documentation techniques - Cisco Systems](#)