

Web MeetingPlace con la Instalación en el sitio DMZ

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Elementos a verificar antes de que usted vaya Onsite](#)

[Verifique la Conectividad](#)

[Haga clic para asistir a las consideraciones](#)

[Elementos a verificar antes de que usted comience el trabajo onsite](#)

[Verifique la Conectividad](#)

[Agrupe el conjunto predeterminado en el MeetingTime](#)

[Instalación del Web MeetingPlace](#)

[Elementos a verificar después del trabajo onsite](#)

[Pruebe las reuniones públicas](#)

[Pruebe las reuniones](#)

[Pruebe a las reuniones estilo conferencia](#)

[Conferencias web y verificación de notificación](#)

[Información Relacionada](#)

Introducción

Este documento delinea los procedimientos de verificación para el uso antes de que usted vaya onsite, o antes de que usted comienza el trabajo onsite, y después de que usted ha completado cualquier Web MeetingPlace de Cisco con el trabajo onsite de la zona desmilitarizada (DMZ).

prerrequisitos

Requisitos

Confirmele han leído la [versión 5.3 de los Release Note del Web MeetingPlace de Cisco](#) y se cumplen los requisitos. Diversos requisitos del modelo de despliegue, divididos en segmentos resolviendo el servidor Access-1 (SMA-1S) y divididos en segmentos resolviendo el servidor Access-2 (SMA-2S) se encuentran en las páginas seis y siete del documento de los Release Note thr.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión MeetingPlace Web de Cisco 5.3
- Arquitectura DMZ (DMZ-B y DMZ-C) — (éstos se refieren como SMA-1S y SMA-2S en la [guía de administrador para la versión 5.3 del MeetingPlace Web conferencing de Cisco para conferencias](#). — configuración y configuración.)

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

Elementos a verificar antes de que usted vaya Onsite

Esta sección delinea los pasos de verificación necesarios antes de que usted vaya onsite.

Verifique la Conectividad

Complete estos pasos:

1. Revise el capítulo 5 en la [guía de administrador para la versión 5.3 del MeetingPlace Web conferencing de Cisco para conferencias](#), que mira cómo configurar la Conferencia del Web externa, junto con la configuración del Secure Socket Layer (SSL).
2. Verifique que el puerto 80 o el puerto 443 (Protocolo SSL) esté abierto de Internet y al servidor DMZ.
3. Verifique que el puerto 80 esté abierto del intranet y a Internet.
4. Verifique que el puerto 5003 esté abierto entre el servidor DMZ y el servidor MeetingPlace de Cisco (MeetingPlace Gateway de Cisco el [GWSIM] del módulo de la integridad del sistema utiliza esto).Iniciado del servidor DMZ al intranet
5. Para el WebShare, asegúrese de tener el puerto 1627 abierto de Internet y al servidor DMZ si usted quiere evitar hacer un túnel.Iniciado de Internet al servidor DMZSi este puerto no está abierto, después el Tunelización a través del puerto 80 o 443 se utiliza, que es el diez por ciento más lento.
6. Para el WebShare, asegúrese de que usted tiene el puerto 1627 abierto del intranet y al servidor DMZ si usted quiere evitar hacer un túnel.Iniciado del intranet al servidor DMZSi este puerto no está abierto, después el Tunelización a través del puerto 80 o 443 se utiliza, que es el diez por ciento más lento.
7. Para el NetMeeting solamente, verifique que usted tenga el puerto 1503 abierto de Internet y al servidor DMZ.Iniciado de Internet al servidor DMZ
8. Para el NetMeeting solamente, verifique que usted tenga el puerto 1503 abierto del intranet y al servidor DMZ.Iniciado del intranet al servidor DMZ

Haga clic para asistir a las consideraciones

Considere estos factores:

1. ¿Puede (o partir) un Domain Name System (DNS) dividido en segmentos ser utilizado? Esto

permite que usted utilice un solo URL en sus notificaciones.

2. Si no, usted debe decidir cómo modificar las plantillas de notificación: ¿Usted planea utilizar dos URL? ¿Usted planea utilizar un diverso URL basado encendido si la reunión es pública o privada?
3. Confirme si usted tiene un piloto de los usuarios finales para probar las funciones después del instalar o de la actualización.
4. ¿Usted utiliza o planea utilizar NT Authentication?

Elementos a verificar antes de que usted comience el trabajo onsite

Verifique la Conectividad

Complete estos pasos:

1. Ping y NSLOOKUP (si está abierto) el nombre de dominio completo (FQDN) o la dirección IP del servidor de Web interno de otro PC interno. Ping meetingplace.company.com (substituya por el nombre de host correcto del servidor) NSLOOKUP meetingplace.company.com (substituya por el nombre de host correcto del servidor) **Nota:** Para utilizar NSLOOKUP, abrir un prompt DOS (vaya al **Start (Inicio) > Run (Ejecutar)**, ingrese el **cmd** y haga clic la **AUTORIZACIÓN**), después para ingresar **NSLOOKUP meetingplace.company.com** (substituya por el nombre de host correcto del servidor).
2. Ping y NSLOOKUP (si está abierto) el FQDN o la dirección IP del servidor Web DMZ de un externo PC.
3. Ping y NSLOOKUP (si está abierto) el FQDN o la dirección IP del servidor Web DMZ de otro PC interno.
4. Ping y NSLOOKUP (si está abierto) el FQDN o la dirección IP del servidor MeetingPlace del servidor Web DMZ.
5. Telnet en el puerto 5003 del servidor Web DMZ al servidor MeetingPlace de Cisco. Siga los siguientes pasos para confirmar que el puerto está abierto: Vaya al **Start (Inicio) > Run (Ejecutar)** y ingrese el **comando telnet servername 5003**, donde está el nombre o el IP Address el *servername* del servidor MeetingPlace, y haga clic la **AUTORIZACIÓN**. ¿Si usted ve una série de caracteres no sensibles (por ejemplo, ☺☻♥, ☹☺/v [\? ¿☻ [\? el ÿç), el puerto 5003 está abierto. Ingrese el **Ctrl-]** (control, corchete derecho) para salir. Si usted consigue una falla de conexión, como se muestra aquí, después el puerto 5003 no está abierto:

```
Could not open connection to the host, on port 5003: Connection failed
```

Agrupe el conjunto predeterminado en el MeetingTime

¿Cuáles son la mayoría de los tipos comunes de reuniones programadas?

Nota: Si las reuniones programadas son sobre todo internas, fije la visualización del valor por defecto del grupo que resuelve todo el mundo la característica a **no**. Si son sobre todo reuniones públicas, después fije la visualización que se encuentra todo el mundo a **sí**.

Instalación del Web MeetingPlace

Complete estos pasos (estos pasos varían basado encendido si se aplican a un despliegue uno o del dos-servidor):

1. Verifique los requisitos de hardware y de software para los servidores. Se asegura que el hardware en la máquina gateway cumple todos los requisitos apropiados. La máquina que recibe más conferencias debe tener el hardware más rápido, mejor.
2. Para el despliegue del SMA-1S, siga los pasos para la implementación en el cuadro 5-1, y para el acceso dividido en segmentos de la reunión para 2 instrumentación del servidor, refieren al cuadro 5-2 en la [guía de administrador para la versión 5.3 del MeetingPlace Web conferencing de Cisco para conferencias](#).

Elementos a verificar después del trabajo onsite

Pruebe las reuniones públicas

Verifique estos elementos:

1. Verifique estas capacidades: Utilice el sitio web interno para iniciar sesión como usuario perfilado. Para programar una reunión pública, utilice el sitio web interno. Para programar una reunión pública con una conexión, utilice el sitio web interno. Usted puede ver las conexiones de un PC interno. Usted recibe las notificaciones para la reunión antedicha. El tecleo para asistir a los trabajos del link internamente. El tecleo para asistir a los trabajos del link de Internet PC. Interno y los visores externos puede unirse a la conferencia en la wWeb., así como la parte y colaborar en la misma conferencia en la wWeb.
2. Confirme estas capacidades y restricciones en el sitio externo: Le abren una sesión como su perfil cuando usted asiste del sitio interno. Usted puede acceder las conexiones y a la presentación de diapositivas del servidor externo. Los invitados no pueden agregar las conexiones o cambiar los permisos o las opciones de visualización de usuario.

Nota: Si la Sala de reuniones aparece ser congelada en el un por ciento o si las características de la Sala de reuniones son grayed hacia fuera, el nombre de host puede ser entrado incorrectamente o la plantilla DMZ no se utiliza actualmente para la reunión externa reorienta.

Pruebe las reuniones

Complete estos pasos de verificación.

1. Verifique estas capacidades: Usted puede programar una reunión privada del sitio web interno. Usted puede ver esta reunión privada de un PC interno. Usted puede programar una reunión privada con una conexión del sitio web interno. Usted puede ver las conexiones de un PC interno. Usted recibe las notificaciones para la reunión antedicha. El tecleo para asistir a los trabajos del link internamente. Los espectadores internos pueden unirse a la conferencia en la wWeb.
2. Verifique estas restricciones: Usted no puede asistir a una reunión privada del sitio web DMZ. Le no reorientan al sitio web DMZ cuando usted se une a la conferencia en la wWeb.

Pruebe a las reuniones estilo conferencia

Complete estos pasos de verificación.

1. Verifique estas capacidades: Usted puede programar a una reunión estilo conferencia pública y privada del intranet. Un usuario perfilado puede reunión estilo conferencia del host A del intranet y de Internet. Se permite a un usuario perfilado colaborar del intranet y de Internet.
2. Verifique estas restricciones para invitados: Un invitado no puede reunión estilo conferencia del host A del intranet. Un invitado no puede reunión estilo conferencia del host A de Internet. No se permite a un invitado colaborar del intranet. No se permite a un invitado colaborar de Internet.

Conferencias web y verificación de notificación

Complete estos pasos de verificación.

1. Para verificar el Tunelización si el puerto 1627 no está abierto: Login a la interfaz de usuario del administrador Web (UI). Login al **Web MeetingPlace de Cisco**. El link **Admin** está en la esquina superior derecha de la página de Bienvenida. Haga clic el link del **servidor de la conferencia de datos**. Haga clic el link **avanzado**. Marque el cuadro del **Tunelización de la fuerza HTTP**. Haga clic el botón de la **conferencia en la wWeb. del unido**. Si el cliente WebShare se abre (la "recepción a la Aplicación MeetingPlace Sharing."), haciendo un túnel es funcional. Si el cliente WebShare no se abre, el hacer un túnel no es funcional. Usted debe [entrar en contacto el Soporte técnico de Cisco](#).
2. Verifique que la notificación esté enviada correctamente y que el tecleo para asistir a los trabajos del link.

Información Relacionada

- [Sistema de conferencia Web MeetingPlace de Cisco la guía del administrador](#)
- [Soporte de tecnología de voz](#)
- [Soporte de Productos de Voice and Unified Communications](#)
- [Troubleshooting de Cisco IP Telephony](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)