Versie 2.0 van de Cisco WebEx Meetings Server-beheerhandleiding

Eerste publicatie: 6 februari 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.

INHOUD

Installatiehandleiding van Cisco WebEx-vergaderingsserver 1

VMware vSphere gebruiken met uw systeem 3

VMware vSphere gebruiken 3

De ESXi-host configureren om een NTP-server te gebruiken 4

Een back-up maken met VMware vCenter 4

Een momentopname maken met VMware vCenter 5

Een bestaand VMDK-bestand aan een nieuwe virtuele machine koppelen 6

Netwerkcontrolelijst voor uw systeem 9

Controlelijst netwerken voor een systeem met publieke toegang en zonder split-horizon DNS 9

Controlelijst netwerken voor een systeem met publieke toegang en split-horizon DNS 10

Controlelijst netwerken voor een systeem zonder openbare toegang 10

Uw systeem installeren met automatische implementatie 11

Algemene concepten voor de implementatie van uw systeem 12

Installatiechecklist 13

Vereiste gegevens voor een automatische implementatie 14

Het OVA-bestand van de VMware vSphere-client implementeren 16

Uw netwerkconfiguratie controleren na een mislukte OVA-implementatie 28

Uw taal voor installatie selecteren 28

De implementatie bevestigen 29

De grootte van uw systeem bevestigen 29

Kiezen welk systeem u moet installeren 29

Het type systeemimplementatie kiezen 30

VMware vCenter-gebruikersgegevens opgeven 30

vCenter-instellingen voor uw virtuele mediamachine selecteren 31

Netwerkinformatie voor de virtuele mediamachine invoeren 31

Openbare toegang toevoegen 32

vCenter-instellingen voor uw Reverse Proxy kiezen 32

De netwerkinformatie voor de Reverse Proxy-virtuele machine invoeren 33

Het openbare VIP-adres invoeren 33
Het privé-VIP-adres invoeren 34
URL's van WebEx-site en WebEx-beheer 34
De URL's van de WebEx-site en –Beheer invoeren 36
Bevestigen dat uw netwerk op de juiste manier is geconfigureerd 36
Uw virtuele machines implementeren 36
Uw systeem controleren 37
Uw systeem installeren met handmatige implementatie 39
Algemene concepten voor de implementatie van uw systeem 39
Installatiechecklist 40
Vereiste gegevens voor een handmatige implementatie 41
Het OVA-bestand van de VMware vSphere-client implementeren 43
Uw netwerkconfiguratie controleren na een mislukte OVA-implementatie 55
Uw taal voor installatie selecteren 55
De implementatie bevestigen 56
De grootte van uw systeem bevestigen 56
Kiezen welk systeem u moet installeren 56
Het type systeemimplementatie kiezen 57
Openbare toegang toevoegen 57
Het openbare VIP-adres invoeren 58
Het privé-VIP-adres invoeren 58
URL's van WebEx-site en WebEx-beheer 59
De URL's van de WebEx-site en –Beheer invoeren 60
Bevestigen dat uw netwerk op de juiste manier is geconfigureerd 61
Uw virtuele machines implementeren 61
Uw systeem controleren 62
Uw mailserver, tijdzone en landinstellingen configureren 65
De mailserver voor uw systeem instellen 65
De tijdzone en landinstelling voor het systeem instellen 66
De mailserver, tijdzone en landinstellingen bevestigen 66
Het eerste beheerdersaccount voor uw systeem instellen 66
Het systeem testen 67
Het systeem na de installatie wijzigen 69
Hoge beschikbaarheid toevoegen, bijwerken, upgraden of het systeem uitbreiden. 69
Voorbereiden op een systeemwijzigende procedure 70

Een systeem met hoge beschikbaarheid toevoegen 73
Een systeem met hoge beschikbaarheid toevoegen met automatische implementatie 73
Een systeem met hoge beschikbaarheid toevoegen met handmatige implementatie 76
Bevestigen dat uw primair systeem en uw HA-systeem dezelfde versie hebben 78
Een systeem met hoge beschikbaarheid toevoegen 79
Het systeem testen 80
Uw systeem uitbreiden naar een groter systeemformaat 83
Voorbereiden op systeemuitbreiding 83
Voorbereiden op een systeemwijzigende procedure 84
Het systeem uitbreiden met automatische implementatie 85
Het systeem uitbreiden met handmatige implementatie 89
Het systeem testen 94
Het systeem bijwerken 95
Het systeem bijwerken 95
Verbinding maken met een ISO-image op het cd/dvd-station 96
Verdergaan met de updateprocedure 97
De update voltooien 98
Het systeem bijwerken 101
Een upgrade voorbereiden 101
Het systeem automatisch upgraden 102
Het systeem handmatig upgraden 105
Het systeem testen 107
Licenties opnieuw configureren en upgraden 108
Het GLO-aanvraagformulier openen 108
Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding 108
Een licentieverzoek opslaan 109
Licenties registreren die opnieuw moeten worden geconfigureerd 109
Licenties upgraden na een software-upgrade 110
Configuratiehandleiding van Cisco WebEx Meetings Server 113
Uw dashboard gebruiken 115
Informatie over uw dashboard 115
Alarmen weergeven en bewerken 117
Uw Geschiedenis hulpmiddelen weergeven 119
Het diagram Actieve vergaderingen gebruiken om vergaderingsproblemen te verhelpen 120

Trends vergadering weergeven 121
De lijst Vergaderingen weergeven 122
Een onderhoudsperiode plannen 123
Een geplande onderhoudsperiode wijzigen 124
Over de onderhoudsmodus 125
De onderhoudsmodus in- of uitschakelen 128
Gebruikers beheren 131
Over het beheren van gebruikers 131
Over door komma's en tabs gescheiden bestanden 132
Veldwaarden CSV-bestand 134
gebruikers toevoegen 138
Gebruikers bewerken 138
Gebruikers activeren 139
Gebruikers deactiveren 139
Gebruikers via Importeren deactiveren 140
Gebruikers importeren 140
Gebruikers exporteren 141
Gebruikers importeren naar een nieuw systeem met een geëxporteerd bestand 141
Traceercodes configureren 142
Traceercodes bewerken 143
Directory-integratie configureren 144
Gebruikersgroepen synchroniseren 148
CUCM gebruiken om AXL Web Service en directorysynchronisatie te configureren 149
CUCM gebruiken om de LDAP-integratie en -verificatie te configureren 150
Gebruikers e-mailen 150
Uw systeem configureren 153
Systeemeigenschappen configureren 153
De instellingen van uw virtuele machine aanpassen 153
Een systeem met hoge beschikbaarheid configureren 154
Een systeem met hoge beschikbaarheid toevoegen 154
Systeem met hoge beschikbaarheid verwijderen 156
Systeemgedrag na componentstoringen 156
Uw virtuele IP-adres wijzigen 158
Openbare toegang configureren 158
Openbare toegang aan uw systeem toevoegen 158

Openbare toegang uitschakelen 160
Het systeem vergroten 160
Algemene instellingen configureren 161
Uw site-instellingen wijzigen 161
Uw beheerinstellingen wijzigen 162
Servers configureren 163
Een mailserver configureren 163
Een SMTP-server configureren 164
Een opslagserver configureren 164
De noodherstelfunctie gebruiken 166
Uw SNMP-instellingen configureren 169
Communityreeksen configureren 169
Communityreeksen toevoegen 169
Communityreeksen bewerken 170
USM-gebruikers configureren 171
USM-gebruikers toevoegen 171
USM-gebruiker bewerken 173
Meldingsdoelen configureren 174
Doel voor meldingen bewerken 175
Meldingsdoelen configureren 175
Licenties beheren 176
Over licenties 176
Licenties uitvoeren met License Manager 183
Licenties uitvoeren met eFulfilment 184
Licenties uitvoeren door contact op te nemen met de technische ondersteuning 186
Instellingen configureren 187
Uw bedrijfsgegevens configureren 188
Uw brandinginstellingen configureren 189
Een bedrijfslogo verwijderen 190
Uw vergaderinstellingen configureren 190
Over vergaderingsbeveiliging 191
Over het configureren van uw audio-instellingen 192
Uw audio-instellingen voor de eerste keer configureren 193
Uw audio-instellingen configureren 195
Uw video-instellingen configureren 197

Uw mobiele instellingen configureren 197
Servicekwaliteit (Quality of Service – QoS) configureren 198
Over QoS-markering 199
Wachtwoorden configureren 200
Uw algemene wachtwoordinstellingen configureren 200
Uw gebruikerswachtwoordinstellingen configureren 201
Uw vergaderwachtwoorden configureren 202
Uw e-mailinstellingen configureren 204
Over e-mailsjablonen 204
Uw downloadinstellingen configureren 224
Over downloads 225
Certificaten beheren 226
SSL-certificaten genereren 227
Een CSR maken (Ondertekeningsaanvraag certificaat) 227
Een SSL-certificaat importeren 228
Een SSL-certificaat exporteren 229
Een SSL-certificaat voor mobiele apparaten exporteren 230
Uw CSR en private code downloaden 231
Een zelfondertekend certificaat genereren 231
Een SSL-certificaat herstellen 232
SSO IdP-certificaten importeren 234
Certificaten voor beveiligde teleconferenties importeren 234
Veiligheid gebruikerssessie configureren 235
Gefedereerd eenmalig aanmelden (SSO) configureren 236
SSO uitschakelen 239
Uw Cloud-functies configureren 240
Beveiliging van de virtuele machine configureren 240
Uw encryptiesleutels bijwerken 240
Over FIPS 241
FIPS-compatibele codering inschakelen 242
FIPS-compatibele codering uitschakelen 242
Uw rapporten beheren 243
Maandelijkse rapporten downloaden 243
Over maandelijkse rapporten 244
Aangepaste gegevensrapporten genereren 246

Informatie over aangepaste gegevensrapporten 246

De ondersteuningsfuncties gebruiken 251

Uw logboek aanpassen 251

Een account voor Remote Support instellen 253

Een account voor Remote Support uitschakelen 253

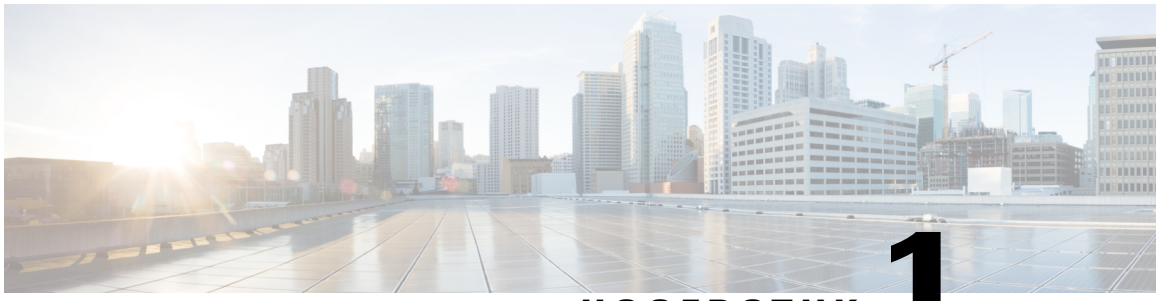
De vergaderingstest gebruiken 254

De systeembrontest gebruiken 254

DEEL I

Installatiehandleiding van Cisco WebEx-vergaderingsserver

- VMware vSphere gebruiken met uw systeem, pagina 3
- Netwerkcontrolelijst voor uw systeem, pagina 9
- Uw systeem installeren met automatische implementatie, pagina 11
- Uw systeem installeren met handmatige implementatie, pagina 39
- Uw mailserver, tijdzone en landinstellingen configureren, pagina 65
- Het systeem na de installatie wijzigen, pagina 69
- Een systeem met hoge beschikbaarheid toevoegen, pagina 73
- Uw systeem uitbreiden naar een groter systeemformaat, pagina 83
- Het systeem bijwerken, pagina 95
- Het systeem bijwerken, pagina 101



HOOFDSTUK 1

VMware vSphere gebruiken met uw systeem

- VMware vSphere gebruiken, pagina 3
- De ESXi-host configureren om een NTP-server te gebruiken, pagina 4
- Een back-up maken met VMware vCenter, pagina 4
- Een momentopname maken met VMware vCenter, pagina 5
- Een bestaand VMDK-bestand aan een nieuwe virtuele machine koppelen, pagina 6

VMware vSphere gebruiken

De virtuele machines voor uw systeem zijn met VMware vSphere geïmplementeerd. Cisco WebEx-vergaderingsserver moet geïnstalleerd zijn op VMware virtuele machines, onderhevig aan de volgende beperkingen

- Gebruik VMware vSphere 5.0, 5.0 Update 1 of 5.1.

  Eerdere versies van vSphere worden niet ondersteund.

- Gebruik VMware ESXi 5.0, 5.0 Update 1 of 5.1.

  Het gebruik van eerdere releases van ESXi leidt tot verwarrende foutberichten over **niet-ondersteunde hardware** waarin het probleem niet expliciet wordt vermeld.

- Zorg ervoor dat de DNS-server die op de ESXi-host is geconfigureerd, de hostnamen van de virtual machines die op die ESXi-host zijn geïmplementeerd, kan omzetten.
- U moet VMware vCenter gebruiken voor het beheren van ESXi-hosts waar het Cisco WebEx Meetings Server-systeem op is geïmplementeerd.
- Selecteer bij het uitschakelen van virtuele machines voor elke machine altijd **In-/uitschakelen** > **Gast afmelden**. (Gebruik niet de optie **Uitschakelen**.)

Opmerking Zie *Systeemvereisten voor Cisco WebEx Meetings Server* voor meer informatie over ondersteunde VMware-configuraties.

De ESXi-host configureren om een NTP-server te gebruiken

Het systeem gebruikt de ESXi-host om de tijd in te stellen. Configureer de ESXi-host om Network Time Protocol (NTP) voor kloksynchronisatie te gebruiken.

Opmerking Dit is een procedure van hoog niveau. Zie uw VMware ESXi-documentatie voor gedetailleerde instructies.

Belangrijk Zorg dat u NTP-configuratie instelt vanuit de ESXi-host.

Procedure

Stap 1 Selecteer de ESXi-host in het overzichtsvenster met gebruik van uw vSphere-client.

Stap 2 Selecteer het tabblad **Configuration** en selecteer **Time Configuration** in de softwaresectie.

Stap 3 Selecteer **Properties** rechtsboven in het venster.

Stap 4 Selecteer **NTP client enabled**.

Stap 5 Selecteer **Options** om de NTP-serverinstellingen te configureren.
Cisco raadt aan dat u **Start en stop with host** selecteert om de mogelijkheid dat de ESXi-host foutief wordt vermindert.

Een back-up maken met VMware vCenter

Back-ups zijn traditionele bestandssystemen die gebruikmaken van VMware-technologie en op SAN gebaseerde gegevensoverdracht. VMware® Data Recovery maakt back-ups van virtuele machines. Het gebruik van de machines en de gegevens of services die ze bieden, worden daarbij niet onderbroken. Data Recovery maakt gebruik van virtuele machines en een clientinvoegtoepassing om back-ups te beheren en herstellen. Het back-upapparaat heeft de indeling OVF (Open Virtualization Format). Voor de Data Recovery-invoegtoepassing is de VMware vSphere-client vereist.

Data Recovery beheert bestaande back-ups en verwijdert back-ups als ze verouderd raken. Het programma ondersteunt ook ontdubbeling om redundante gegevens te verwijderen. We raden u aan om, voordat u procedures uitvoert waarbij het systeem wordt gewijzigd, een back-up van alle virtuele machines te maken met VMware Data Recovery (beschikbaar in VMware vSphere Release 5.0) of vSphere Data Protection (beschikbaar in vSphere Release 5.1). (VMware Data Recovery/vSphere Data Protection wordt met VMware vSphere meegeleverd, behalve in de vSphere Essentials Kit. Zie http://www.vmware.com/pdf/vdr_11_admin.pdf voor meer informatie.)

Ook met een opslagserver kunnen back-ups worden gemaakt. Zie Een opslagserver configureren voor meer informatie.

Een *momentopname* van een virtuele machine is een *beeld* van het systeem op een specifiek tijdstip. Een momentopname is niet hetzelfde als een back-up. Met het oog op prestaties adviseren wij u back-ups van uw virtuele machines te maken en deze op een andere opslaglocatie te bewaren dan de fysieke schijven waarop

uw virtuele machines staan. Zie Een momentopname maken met VMware vCenter voor meer informatie over momentopnamen en bekende prestatieproblemen.

Procedure

Stap 1 Plaats het systeem in onderhoudsmodus. Meer informatie vindt u in Over de onderhoudsmodus, op pagina 125
Zorg dat er geen actieve vergaderingen zijn en dat u een tijdstip hebt geselecteerd waar u uw gebruikers zo weinig mogelijk hindert.

Stap 2 Volg de instructies in uw VMware vSphere-documenten en gebruik VMware-gegevensherstel (vanaf vSphere-release 5.1 VMware vSphere-gegevensbeveiliging genoemd) om een back-up te maken van uw systeem en elke virtuele machine.
Zie de *beheerhandleiding van VMware-gegevensherstel* of de *beheerhandleiding van vSphere-gegevensbeveiliging* voor de complete informatie over deze back-up.

Opmerking Cisco beveelt aan back-ups te verwijderen nadat uw systeemomvattende procedure is voltooid, u het systeem hebt getest en tevreden bent met de resultaten.

Een momentopname maken met VMware vCenter

Momentopnamen van virtuele machines worden gebruikt om virtuele machines snel te herstellen na procedures waarbij het systeem is gewijzigd. Een momentopname is een *beeld* van uw systeem op een specifiek tijdstip. Een momentopname is niet hetzelfde als een back-up (zie Een back-up maken met VMware vCenter). We raden u aan om niet alleen momentopnamen van uw systeem te maken, maar ook back-ups.

Opmerking Als het schijfbestand van een originele virtuele machine verloren gaat, kunt u de virtuele machine niet herstellen met een momentopname.

Momentopnamen worden opgeslagen op de fysieke schijven waarop uw virtuele machines staan. Als u deze momentopnamen niet tijdig verwijdert, kunnen uw eindgebruikers kwaliteitsproblemen met audio en video ervaren. Dit is een bekend probleem dat de prestaties van virtuele machines beïnvloedt. Om goede prestaties te garanderen adviseren wij u daarom back-ups te maken, of de back-ups van uw virtuele machine op een andere locatie te bewaren dan de fysieke schijven waar uw virtuele machine op staat. Momentopnamen kunnen ook worden gebruikt voor updates, maar voor systeemupgrades raden we u aan om alle momentopnamen te verwijderen en een back-up te maken van het originele systeem. (Voor meer informatie over dit bekende probleem met VMware-momentopnamen, gaat u naar de VMware-website en leest u het (Engelstalige) witboek *Best Practices for Running VMware vSphere on Network Attached Storage*. U kunt ook in de VMware Knowledge Base zoeken naar **snapshot impact performance** voor meer (Engelstalige) informatie.)

Cisco raadt u aan om, voordat u procedures gaat uitvoeren waarbij het systeem wordt gewijzigd, een back-up van uw systeem te maken (vooral wanneer u een upgrade gaat uitvoeren), of een momentopname te maken van alle virtuele machines (vooral wanneer u een update gaat uitvoeren). U kunt een back-up van uw systeem maken met VMware Data Recovery (vanaf vSphere Release 5.1 wordt dit VMware vSphere Data Protection genoemd) of een momentopname van elke virtuele machine maken.
(VMware-gegevensherstel/vSphere-gegevensbeveiliging maakt deel uit van VMware vSphere, behalve in de vSphere Essentials-kit.)

Om goede prestaties te garanderen, moet u de momentopnamen van uw virtuele machines op een andere locatie bewaren dan de fysieke schijven waar uw virtuele machines op staan.

Vergeet niet het gedeelte over de voorbereiding van de specifieke procedure te lezen. Cisco vermeldt voor elke procedure aandachtspunten.

Onthouden Als uw systeem meerdere virtuele machines bevat, dient u een momentopname te maken van elke virtuele machine na het selecteren van **Power** > **Shut Down Guest**. Label de momentopname van elke virtuele machine met hetzelfde voorvoegsel (bijvoorbeeldAugustus 20), zodat u kunt zien dat deze momentopnamen op hetzelfde moment zijn gemaakt.

Opmerking Cisco raadt u aan om momentopnamen niet langer dan 24 uur te bewaren. Als u ze langer wilt bewaren, maakt u in plaats daarvan een back-up. Voor meer informatie over VMware-gegevensherstel (vanaf vSphere-release 5.1 VMware vSphere-gegevensbeveiliging genoemd) kunt u Een back-up maken met VMware vCenter, op pagina 4 raadplegen.

Procedure

Stap 1 Plaats het systeem in onderhoudsmodus. Meer informatie vindt u in Over de onderhoudsmodus, op pagina 125.
Zorg dat er geen actieve vergaderingen zijn en dat u een tijdstip hebt geselecteerd waar u uw gebruikers zo weinig mogelijk hindert.

Stap 2 In VMware vCenter selecteert u **Power** > **Shut Down Guest** voor elke virtuele machine.

Stap 3 Selecteer **Snapshot** > **Take Snapshot** voor elke virtuele machine.

Stap 4 Voer een naam in voor de momentopname en selecteer **OK**.

Volgende stappen

- Voltooi de procedure en test uw systeem om te bevestigen dat het gelukt is.
- Als u moet terugkeren naar een momentopname moet u ervoor zorgen dat de momentopname voor elke virtuele machine op hetzelfde moment genomen werd. Een systeem inschakelen met verkeerd gecombineerde momentopnamen kan leiden tot mogelijke corruptie van de database.

Een bestaand VMDK-bestand aan een nieuwe virtuele machine koppelen

Dit gedeelte beschrijft hoe u VMDK-bestanden van een bestaande virtuele beheermachine aan een nieuwe virtuele beheermachine koppelt met behulp van VMware vCenter.

Hoewel er meerdere redenen zijn voor het verplaatsen van een virtual disk VMDK-bestand, concentreert deze rubriek zich enkel op de procedure voor het verplaatsen van gegevens van een virtuele beheermachine naar een andere virtuele beheermachine. U maakt gebruik van deze procedure als u uw systeem uitbreidt of upgradet. (We hergebruiken de systeemgegevens opgeslagen op harde schijf 4 van de virtuele beheermachine.)

Voorzichtig Maak een kopie van het VDMK-bestand op harde schijf 4 en kopieer het rechtstreeks in de virtuele machinemap van de virtuele beheermachine in het geüpgrade of uitgebreide systeem. Als u de harde schijf 4 gewoon toevoegt, staan de gegevens nog steeds opgeslagen in de virtuele machinemap van de oude virtuele beheermachine. Als u per ongeluk de oude virtuele beheermachine in de vCenter-inventaris wist, verliest uw huidige systeem toegang tot de harde schijf 4.

Opmerking Wanneer u gebruik maakt van Direct-attached storage (DAS), moet u het virtuele machine VMDK-bestand migreren naar een LUN waartoe de nieuwe virtuele beheermachine toegang heeft.

Opmerking We verwijzen naar de virtuele beheermachine voor de systeemomvattende procedure als de 'bestaande' virtuele beheermachine. De virtuele beheermachine wordt na de uitbreiding of upgrade de 'nieuwe' virtuele beheermachine genoemd.

Procedure

Stap 1 Navigeer de inventaris in VMware vCenter en zoek de bestaande virtuele beheermachine voor uw systeem.

Stap 2 Klik met de rechter muisknop op de naam van de virtuele machine en selecteer **Edit Settings...**
Het venster **Eigenschappen virtuele machine** wordt weergegeven.

Stap 3 Selecteer het tabblad **Hardware** en selecteer vervolgens **Harde schijf 4**.

Stap 4 Kopieer en plak de locatie van het **Disk File** in een ander document ter referentie voor later.
Dit beschrijft de locatie van dat VMDK-bestand in VMware vCenter.

De reeks is vergelijkbaar met `[EMC-LUN10-RAID5] webex-sysA-admin/webex-sysA-admin_3-000001.vmdk`. Als u voordien uw systeem hebt bijgewerkt, volgt de bestandsnaam niet de naamgevingsconventies van de bestaande virtuele machine.

Stap 5 Noteer de opslaglocatie voor Harde schijf 4 en de mapnaam van de virtuele machine.
De bestandsnaamreeks is vergelijkbaar met `[EMC-LUN8-RAID5] webex-sysB-admin`.

Stap 6 Sluit het venster **Edit Settings...** zonder wijzigingen uit te voeren.

Stap 7 Wijzig de weergave van vCenter naar de weergave Gegevensopslag en Cluster gegevensopslag. Selecteer **Weergeven** > **Inventaris** > **Gegevensopslag en gegevensopslagclusters**.

Stap 8 Selecteer de opslaglocatie waar uw bestaande virtuele beheermachine zich bevindt (in stap 5) en selecteer **Browse this datastore**

Stap 9 Selecteer de opslaglocatie waar uw pas geïmplementeerde (voor het uitgebreide of bijgewerkte systeem) virtuele beheermachine zich bevindt, en selecteer **Browse this datastore**.

Stap 10 Plaats de twee browservensters voor gegevensopslag (voor de bestaande en de nieuwe virtuele beheermachine) naast elkaar zodat u de mappen van beide virtuele beheermachines kunt zien.

Stap 11 Open de mappen van de beide virtuele machines en kopieer het VMDK-bestand van de map van de bestaande virtuele beheermachine naar de map van de nieuwe virtuele beheermachine.

a) Zoek in de map van de bestaande virtuele beheermachine het VMDK-bestand dat aan Harde schijf 4 is gekoppeld. Gebruik de bestandslocatie die u in stap 4 hebt genoteerd om de nauwkeurigheid te bevestigen.
b) Klik met rechtermuisknop op het bestand en selecteer **Copy**.

c) Klik met de rechter muisknop in de map van de nieuwe virtuele beheermachine en selecteer **Paste**. Sluit de beide gegevensopslagvensters wanneer de plakbewerking is voltooid.

d) Plaats de weergave van vCenter terug op een lijst met hosts en clusters door **View** > **Inventory** > **Hosts and Clusters** te selecteren.

Stap 12 Navigeer de inventaris in VMware vCenter en zoek de nieuwe (uitgebreide of bijgewerkte) virtuele beheermachine voor uw systeem.

Stap 13 Klik met de rechter muisknop op de naam van de pas geïmplementeerde virtuele machine en selecteer **Edit Settings...**.
Het venster **Eigenschappen virtuele machine** wordt weergegeven.

Stap 14 Selecteer het tabblad **Hardware** en selecteer vervolgens **Harde schijf 4**.

Stap 15 Selecteer **Remove**.
Deze handeling verwijdert de virtuele schijf niet onmiddellijk. Het verwijderen van de bestaande virtuele schijf wordt gepland.

Stap 16 Selecteer **Toevoegen**.
De wizard **Add Hardware** verschijnt.

Stap 17 Selecteer **Hard Disk** en daarna **Next**.

Stap 18 Selecteer **Use and existing virtual disk** en daarna **Next**.

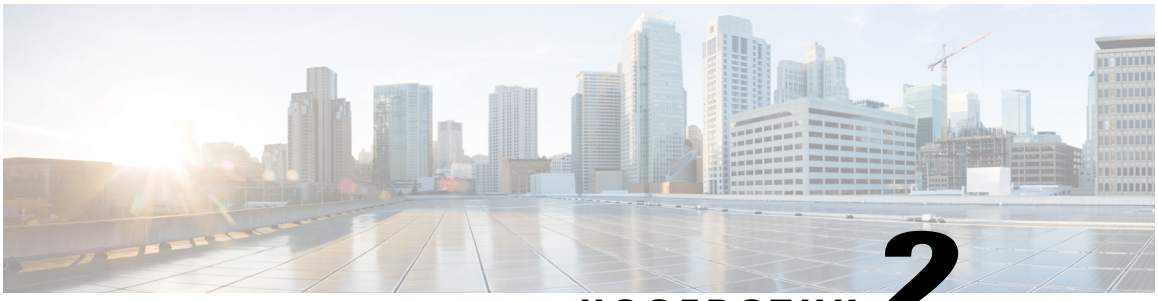
Stap 19 Selecteer **Bladeren** en navigeer naar de gegevensopslag waar de nieuwe, uitgebreide of bijgewerkte virtuele beheermachine zich bevindt. Ga naar de map van de nieuwe virtuele beheermachine. Dubbelklik op deze map en selecteer de virtuele schijf die u in stap 11 hebt gekopieerd. Selecteer **OK**.

Stap 20 In het vervolgkeuzemenu **Knooppunt virtueel apparaat** selecteert u **SCSI (0:3)** en daarna **Volgende**.

Stap 21 Controleer uw wijzigingen. Als alles correct is, selecteert u **Finish**. Anders selecteert u **Vorige** en corrigeert u mogelijke fouten.
Nadat de wizard is voltooid, ziet u een nieuwe schijf de klaar staat om toegevoegd te worden in het tabblad Hardware.

Stap 22 Voer de handelingen Toevoegen en Verwijderen uit door **OK** te selecteren.

Stap 23 Bekijk de herconfiguratietaak van deze virtuele machine in het VMware vCenter-deelvenster **Recent Tasks** om zeker te zijn dat er geen fouten zijn.



HOOFDSTUK 2

Netwerkcontrolelijst voor uw systeem

- Controlelijst netwerken voor een systeem met publieke toegang en zonder split-horizon DNS, pagina 9
- Controlelijst netwerken voor een systeem met publieke toegang en split-horizon DNS, pagina 10
- Controlelijst netwerken voor een systeem zonder openbare toegang, pagina 10

Controlelijst netwerken voor een systeem met publieke toegang en zonder split-horizon DNS

Tijdens de implementatie van uw systeem geven we een pagina weer met koppelingen naar de netwerkcontrolelijsten. Deze controlelijsten bieden een samenvatting van de DNS-server, firewall en andere netwerkwijzigingen die vereist zijn voor succesvolle implementatie. Zorg dat u deze noodzakelijke wijzigingen uitvoert voordat u de implementatie start, aangezien we vlak voor het einde van het implementatieproces een controle van de netwerkverbinding uitvoeren.

Opmerking De DNS zonder split-horizon is de meest voorkomende DNS-configuratie voor bedrijven. Voor meer informatie over deze DNS zonder split horizon raadpleegt u de *planningshandleiding van Cisco WebEx Meetings Server*.

Opmerking Als u een groot systeem implementeert, moet u een handmatige implementatie kiezen.

Selecteer de geschikte controlelijst in de *Planningshandleiding van Cisco WebEx-vergaderingsserver*.

- Automatische implementatie: zie "Netwerkcontrolelijst voor installatie of uitbreiding met automatische implementatie, openbare toegang en een DNS zonder split horizon"
- Handmatige implementatie: zie "Netwerkcontrolelijst voor installatie of uitbreiding met handmatige implementatie, openbare toegang en een DNS zonder split horizon"

Controlelijst netwerken voor een systeem met publieke toegang en split-horizon DNS

Tijdens de implementatie van uw systeem geven we een pagina weer met koppelingen naar de netwerkcontrolelijsten. Deze controlelijsten bieden een samenvatting van de DNS-server, firewall en andere netwerkwijzigingen die vereist zijn voor succesvolle implementatie. Zorg dat u deze noodzakelijke wijzigingen uitvoert voordat u de implementatie start, aangezien we vlak voor het einde van het implementatieproces een controle van de netwerkverbinding uitvoeren.

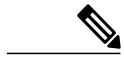
Opmerking Als u een groot systeem implementeert, moet u een handmatige implementatie kiezen.

Selecteer de geschikte controlelijst in de *Planningshandleiding van Cisco WebEx-vergaderingsserver*.

- Automatische implementatie: zie "Netwerkcontrolelijst voor installatie of uitbreiding met automatische implementatie, openbare toegang en een split horizon DNS"
- Handmatige implementatie: zie "Netwerkcontrolelijst voor installatie of uitbreiding met handmatige implementatie, openbare toegang en een split horizon DNS"

Controlelijst netwerken voor een systeem zonder openbare toegang

Tijdens de implementatie van uw systeem geven we een pagina weer met koppelingen naar de netwerkcontrolelijsten. Deze controlelijsten bieden een samenvatting van de DNS-server, firewall en andere netwerkwijzigingen die vereist zijn voor succesvolle implementatie. Zorg dat u deze noodzakelijke wijzigingen uitvoert voordat u de implementatie start, aangezien we vlak voor het einde van het implementatieproces een controle van de netwerkverbinding uitvoeren.



Opmerking Als u een groot systeem implementeert, moet u een handmatige implementatie kiezen.

Selecteer de geschikte controlelijst in de *Planningshandleiding van Cisco WebEx-vergaderingsserver*.

- Automatische implementatie: zie "Netwerkcontrolelijst voor installatie of uitbreiding met automatische implementatie en zonder openbare toegang"
- Handmatige implementatie: zie "Netwerken Controlelijst voor een installatie of uitbreiding met handmatige installatie en geen openbare toegang"

HOOFDSTUK 3

Uw systeem installeren met automatische implementatie

- Algemene concepten voor de implementatie van uw systeem, pagina 12
- Installatiechecklist, pagina 13
- Vereiste gegevens voor een automatische implementatie, pagina 14
- Het OVA-bestand van de VMware vSphere-client implementeren, pagina 16
- Uw taal voor installatie selecteren, pagina 28
- De implementatie bevestigen, pagina 29
- De grootte van uw systeem bevestigen, pagina 29
- Kiezen welk systeem u moet installeren, pagina 29
- Het type systeemimplementatie kiezen, pagina 30
- VMware vCenter-gebruikersgegevens opgeven, pagina 30
- vCenter-instellingen voor uw virtuele mediamachine selecteren, pagina 31
- Netwerkinformatie voor de virtuele mediamachine invoeren, pagina 31
- Openbare toegang toevoegen, pagina 32
- vCenter-instellingen voor uw Reverse Proxy kiezen, pagina 32
- De netwerkinformatie voor de Reverse Proxy-virtuele machine invoeren, pagina 33
- Het openbare VIP-adres invoeren, pagina 33
- Het privé-VIP-adres invoeren, pagina 34
- URL's van WebEx-site en WebEx-beheer, pagina 34
- De URL's van de WebEx-site en –Beheer invoeren, pagina 36
- Bevestigen dat uw netwerk op de juiste manier is geconfigureerd, pagina 36
- Uw virtuele machines implementeren, pagina 36
- Uw systeem controleren, pagina 37

Algemene concepten voor de implementatie van uw systeem

Systeemgroottes

- Systeem voor 50 gelijktijdige gebruikers
  - Geschikt voor een bedrijf met 500 tot 1000 werknemers
  - Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine en een optionele Reverse Proxy (voor publieke toegang)
- Systeem voor 250 gelijktijdige gebruikers
  - Geschikt voor een bedrijf met 2500 tot 5000 werknemers
  - Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine, een virtuele mediamachine en een optionele Reverse Proxy (voor publieke toegang)
- Systeem voor 800 gelijktijdige gebruikers
  - Geschikt voor een bedrijf met 8000 tot 16.000 werknemers
  - Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine, een virtuele mediamachine en een optionele Reverse Proxy (voor publieke toegang)
- Systeem voor 2000 gelijktijdige gebruikers
  - Geschikt voor een bedrijf met 20.000 tot 40.000 werknemers
  - Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine, 3 virtuele mediamachines, 2 webmachines en een optionele Reverse Proxy (voor publieke toegang)

Gebruikte termen tijdens de implementatie

Veldnaam	Beschrijving
URL van WebEx-site	Beveiligde http-URL voor gebruikers om vergaderingen te hosten en bij te wonen.
URL WebEx-beheer	Beveiligde http-URL voor beheerders om het systeem te configureren, controleren en beheren.
Openbaar VIP	IP-adres voor de URL van de WebEx-site
Privé-VIP	• IP-adres voor de URL van de beheersite • Het IP-adres voor de URL van de WebEx-site (alleen voor interne gebruikers, als u een DNS met split-horizon hebt).

Installatiechecklist

Beperking U moet VMware vCenter gebruiken voor het beheren van ESXi-hosts waar het Cisco WebEx Meetings Server-systeem op is geïmplementeerd.

Netwerkwijzigingen

Raadpleeg de toepasselijke netwerkchecklist voor uw implementatie. Er zijn twee overwegingen:

- Publieke toegang: of gebruikers wel of niet buiten uw firewall vergaderingen kunnen hosten of toegang tot vergaderingen kunnen krijgen via internet of mobiele apparaten.

  Cisco beveelt openbare toegang aan, omdat dit tot een betere gebruikerservaring voor uw mobiele werkkrachten leidt.

- Type DNS-instelling in uw bedrijf: DNS met split-horizon of een DNS zonder split-horizon (meest voorkomende DNS-configuratie).

  Voor meer informatie over deze typen DNS-instelling kunt u de *Planningshandleiding van Cisco WebEx-vergaderingsserver* raadplegen.

- Open poort 10200 van op het bureaublad van de beheerder naar de virtuele beheermachine.

  Poort 10200 wordt gebruikt door de webbrowser tijdens de implementatie.

Selecteer de juiste checklist voor uw implementatie:

- Controlelijst netwerken voor een systeem met publieke toegang en zonder split-horizon DNS, op pagina 9
- Controlelijst netwerken voor een systeem zonder openbare toegang, op pagina 10
- Controlelijst netwerken voor een systeem met publieke toegang en split-horizon DNS, op pagina 10

Verplichte gegevens

Opmerking Welke gegevens zijn vereist, is afhankelijk van de implementatie die u uitvoert; een automatische implementatie (ondersteunt 50 gelijktijdige gebruikers, 250 gelijktijdige gebruikers en 800 gelijktijdige gebruikers) of een handmatige implementatie (ondersteunt alle systeemgroottes). Cisco raadt u aan een automatische implementatie te selecteren, tenzij u een systeem met 2000 gebruikers implementeert. In dat geval is een handmatige implementatie vereist. Raadpleeg de toepasselijke koppeling hieronder.

Kies een van de volgende opties voor een controlelijst van de vereiste gegevens voor uw implementatietype:

- Vereiste gegevens voor een automatische implementatie, op pagina 14
- Vereiste gegevens voor een handmatige implementatie, op pagina 41

Vereiste gegevens voor een automatische implementatie

Dit zijn de vereiste gegevens voor uw systeem, op volgorde.

Opmerking Zorg dat u de FQDN's, de IP-adressen, URL's van WebEx-site en beheersite en VIP-adressen van de virtuele machine aan uw DNS-servers toevoegt voordat u het systeem implementeert. Wij gebruiken deze informatie om IP-adressen voor u op te zoeken tijdens de implementatie.

Ter voorkoming van DNS-problemen kunt u wellicht beter deze URL's en IP-adressen testen voordat u de OVA-implementatie start. U kunt deze fouten beter herstellen, anders mislukt de implementatie van het systeem.

Veldnaam	Beschrijving	Waarde voor uw systeem
vCenter-URL	Beveiligd http-adres van de vCenter-server voor de virtuele machines in uw systeem.	
vCenter-gebruikersnaam	Gebruikersnaam om de virtuele machines voor uw systeem te implementeren. Deze gebruiker moet over beheerdersrechten beschikken: om virtuele machines te gebruiken, configureren, in- of uit te schakelen en te verwijderen.	
vCenter-wachtwoord	Wachtwoord van de vCenter-gebruiker.	
(alleen voor systemen met 250 en 800 gelijktijdige gebruikers) ESXi-host	ESXi-host voor de virtuele mediamachine. **Opmerking** Deze ESXi-host moet op dezelfde vCenter zitten als de URL van de vCenter hierboven.	
(alleen voor systemen met 250 en 800 gelijktijdige gebruikers) Gegevensopslag	Gegevensopslag voor de virtuele mediamachine.	
(alleen voor systemen met 250 en 800 gelijktijdige gebruikers) Poortgroep voor virtuele machines	Poortgroep voor de virtuele mediamachine. **Opmerking** Cisco raadt u aan dezelfde poortgroep te kiezen als de poortgroep die u voor de virtuele beheermachine hebt geselecteerd.	
(alleen voor systemen met 250 en 800 gelijktijdige gebruikers) FQDN voor de virtuele mediamachine.	Volledige domeinnaam (met alleen kleine letters) van de virtuele mediamachine.	

Veldnaam	Beschrijving	Waarde voor uw systeem
(alleen voor systemen met 250 en 800 gelijktijdige gebruikers) IPv4-adres voor de virtuele mediamachine	IPv4-adres voor de virtuele mediamachine. Wij zullen automatisch het overeenstemmende IPv4-adres opzoeken voor deze virtuele mediamachine.	
(alleen openbare toegang) ESXi-host	ESXi-host voor de Reverse Proxy virtuele machine. **Opmerking** Cisco raadt u aan een andere ESXi-host te selecteren dan de host die u hebt gekozen voor de virtuele beheermachine en andere interne virtuele machine. Om verkeer op de Reverse Proxy in te schakelen, moet u ervoor zorgen dat de ESXi host is geconfigureerd met een poortgroep die de VLAN kan doorsturen waarvan het IP-adres wordt gebruikt door de Reverse Proxy.	
(alleen openbare toegang) Gegevensopslag	Gegevensopslag voor de Reverse Proxy virtuele machine.	
(alleen openbare toegang) Poortgroep virtuele machine	Poortgroep voor de Reverse Proxy virtuele machine. **Opmerking** Cisco raadt u voor uw veiligheid aan een andere poortgroep te selecteren dan de host die u hebt gekozen voor de virtuele beheermachine.	
(alleen openbare toegang) FQDN voor de Reverse Proxy	Volledige domeinnaam (met alleen kleine letters) van de Reverse Proxy-virtuele machine.	
(alleen openbare toegang) Reverse Proxy IPv4-adres	IPv4-adres voor de Reverse Proxy virtuele machine. Wij zullen automatisch het overeenstemmende IPv4-adres opzoeken voor deze Internet Reverse Proxy virtuele machine.	
(alleen openbare toegang) IPv4-gateway	IPv4-gateway voor de Reverse Proxy virtuele machine.	
(alleen openbare toegang) IPv4-Subnetmasker	Subnetmasker voor de Reverse Proxy virtuele machine.	

Veldnaam	Beschrijving	Waarde voor uw systeem
(alleen openbare toegang) IPv4-adres primaire DNS-server	DNS-server voor de Reverse Proxy virtuele machine.	
(alleen openbare toegang) IPv4-adres secundaire DNS-server	(Optioneel) Extra DNS-server voor de Reverse Proxy virtuele machine.	
Openbaar VIP	IP-adres voor de URL van de WebEx-site (toegang voor sitegebruikers om vergaderingen te hosten en bij te wonen)	
Privé-VIP	• IP-adres voor de URL van de beheerwebsite (voor beheerders om het systeem te configureren, controleren en beheren.) • Het IP-adres voor de URL van de WebEx-site (alleen voor interne gebruikers, als u een DNS met split-horizon hebt).	
URL van WebEx-site	Beveiligde http-URL (met alleen kleine letters) voor gebruikers om vergaderingen te hosten en bij te wonen.	
URL WebEx-beheer	Beveiligde http-URL (met alleen kleine letters) voor beheerders om het systeem te configureren, controleren en beheren.	

Wat moet u nog meer doen

Met deze informatie start u de implementatie van het systeem door de implementatie-URL in te voeren in een browservenster. (De implementatie-URL wordt weergegeven in het consolevenster voor de virtuele beheermachine.)

Opmerking Als het systeem opnieuw is opgestart voordat de configuratie is voltooid, wordt een nieuwe toegangscode gegenereerd en moet u de implementatie-URL gebruiken met de nieuwe toegangscode.

Het OVA-bestand van de VMware vSphere-client implementeren

Voordat u uw systeem implementeert, moet u de VMware vSphere-client gebruiken om de virtuele beheermachine voor uw systeem te implementeren.

Opmerking De volgende procedure wordt verstrekt als algemene handleiding. Welke schermen precies worden weergegeven tijdens de OVA-implementatie, is afhankelijk van uw vCenter-, opslag- en netwerkconfiguratie. Dit kan enigszins afwijken van deze procedure. Bekijk uw VMware vSphere-documentatie voor volledige informatie over de OVA-wizard.

Voordat u begint

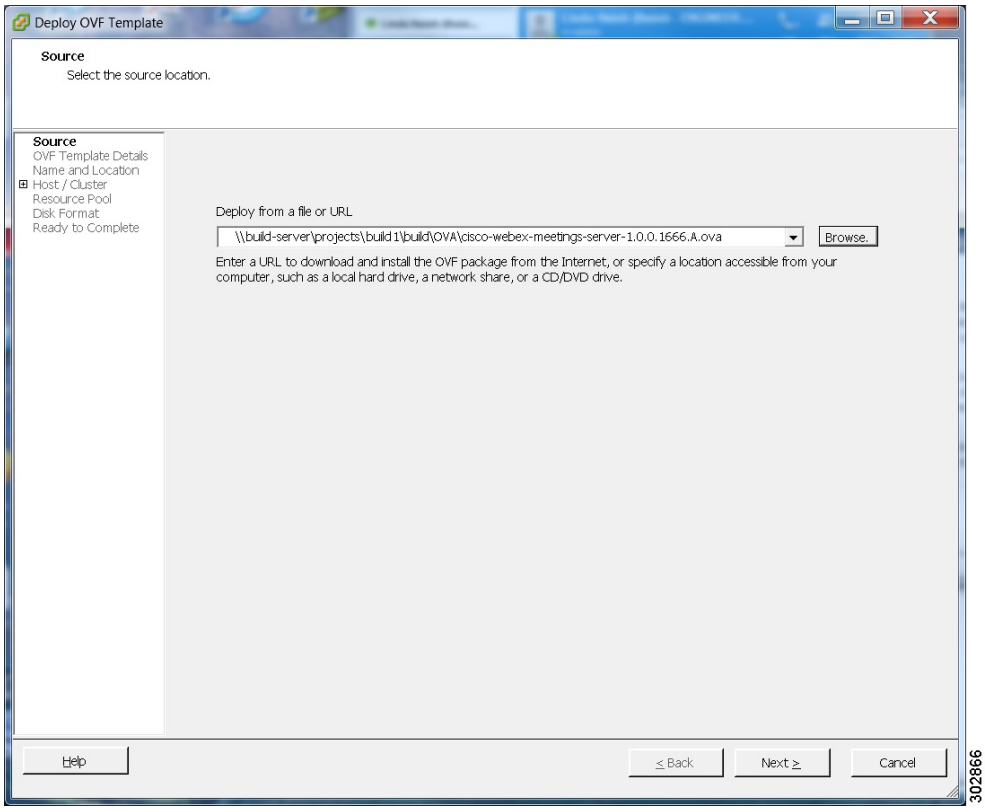
Verkrijg het OVA-bestand van de Cisco WebEx-vergaderingsserver voor uw systeem en plaats het in een locatie die toegankelijk is vanaf VMware vSphere.

U moet VMware vCenter gebruiken voor het beheren van ESXi-hosts waar het Cisco WebEx Meetings Server-systeem op is geïmplementeerd. Gebruik de vSphere-client om u aan te melden bij vCenter en implementeer het OVA-bestand voor de virtuele beheermachine.

Procedure

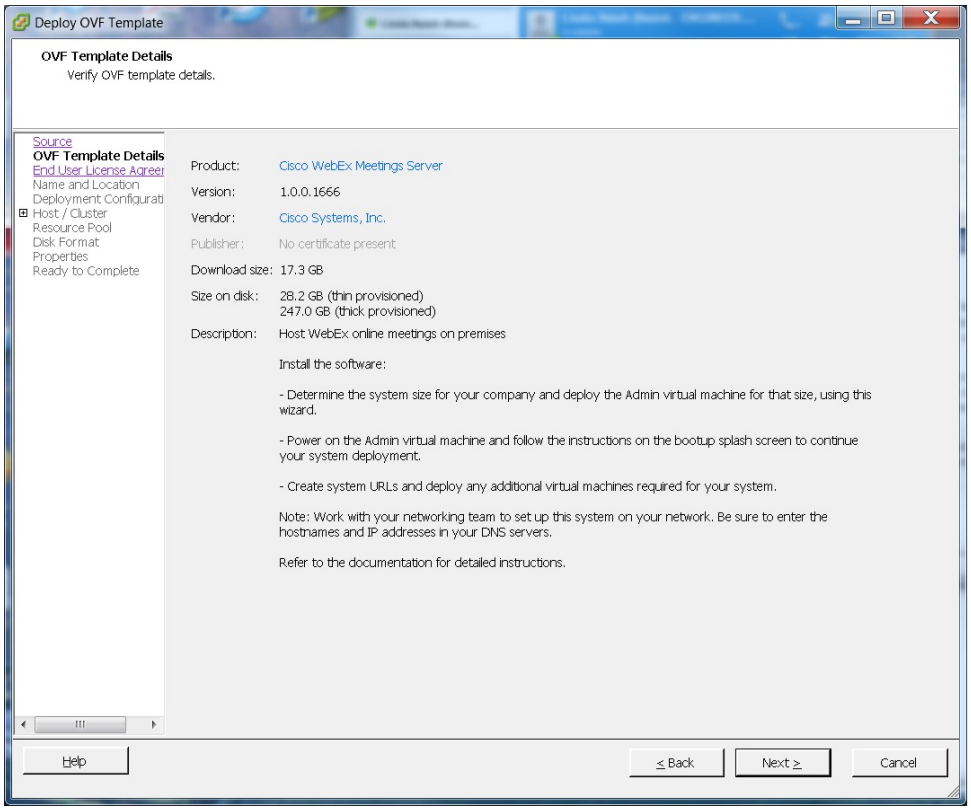
Stap 1 Meld u aan bij uw VMware vSphere-client.
Zorg dat u zich als gebruiker met beheerdersrechten aanmeldt: om virtuele machines te gebruiken, configureren, in- of uit te schakelen en te verwijderen.

Stap 2 Selecteer **File** > **Deploy OVF Template...**



Stap 3 Selecteer **Bladeren** om naar de locatie van het OVA-bestand te navigeren. Selecteer **Volgende**.

U kunt op de koppeling **Cisco WebEx Meetings Server** klikken om naar een webpagina met uitgebreide informatie over dit systeem te gaan.



Stap 4 Lees de licentieovereenkomst voor eindgebruikers en selecteer **Accept** en dan **Next**.

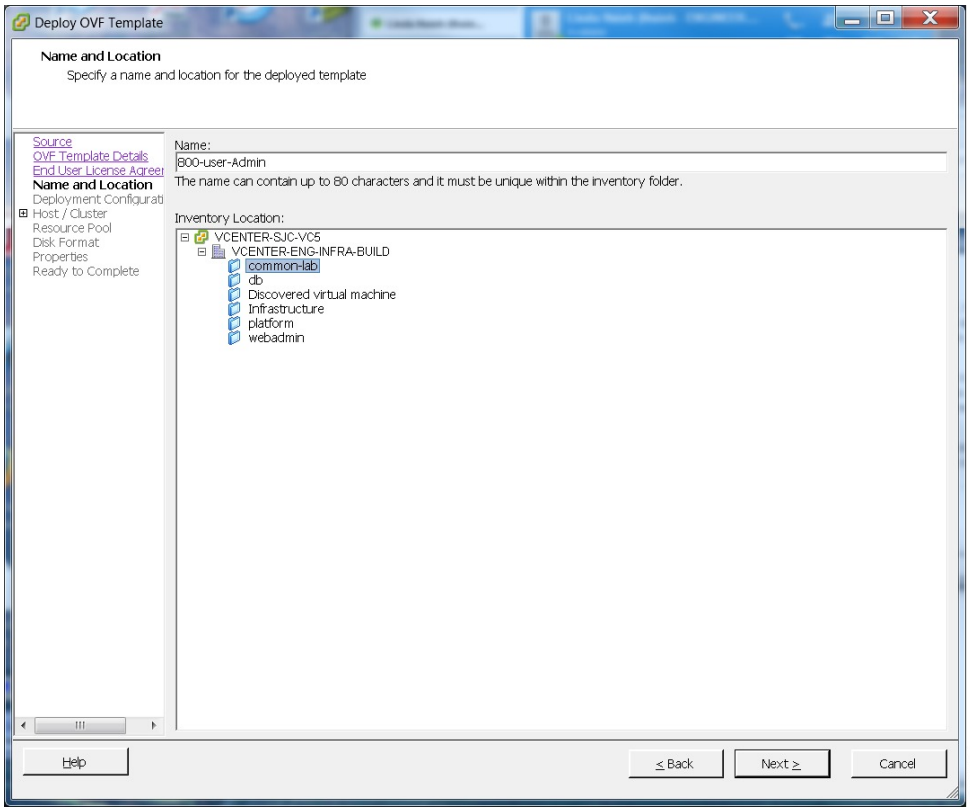
Stap 5 Navigeer in het vCenter-overzicht naar de locatie waar u de virtuele beheermachine wilt plaatsen en selecteer deze locatie.

Stap 6 Voer de naam van de virtuele beheermachine in voor uw systeemgrootte en selecteer **Next**. Zie Systeemgroottes voor meer informatie over het selecteren van de juiste omvang voor uw bedrijf.

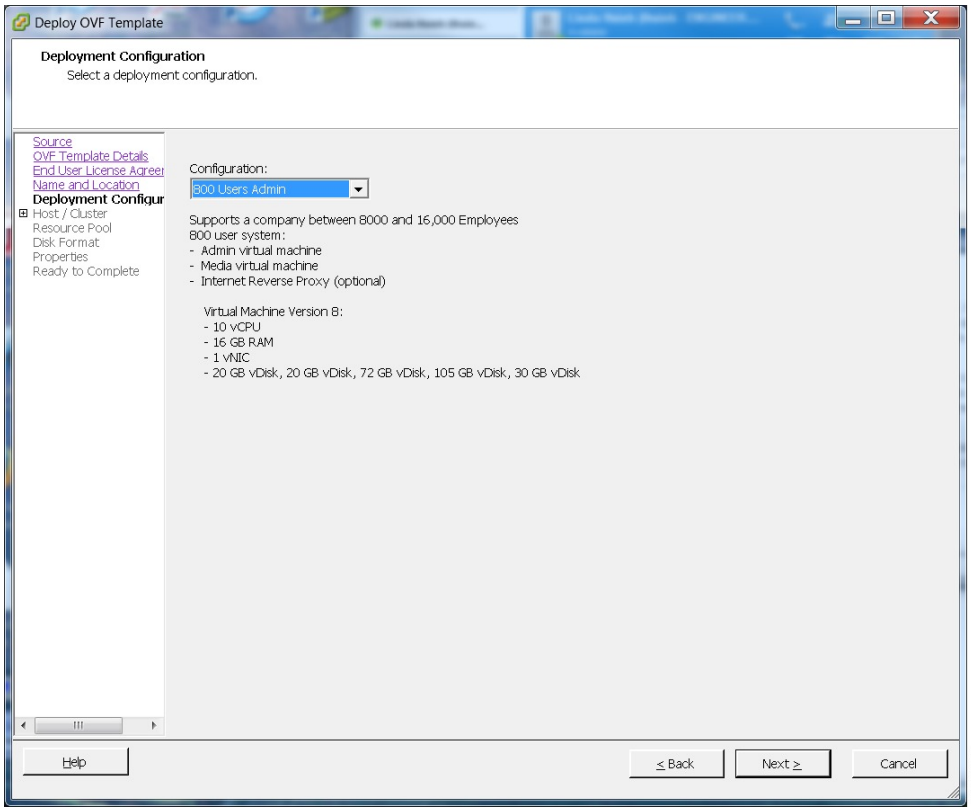
Opmerking U moet de virtuele beheermachine implementeren voordat u de andere virtuele machines implementeert. Als u automatische implementatie selecteert (aanbevolen), implementeren wij de andere virtuele machines voor u. Als u voor handmatige implementatie kiest (verplicht voor systemen met 2000 gelijktijdige gebruikers), moet u met deze wizard de andere virtuele machines implementeren nadat u de virtuele beheermachine hebt geïmplementeerd.

Cisco raadt aan om in de naam van de virtuele machine het type machine te gebruiken (bijvoorbeeld 'beheer' in de naam van de virtuele beheermachine), zodat de machine goed te herkennen is in het vCenter-overzicht.

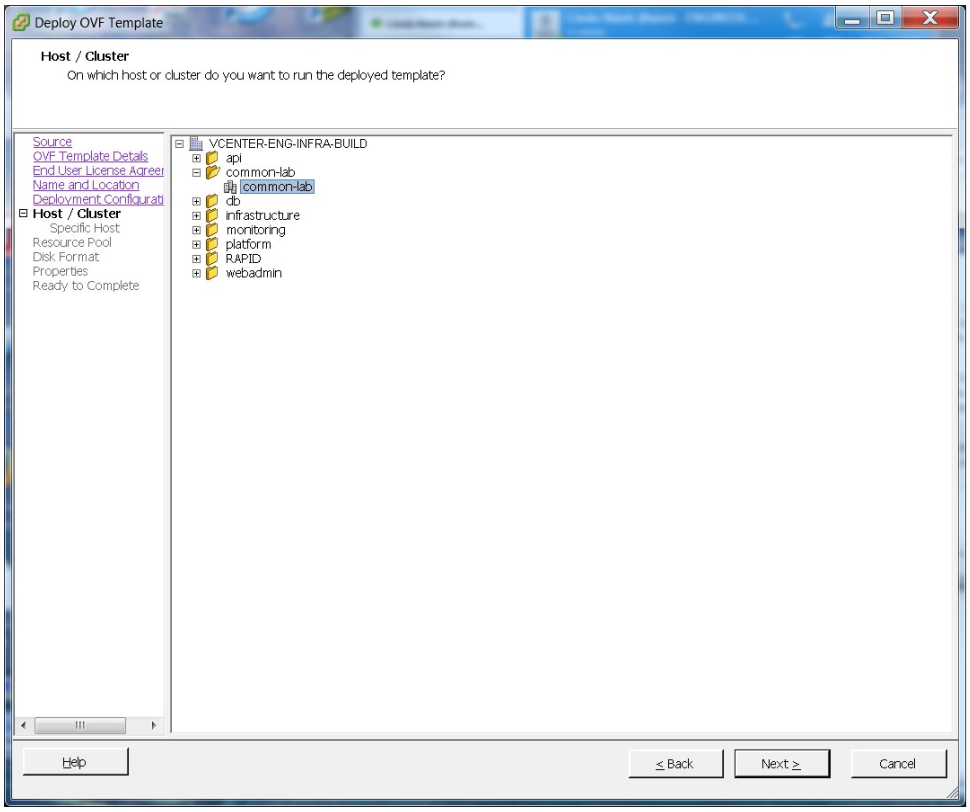
Opmerking Alle interne virtuele machines voor uw systeem moeten zich in hetzelfde subnet bevinden als de virtuele beheermachines. (Afhankelijk van de geselecteerde systeemomvang hebt u mogelijk een of meer interne virtuele machines nodig voor media en het web.)



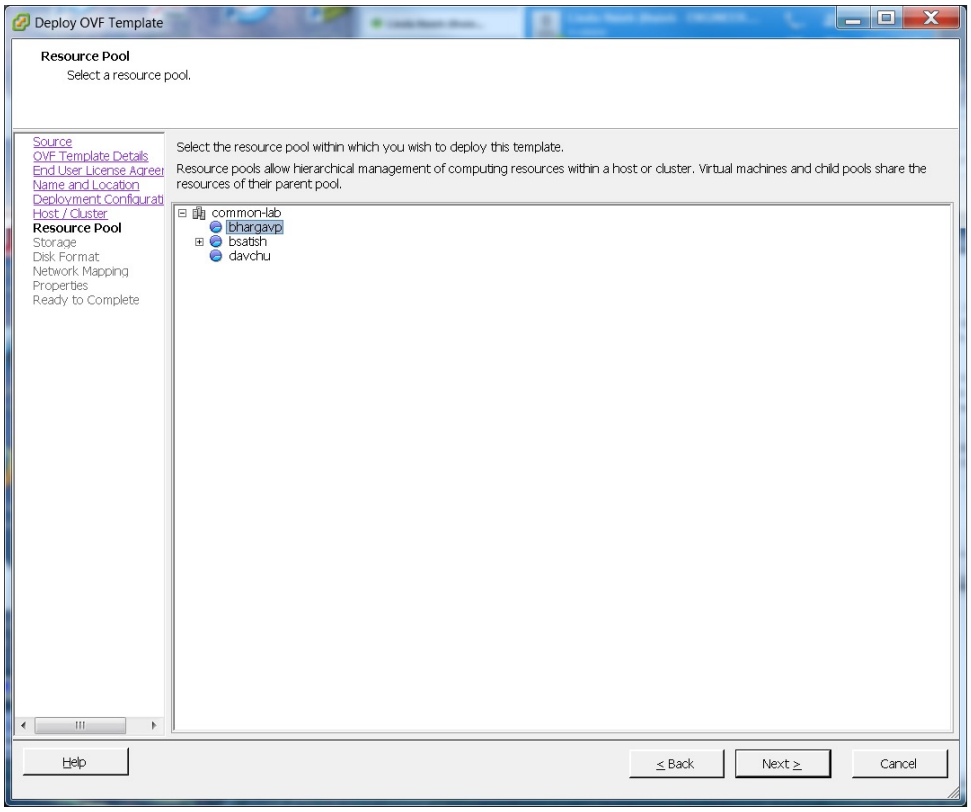
Stap 7 Selecteer in de vervolgkeuzelijst de virtuele machine voor uw systeemomvang en selecteer **Volgende**. Zorg ervoor dat u de virtuele beheermachine vóór alle andere virtuele machines in uw systeem implementeert.



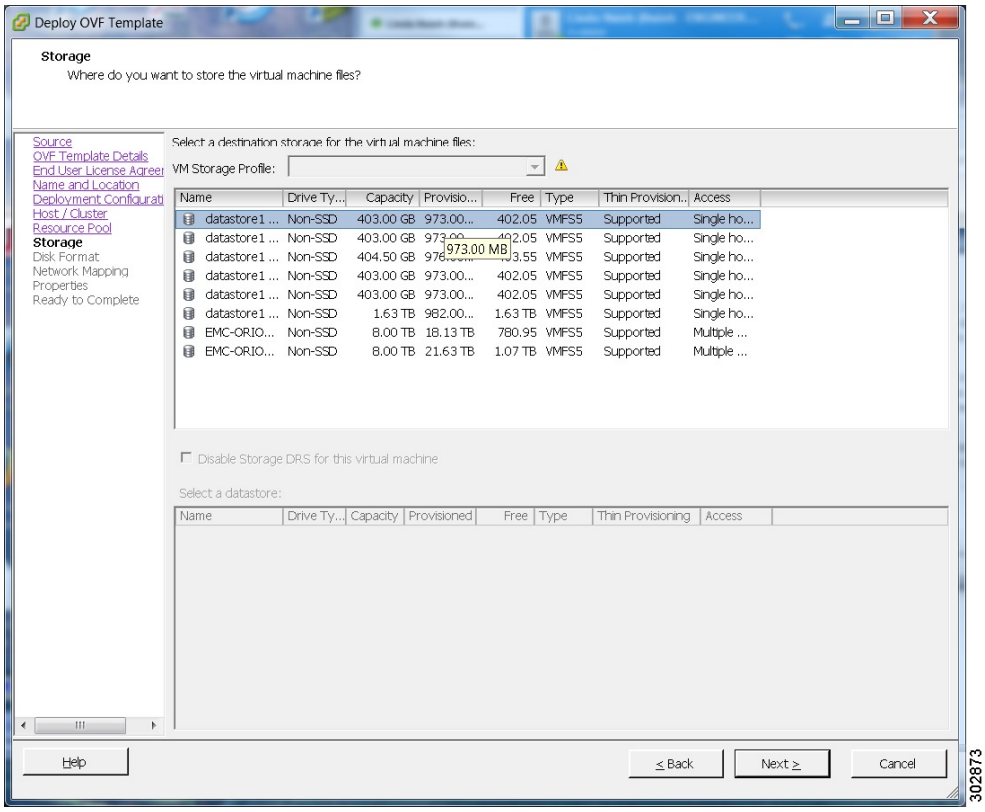
Stap 8 Navigeer door het vCenter-overzicht en selecteer de ESXi-host of het cluster waar u de virtuele machines voor uw systeem wilt implementeren. Selecteer **Volgende**.

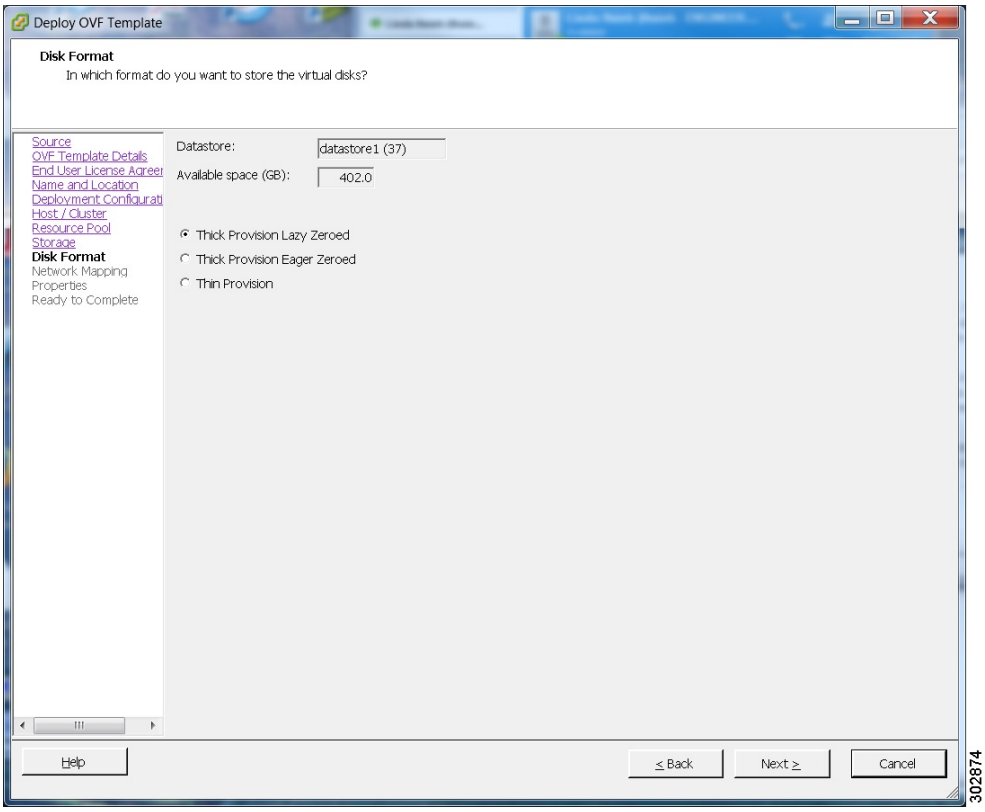


Stap 9 Als het cluster een resource-pool bevat, selecteert u de resource-pool waar u de OVA-sjabloon wilt implementeren en selecteert u **Volgende**.
Resource-pools delen CPU- en geheugenbronnen voor VMware-functies als DRS of vMotion. Resource-pools moeten aan één ESXi-host worden toegewezen. Het is niet raadzaam om resource-pools van VMware te gebruiken met Cisco WebEx Meetings Server.



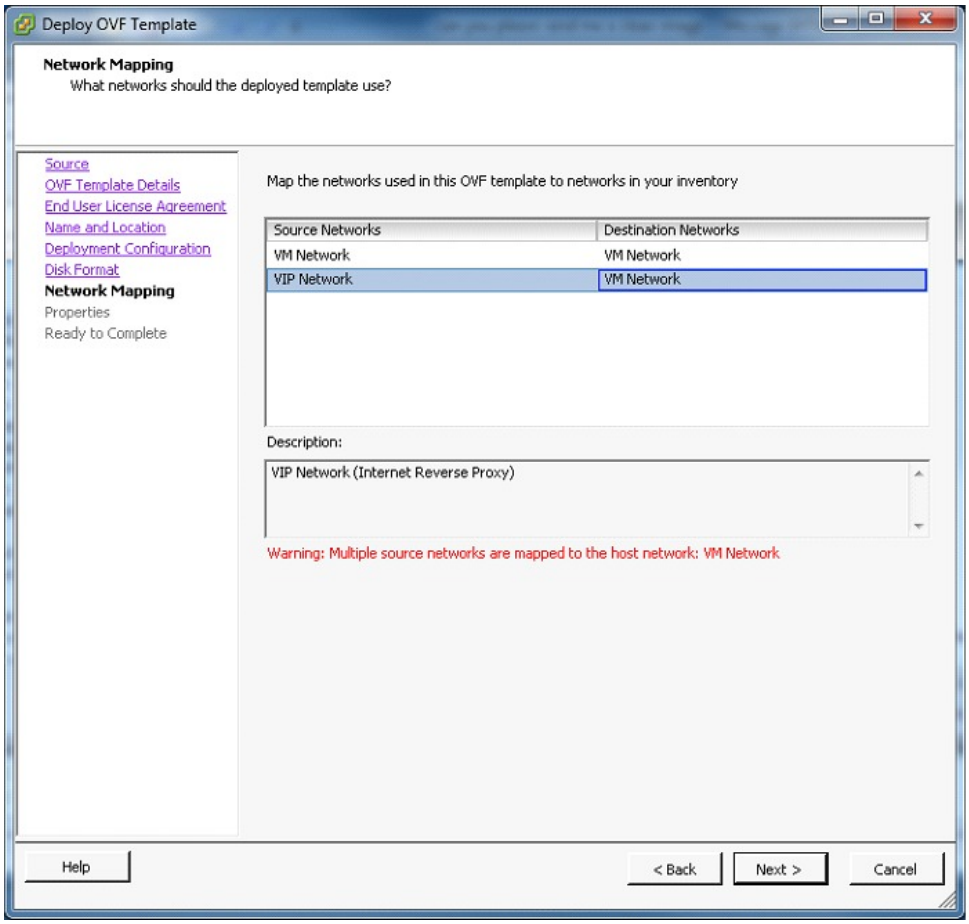
Stap 10 Selecteer de gegevensopslag en het soort provisioning voor uw virtuele machine.
U moet **Thick provisioning** selecteren en ervoor zorgen dat de maximaal vereiste virtuele schijfruimte voor uw systeem beschikbaar is. Met thin provisioning wijst VMware de ruimte van het bestandssysteem toe *op basis van behoefte*. Dit kan tot slechte prestaties leiden. Lazy zero is voldoende en eager zero acceptabel, maar het duurt langer voordat eager zero is voltooid.


Deploy OVF Template
Storage
Where do you want to store the virtual machine files?
Source
OVF Template Details
End User License Agreer
Name and Location
Deployment Configurati
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Select a destination storage for the virtual machine files:
VM Storage Profile:
Name
Drive Ty...
Capacity
Provisio...
Free
Type
Thin Provision...
Access
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 404.50 GB 976.00... 403.55 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 1.63 TB 982.00... 1.63 TB VMFS5 Supported Single ho...
EMC-ORIO... Non-SSD 8.00 TB 18.13 TB 780.95 VMFS5 Supported Multiple ...
EMC-ORIO... Non-SSD 8.00 TB 21.63 TB 1.07 TB VMFS5 Supported Multiple ...
973.00 MB
Disable Storage DRS for this virtual machine
Select a datastore:
Name
Drive Ty...
Capacity
Provisioned
Free
Type
Thin Provisioning
Access
Help
< Back
Next >
Cancel
302873



Stap 11 Netwerktoewijzing instellen. Selecteer een doelnetwerk voor elk bronnetwerk in de vervolgkeuzelijst in de kolom **Destination Networks**. Selecteer **Volgende**.

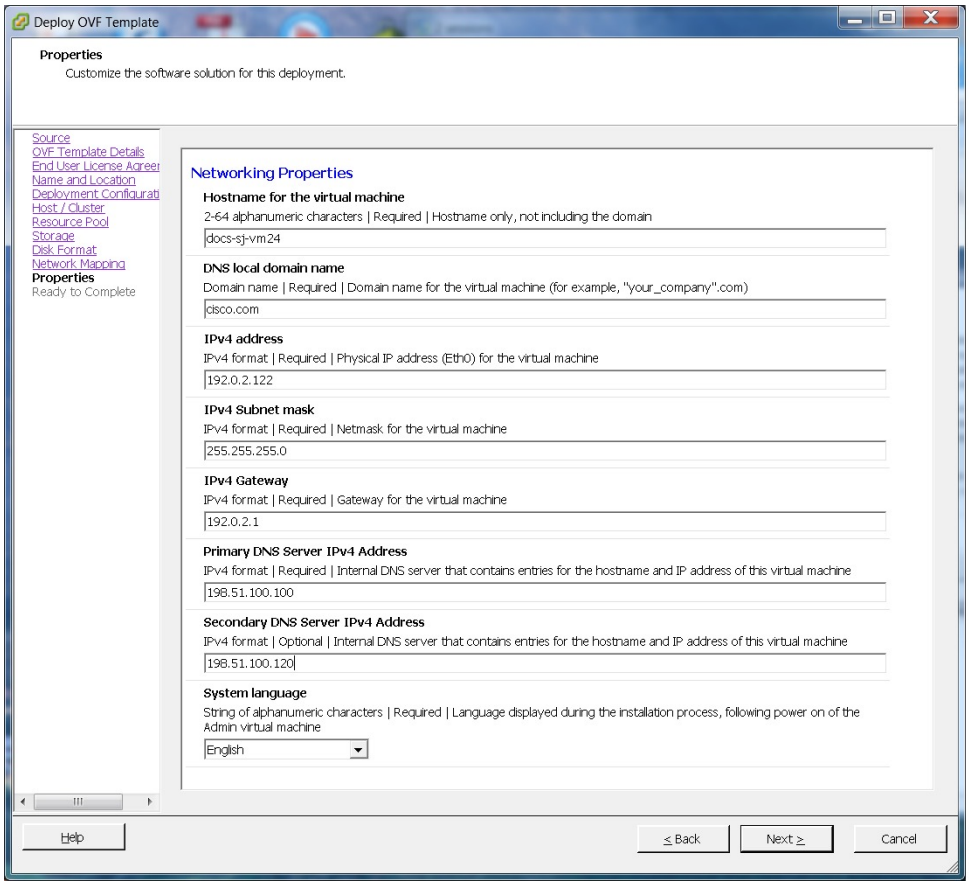
Opmerking Het VM-netwerk en het VIP-netwerk moeten aan dezelfde waarde in de kolom Netwerk worden toegewezen. U kunt het waarschuwingsbericht negeren over netwerken met meerdere bronnen gemapt aan hetzelfde hostnetwerk.



Stap 12 Voer de volgende informatie in voor de virtuele machine en selecteer **Next**:

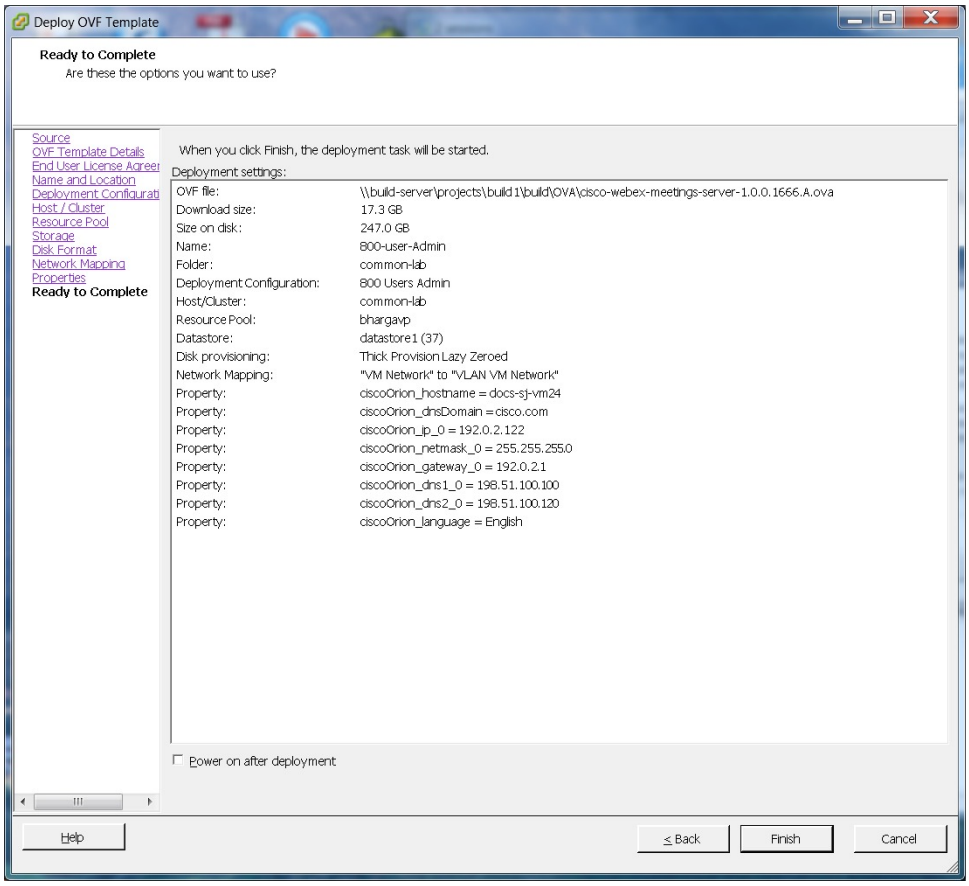
- Hostnaam van de virtuele machine (gebruik hier niet het domein)
- Domein voor de virtuele machine
- IPv4-adres (Eth0) van de virtuele machine
- Subnetmasker van de virtuele machine
- Gateway-IP-adres
- Primaire DNS-server die vermeldingen voor de hostnaam en het IP-adres van deze virtuele machine bevat
- Secundaire DNS-server die vermeldingen voor de hostnaam en het IP-adres van deze virtuele machine bevat
- De taal die tijdens het installatieproces wordt gebruikt nadat de virtuele beheermachine is ingeschakeld

Opmerking Om DNS-problemen te voorkomen, kunt u de URL's en IP-adressen testen voordat u de OVA-implementatie start. Als er fouten optreden, mislukt de implementatie.



Stap 13 Bevestig de informatie die u hebt ingevoerd. Hebt u zich vergist? Selecteer dan **Vorige** en wijzig de waarden.

Stap 14 Schakel het selectievakje **Inschakelen na implementatie** in en selecteer vervolgens **Voltooien**.



Stap 15 Als u een virtuele beheermachine implementeert, gaat u naar vCenter en opent u een consolevenster voor de virtuele machine. Zodra het wordt ingeschakeld, controleren we de netwerkinformatie die u hebt ingevoerd tijdens de OVA-implementatie.

- Als we de verbinding kunnen bevestigen, wordt een groen vinkje weergegeven.
- Als er een probleem optreedt, wordt een rode X weergegeven. Herstel de fout en probeer de OVA-implementatie opnieuw uit te voeren.

Stap 16 Wanneer alle informatie is bevestigd, noteert u de hoofdlettergevoelige URL die in het consolevenster wordt weergegeven.
Een softwarebeheerder typt deze URL in een webbrowser en gaat verder met de systeemimplementatie.

Opmerking Als het systeem opnieuw wordt opgestart voordat de configuratie is voltooid, wordt een nieuwe toegangscode gegenereerd en moet u de URL met de nieuwe toegangscode gebruiken.

Volgende stappen

Als u een handmatige implementatie uitvoert, raadt Cisco u aan om de resterende virtuele machines voor uw systeem op dit moment te implementeren. Hiermee voorkomt u problemen als time-outs bij het inschakelen van virtuele machines.

Als de implementatie is geslaagd, gaat u verder met de systeemimplementatie in een browservenster.

Zie Uw netwerkconfiguratie controleren na een mislukte OVA-implementatie als de implementatie is mislukt.

Uw netwerkconfiguratie controleren na een mislukte OVA-implementatie

Bevestig de netwerkwaarden voor de virtuele machine.

Belangrijk Gebruik niet **Edit Settings...** voor de virtuele machines in uw systeem, behalve na een mislukte implementatie. Zodra het systeem operationeel is, dient u de WebEx-beheerwebsite te gebruiken om verdere wijzigingen aan de instellingen van de virtuele machine door te voeren. Als u gebruikmaakt van uw vSphere Client, worden deze wijzigingen niet aanvaard door het systeem.

Opmerking Raadpleeg uw VMware vSphere-documenten voor gedetailleerde stappen.

Procedure

Stap 1 Selecteer in de vSphere client **Power** > **Shut Down Guest** op de virtuele machine.

Stap 2 Zoek de virtuele machine in de inventaris en klik met de rechtermuisknop op **Edit Settings...**.

Stap 3 Selecteer het tabblad **Options**.

Stap 4 Selecteer **Properties** en bevestig dat alle netwerkinformatie correct is ingevoerd. Als er veranderingen nodig zijn, dient u de OVA opnieuw te implementeren met de juiste instellingen.
Een mogelijke reden van een netwerkprobleem is dat de VLAN-routering niet correct is ingesteld voor de ESXi-host. Omdat de virtuele machine op die VLAN staat, zal de virtuele machine geen netwerkverbinding hebben. Via het netwerk waar de ESXi-host zich bevindt, moet u het IP-adres van de standaard gateway kunnen pingen van de VLAN die u gaat gebruiken voor de virtuele machines in uw systeem.

Uw taal voor installatie selecteren

Bepaal uw voorkeurstaal voor het instellen van het systeem.

Opmerking Sluit dit browservenster niet totdat de systeemimplementatie is voltooid. Als u de browser te vroeg sluit, moet u de implementatie mogelijk opnieuw starten.

Voordat u begint

Zorg dat u de virtuele beheermachine van VMware vCenter hebt geïmplementeerd. Zie Het OVA-bestand van de VMware vSphere-client implementeren, op pagina 16

Procedure

Stap 1 Selecteer de taal in het vervolgkeuzemenu.

Stap 2 Selecteer **Volgende**.

De implementatie bevestigen

Procedure

Stap 1 Geef aan of u een nieuw systeem implementeert of een bestaand systeem uitbreidt.

Stap 2 Selecteer **Volgende**.

De grootte van uw systeem bevestigen

U hebt de grootte van uw systeem geselecteerd toen u de virtuele beheermachine hebt geïmplementeerd met gebruik van het OVA-bestand.

- Bevestig dat de systeemgrootte die u hebt geselecteerd tijdens de OVA-implementatie juist is.
  - Als de systeemgrootte die u hebt geselecteerd juist is, selecteert u **Next**.
  - Als de systeemgrootte die u hebt geselecteerd onjuist is, selecteert u **I want to change System Size**.

a) Selecteer **Power** > **Shut Down Guest** met gebruik van uw VMware vSphere-client voor de virtuele beheermachine met de onjuiste systeemgrootte.
b) Klik met uw rechtermuisknop op de virtuele machine en selecteer **Deleting from Disk**.
c) Implementeer het OVA-bestand opnieuw en selecteer de virtuele beheermachine voor de juiste systeemgrootte.

Kiezen welk systeem u moet installeren

Procedure

Stap 1 Bepaal het type installatie.

- Als u dit systeem voor de eerste keer installeert, kiest u **Install a primary system**.
- Als u al een primair systeem hebt geïnstalleerd en een redundant systeem met hoge beschikbaarheid wilt, kiest u **Create a High Availability (HA) redundant system**.

Opmerking U dient geen HA-systeem te installeren alvorens het primaire systeem te installeren, daar u het HA-systeem niet kunt gebruiken totdat het primaire systeem geïnstalleerd is.

Stap 2 Selecteer **Volgende**.

Het type systeemimplementatie kiezen

Bepaal hoe u elke andere virtuele machine wilt implementeren die vereist is voor uw systeem. Als u een systeem voor 2000 gebruikers hebt geselecteerd, moet u een handmatige implementatie selecteren.

Procedure

Stap 1 Selecteer of u de virtuele machines zelf wilt implementeren of dat wij ze voor u implementeren.

- **Automatisch**: Dit is de snelste installatiemethode. Wij implementeren alle virtuele machines die vereist zijn voor uw systeem.
  Cisco raadt u aan **Automatic** te selecteren tenzij u een systeem met 2000 gebruikers implementeert, wat een handmatige implementatie vereist.

  Opmerking Door Cisco WebEx-beheer te gebruiken, kunt u nog steeds wijzigingen aanbrengen aan uw systeem, na de implementatie.
- **Handmatig**: U moet elke virtuele machine handmatig implementeren met VMware vCenter. Nadat u nog een aantal vragen over uw systeem hebt beantwoord, geven wij een lijst met virtuele machines die vereist zijn voor uw systeem.

Uw beslissing wat betreft automatische of handmatige implementatie hangt af van het volgende:

- Als u tijdsdruk hebt, is een automatische implementatie sneller dan een handmatige implementatie.
- Als u de voorkeur geeft aan stapsgewijze instructies, selecteert u een automatische implementatie.
- Als u bekend bent met VMware vCenter en uw vCenter-gegevens niet wilt verschaffen, selecteer dan handmatige implementatie.

Stap 2 Selecteer **Volgende**.

VMware vCenter-gebruikersgegevens opgeven

Als u voor automatische implementatie kiest, moet u in Cisco WebEx Meetings Server uw vCenter-gebruikersgegevens opgeven om de virtuele machines te laten implementeren.

Voordat u begint

Alle ESXi-hosts van uw systeem moeten bij hetzelfde VMware vCenter horen.

Procedure

Stap 1 Voer de beveiligde https-URL in van het vCenter waarin uw systeem wordt geïmplementeerd.

Stap 2 Voer de gebruikersnaam in die we gebruiken om de virtuele machines te implementeren. De vCenter-gebruiker moet over voldoende beheerdersrechten beschikken om virtuele machines te kunnen implementeren, configureren, in- en uitschakelen en verwijderen.

Stap 3 Voer het wachtwoord van deze gebruiker in.

Stap 4 Selecteer **Volgende**.

vCenter-instellingen voor uw virtuele mediamachine selecteren

De virtuele mediamachine is vereist voor 250 gebruikers en 800 systeemimplementaties van gebruikers.

Procedure

Stap 1 Kies de ESXi-host voor de virtuele mediamachine in de vervolgkeuzelijst.

Stap 2 Kies de gegevensopslag voor de virtuele mediamachine.

Stap 3 Kies de poortgroep van de virtuele machine voor de virtuele mediamachine.
Cisco raadt u aan dezelfde poortgroep te kiezen als de poortgroep die u voor de virtuele beheermachine hebt geselecteerd.

Stap 4 Selecteer **Volgende**.

Netwerkinformatie voor de virtuele mediamachine invoeren

Wanneer de FQDN (Fully Qualified Domain Name) van de virtuele mediamachine is ingevoerd, probeert Cisco WebEx Meetings Server de netwerkinformatie in te vullen.

Opmerking De virtuele mediamachine moet zich op hetzelfde subnet als de virtuele beheermachine bevinden. Bewerk het domein, de IPv4-gateway, het subnetmasker en de DNS-servers van de virtuele mediamachine niet.

Procedure

Stap 1 Voer de FQDN voor de virtuele mediamachine in.
U moet de hostnaam en het IP-adres van de virtuele mediamachine al in uw DNS-servers hebben ingevoerd. Cisco WebEx Meetings Server zoekt het **IPv4-adres** op en vult het in.

Stap 2 Selecteer **Volgende**.

Openbare toegang toevoegen

Als u openbare toegang toevoegt, kunnen gebruikers vergaderingen hosten of bijwonen via internet of mobiele apparaten. Voor aanvullende informatie over het instellen hiervan voor uw bedrijf, raadpleegt u de *Planningshandleiding van Cisco WebEx-vergaderingsserver*.

Opmerking U kunt deze optie altijd wijzigen via de WebEx-beheerwebsite.

Procedure

Stap 1 Kies of externe gebruikers vergaderingen kunnen hosten of bijwonen.

- Als u openbare toegang wilt toevoegen, bevestigt u dat het selectievakje **Create an Internet Reverse Proxy virtual machine** is geselecteerd.
- Als u wilt dat alleen interne gebruikers (achter uw bedrijfsfirewall) vergaderingen hosten of bijwonen, schakelt u het selectievakje **Create an Internet Reverse Proxy virtual machine** uit.

Stap 2 Selecteer **Volgende**.

Volgende stappen

- Met openbare toegang: vCenter-instellingen voor uw Reverse Proxy kiezen, op pagina 32
- Zonder openbare toegang: Het privé-VIP-adres invoeren, op pagina 34

vCenter-instellingen voor uw Reverse Proxy kiezen

Openbare toegang vereist een Reverse Proxy-virtuele machine. Voer de waarden in die u hebt ingevuld in uw installatiecontrolelijst.

Hoewel dit niet verplicht is, raadt Cisco u voor uw veiligheid aan de Reverse Proxy op een ander subnet dan de virtuele beheermachine te plaatsen. Dit maakt het mogelijk een veilig netwerk tot stand te brengen tussen de Reverse proxy en uw interne (beheer en media, indien van toepassing) virtuele machines.

Opmerking Zorg ervoor dat de voor VMware vCenter benodigde firewallpoorten zijn geopend, zodat vCenter de Reverse Proxy-virtuele machine kan implementeren. Voor meer informatie over de benodigde firewallpoorten kunt u de *Planningshandleiding van Cisco WebEx Meetings Server* raadplegen.

Procedure

Stap 1 Kies de ESXi-host voor de Reverse Proxy-virtuele machine in de vervolgkeuzelijst.

Stap 2 Kies de gegevensopslag voor de Reverse Proxy.

Stap 3 Kies de poortgroep van de virtuele machine voor de Reverse Proxy.

Stap 4 Selecteer **Volgende**.

De netwerkinformatie voor de Reverse Proxy-virtuele machine invoeren

Met Reverse Proxy kunnen gebruikers vergaderingen hosten of bijwonen via internet en mobiele apparaten.

Voordat u begint

- Om veiligheidsredenen adviseert Cisco dat u de Reverse Proxy in een ander subnet plaatst dan de virtuele beheermachine.
- Voer de hostnaam en het IP-adres van de Reverse Proxy in uw DNS-servers in om zoekopdrachten vanaf een extern netwerk in te schakelen.

Opmerking Als u DNS-servers hebt die zoekopdrachten vanaf interne netwerken inschakelen, voert u de hostnaam en het IP-adres van de Reverse Proxy ook in deze DNS-servers in. Dit maakt het mogelijk een veilige verbinding tot stand te brengen tussen uw interne virtuele machines (beheer en media, indien van toepassing) en de Reverse Proxy.

- Voer het volgende in voor de Reverse Proxy en selecteer **Next**:
  - Volledige domeinnaam (FQDN)
    U moet de hostnaam en het IP-adres van de Reverse-proxy virtuele mediamachine al in uw DNS-servers hebben ingevoerd. Wij zullen opzoeken en het veld **Ipv4 Address** voor u invullen.
  - IPv4-gateway
  - IPv4-subnetmasker
  - IPv4-adres primaire DNS-server
  - (optioneel) IPv4-adres secundaire DNS-server

Het openbare VIP-adres invoeren

- Dit openbaar VIP-adres moet zichtbaar zijn van zowel het Internet als het interne netwerk (enkel split-horizon DNS).
- Het openbare VIP-adres moet zich op hetzelfde subnet bevinden als de Reverse Proxy-virtuele machine.

- Als u geen split-horizon DNS hebt, gebruiken alle gebruikers het openbare VIP-adres om vergaderingen te hosten en bij te wonen.
- Als u een split-horizon DNS hebt en openbare toegang hebt toegevoegd, gebruiken externe gebruikers het openbare VIP-adres om vergaderingen te hosten en bij te wonen.

Voor meer informatie over DNS zonder split-horizon en met split-horizon en publieke toegang, raadpleegt u de *Planningshandleiding van Cisco WebEx-vergaderingsserver*.

Opmerking Als u een systeem met hoge beschikbaarheid (HA – high availability) maakt, hoeft u deze informatie niet opnieuw in te voeren, omdat we de informatie gebruiken die u voor het primaire systeem hebt ingevoerd.

- Voer het openbare VIP IPv4-adres in en selecteer **Next**.

Het privé-VIP-adres invoeren

Beheerders configureren, controleren en onderhouden het systeem via de URL van de beheerwebsite die wordt gekoppeld aan het persoonlijke VIP-adres.

Opmerking Als u een split horizon DNS hebt, gebruiken interne gebruikers het persoonlijke VIP-adres om vergaderingen te hosten en bij te wonen.

Opmerking Als u een systeem met hoge beschikbaarheid (HA – high availability) toevoegt, hoeft u deze informatie niet opnieuw in te voeren, omdat we de informatie gebruiken die u voor het primaire systeem hebt ingevoerd.

Voordat u begint

Het privé virtuele IP (VIP)-adres moet zich op hetzelfde subnet bevinden als uw interne (beheer en media, indien van toepassing) virtuele machines.

- Voer het openbare privé-VIP-adres van IPv4 in en selecteer **Next**.

URL's van WebEx-site en WebEx-beheer

URL van WebEx-site

Eindgebruikers hebben toegang tot de URL van de WebEx-site om vergaderingen te hosten of bij te wonen. Deze URL verwijst naar het privé-VIP-adres of het openbare VIP-adres, afhankelijk of u wel of niet een split-horizon DNS gebruikt.

- Verwijst naar het openbare VIP-adres voor alle gebruikers, als u geen split-horizon DNS hebt.
- Verwijst naar het openbare VIP-adres voor externe gebruikers als u split-horizon DNS hebt.
- Verwijst naar het privé-VIP-adres voor interne gebruikers als u split-horizon DNS hebt.

URL WebEx-beheer

Beheerders hebben toegang tot de URL van WebEx-beheer om het systeem te configureren, te beheren en te controleren. Deze URL verwijst naar het privé VIP-adres.

Namen voor de URL's van de WebEx-site en WebEx-beheer

U kunt bijna alle namen voor deze URL's kiezen; deze dienen wel uit kleine letters te bestaan. De volgende namen kunt u echter niet als hostnaam in de site-URL's gebruiken:

- dezelfde naam als de hostnamen voor de virtuele machines die deel uitmaken van het systeem
- Verificatie
- client
- bedrijfslogo
- verzender
- Documenten
- elm-admin
- elm-client-services
- E-mailberichten
- Onderhoud
- Manager
- orion
- oriondata
- oriontemp
- NBR
- npp
- probe
- Herinnering
- Root
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- Versie
- WBXService
- WebEx

De URL's van de WebEx-site en –Beheer invoeren

- U kunt de hostnamen van de virtuele machines in uw systeem niet hergebruiken in het hostnaamgedeelte van de URL's van het Beheer of de WebEx-site
- De URL van de WebEx-site Site moet verschillen van de URL van het WebEx-beheer.

Opmerking Als u een systeem met hoge beschikbaarheid (HA – high availability) toevoegt, hoeft u deze informatie niet opnieuw in te voeren, omdat we de informatie gebruiken die u voor het primaire systeem hebt ingevoerd.

- Voer de volgende beveiligde (https) URL's in en selecteer **Next**.
  - URL van de WebEx-site voor gebruikers om vergaderingen te hosten en bij te wonen
  - URL van WebEx-beheer voor systeembeheerders om uw systeem te beheren

Bevestigen dat uw netwerk op de juiste manier is geconfigureerd

Dit scherm bevat koppelingen naar online Help voor de netwerkwijzigingen die vereist zijn voor uw systeem. De online Help bevat informatie over DNS-serverwijziging en firewallinstellingen.

Opmerking U moet de nodige aanpassingen aan uw DNS-server en firewall uitvoeren, omdat wij de netwerkverbinding in de volgende stap zullen testen.

- Als u dit nog niet hebt gedaan, voltooit u de netwerkconfiguratie en selecteert u **Next**.
  Zodra u **Next** selecteert:
  - Automatische implementatie: Wij beginnen met het implementeren van de virtuele machines die vereist zijn voor uw systeem.
  - Handmatige implementatie: Op het volgende scherm voert u de hostnamen in voor uw virtuele machines en implementeert u ze, als u dat nog niet gedaan hebt. Als u ze al hebt geïmplementeerd, schakelt u ze in en controleert u of alle virtuele machines goed opstarten.

Uw virtuele machines implementeren

Gebaseerd op de informatie die u eerder hebt ingevoerd, implementeren wij de virtuele machines die vereist zijn voor uw systeem.

Opmerking De implementatie duurt een paar minuten om te voltooien. Verlaat deze pagina niet totdat alle virtuele machines zijn geïmplementeerd en ingeschakeld, of de implementatie is mislukt en foutberichten het probleem aangeven.

- Voltooi een van de volgende opties
  - Als er geen fouten worden aangetroffen en er allemaal groene vinkjes voor de status worden weergegeven, selecteert u **Volgende**.
  - Als u fouten ziet, herstelt u de fouten en selecteert u **Volgende**.

Opmerking Mogelijk wilt u **Logbestand downloaden** selecteren om het logbestand voor deze implementatie te verkrijgen. Hiermee krijgt u een opname van de implementatie, die u kunt gebruiken om problemen bij een mislukte implementatie op te lossen.

Opmerking Voordat u de implementatie opnieuw uitvoert, moet u virtuele machines met problemen uitschakelen. Anders ziet u mogelijk foutberichten over bestaande virtuele machines wanneer u de systeemimplementatie opnieuw uitvoert.

Uw systeem controleren

Gebaseerd op de informatie die u eerder hebt ingevoerd, controleren wij de configuratie van uw systeem. We bevestigen dat de virtuele machines de vereiste minimale configuratie hebben en we valideren de URL's van de WebEx-site en het WebEx-beheer.

Opmerking De systeemcontrole duurt een paar minuten om te voltooien. Verlaat deze pagina niet totdat alle controles zijn voltooid of de systeemcontrole is mislukt, met foutberichten die het probleem aangeven.

Opmerking Als u de pagina opnieuw laadt voordat de controles zijn voltooid, wordt u terugverwezen naar de eerste pagina van deze systeemimplementatie. Als de controles echter zijn voltooid, wordt u naar de eerste pagina van basisconfiguratie gebracht (waar u de mailserver en een beheerder instelt).

Opmerking De beheersite-URL die wordt gebruikt tijdens het implementatieproces is de hostnaam van de virtuele beheermachine. Tijdens de basisconfiguratie wordt de hostnaam echter vervangen door de daadwerkelijke URL van de beheersite. Als gevolg hiervan is het mogelijk dat het systeem u vraagt de certificaatuitzondering te accepteren wanneer u zich voor de eerste keer aanmeldt bij de beheersite.

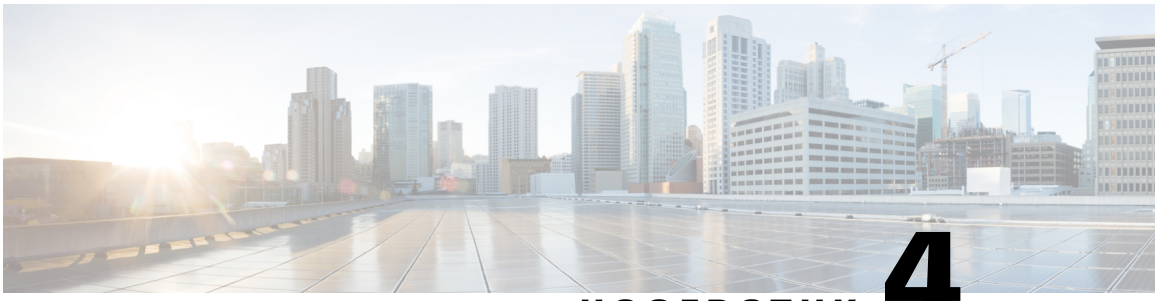
- Voltooi een van de volgende opties:

- Als er geen fouten zijn en de status allemaal groene vinkjes toont, selecteert u **Next**. Doorgaan met De mailserver voor uw systeem instellen, op pagina 65.
- Als er een probleem is met de netwerkverbinding, controleert u of de URL's van uw WebEx-site en –beheer en de IP-adressen juist zijn ingevoerd. Controleer of deze sites zich in het juiste subnet bevinden en juist in uw DNS-servers zijn ingevoerd.
- Als er problemen zijn met uw systeem bij het voldoen aan de minimale systeemcapaciteit, hebt u twee opties.
  - We raden u aan alle virtuele machines van VMware vCenter uit te schakelen en deze handmatig te verwijderen. Probeer vervolgens de systeemimplementatie op een systeem met hulpbronnen die voldoen aan de minimale vereisten of ze overschrijden.
  - U kunt ervoor kiezen om verder te gaan met uw huidige installatie. Als u doorgaat, erkent u dat u afstand doet van het recht op technische ondersteuning van Cisco. Bevestig door het selectievakje in het foutbericht aan te vinken en selecteer **Next**.
- Als er andere problemen zijn met een of meer van uw virtuele machines, schakelt u deze virtuele machines uit vanaf VMware vCenter en verwijdert u ze handmatig. Probeer vervolgens de systeemimplementatie opnieuw nadat de problemen zijn opgelost.

Opmerking Voordat u de implementatie opnieuw uitvoert, moet u virtuele machines met problemen uitschakelen. Anders ziet u mogelijk foutberichten over bestaande virtuele machines wanneer u de systeemimplementatie opnieuw uitvoert.

- In zeldzame gevallen kunt u **Not tested** zien.
  Dit betekent niet dat er een probleem is met uw virtuele machines. Dit zegt gewoon dat we de systeemcontroles niet voltooid hebben; bijvoorbeeld vanwege een tijdelijk verlies van netwerkverbinding. Zodra u de implementatie voltooid hebt, kunt u zich aanmelden op de Beheersite en deze bronnen controleren.

- Selecteer **Continue** om naar de eerste pagina van de basisconfiguratie te gaan (waar u de mailserver en een beheerder instelt). Indien een andere beheerder de basisconfiguratie doet, schrijft u deze URL op en verzendt u deze naar de softwarebeheerder.



HOOFDSTUK 4

Uw systeem installeren met handmatige implementatie

- Algemene concepten voor de implementatie van uw systeem, pagina 39
- Installatiechecklist, pagina 40
- Vereiste gegevens voor een handmatige implementatie, pagina 41
- Het OVA-bestand van de VMware vSphere-client implementeren, pagina 43
- Uw taal voor installatie selecteren, pagina 55
- De implementatie bevestigen, pagina 56
- De grootte van uw systeem bevestigen, pagina 56
- Kiezen welk systeem u moet installeren, pagina 56
- Het type systeemimplementatie kiezen, pagina 57
- Openbare toegang toevoegen, pagina 57
- Het openbare VIP-adres invoeren, pagina 58
- Het privé-VIP-adres invoeren, pagina 58
- URL's van WebEx-site en WebEx-beheer, pagina 59
- De URL's van de WebEx-site en –Beheer invoeren, pagina 60
- Bevestigen dat uw netwerk op de juiste manier is geconfigureerd, pagina 61
- Uw virtuele machines implementeren, pagina 61
- Uw systeem controleren, pagina 62

Algemene concepten voor de implementatie van uw systeem

Systeemgroottes

- Systeem voor 50 gelijktijdige gebruikers

- Geschikt voor een bedrijf met 500 tot 1000 werknemers
- Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine en een optionele Reverse Proxy (voor publieke toegang)

- Systeem voor 250 gelijktijdige gebruikers
  - Geschikt voor een bedrijf met 2500 tot 5000 werknemers
  - Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine, een virtuele mediamachine en een optionele Reverse Proxy (voor publieke toegang)

- Systeem voor 800 gelijktijdige gebruikers
  - Geschikt voor een bedrijf met 8000 tot 16.000 werknemers
  - Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine, een virtuele mediamachine en een optionele Reverse Proxy (voor publieke toegang)

- Systeem voor 2000 gelijktijdige gebruikers
  - Geschikt voor een bedrijf met 20.000 tot 40.000 werknemers
  - Primair systeem (zonder hoge beschikbaarheid) bevat een virtuele beheermachine, 3 virtuele mediamachines, 2 webmachines en een optionele Reverse Proxy (voor publieke toegang)

Gebruikte termen tijdens de implementatie

Veldnaam	Beschrijving
URL van WebEx-site	Beveiligde http-URL voor gebruikers om vergaderingen te hosten en bij te wonen.
URL WebEx-beheer	Beveiligde http-URL voor beheerders om het systeem te configureren, controleren en beheren.
Openbaar VIP	IP-adres voor de URL van de WebEx-site
Privé-VIP	• IP-adres voor de URL van de beheersite • Het IP-adres voor de URL van de WebEx-site (alleen voor interne gebruikers, als u een DNS met split-horizon hebt).

Installatiechecklist

Beperking U moet VMware vCenter gebruiken voor het beheren van ESXi-hosts waar het Cisco WebEx Meetings Server-systeem op is geïmplementeerd.

Netwerkwijzigingen

Raadpleeg de toepasselijke netwerkchecklist voor uw implementatie. Er zijn twee overwegingen:

- Publieke toegang: of gebruikers wel of niet buiten uw firewall vergaderingen kunnen hosten of toegang tot vergaderingen kunnen krijgen via internet of mobiele apparaten.

  Cisco beveelt openbare toegang aan, omdat dit tot een betere gebruikerservaring voor uw mobiele werkkrachten leidt.

- Type DNS-instelling in uw bedrijf: DNS met split-horizon of een DNS zonder split-horizon (meest voorkomende DNS-configuratie).

  Voor meer informatie over deze typen DNS-instelling kunt u de *Planningshandleiding van Cisco WebEx-vergaderingsserver* raadplegen.

- Open poort 10200 van op het bureaublad van de beheerder naar de virtuele beheermachine.

  Poort 10200 wordt gebruikt door de webbrowser tijdens de implementatie.

Selecteer de juiste checklist voor uw implementatie:

- Controlelijst netwerken voor een systeem met publieke toegang en zonder split-horizon DNS, op pagina 9
- Controlelijst netwerken voor een systeem zonder openbare toegang, op pagina 10
- Controlelijst netwerken voor een systeem met publieke toegang en split-horizon DNS, op pagina 10

Verplichte gegevens

Opmerking Welke gegevens zijn vereist, is afhankelijk van de implementatie die u uitvoert; een automatische implementatie (ondersteunt 50 gelijktijdige gebruikers, 250 gelijktijdige gebruikers en 800 gelijktijdige gebruikers) of een handmatige implementatie (ondersteunt alle systeemgroottes). Cisco raadt u aan een automatische implementatie te selecteren, tenzij u een systeem met 2000 gebruikers implementeert. In dat geval is een handmatige implementatie vereist. Raadpleeg de toepasselijke koppeling hieronder.

Kies een van de volgende opties voor een controlelijst van de vereiste gegevens voor uw implementatietype:

- Vereiste gegevens voor een automatische implementatie, op pagina 14
- Vereiste gegevens voor een handmatige implementatie, op pagina 41

Vereiste gegevens voor een handmatige implementatie

Bij een handmatige implementatie maakt u alle virtuele machines voor uw systeem aan met de OVA-wizard van uw vSphere-client. Daarna installeert u uw systeem met een handmatige implementatie.

U moet handmatige implementatie kiezen indien u een systeem voor 2000 gebruikers implementeert.

Opmerking Zorg dat u de FQDN's, de IP-adressen, URL's van WebEx-site en beheersite en VIP-adressen van de virtuele machine aan uw DNS-servers toevoegt voordat u het systeem implementeert. Wij gebruiken deze informatie om de netwerkverbinding aan het einde van de implementatie te controleren.

Ter voorkoming van DNS-problemen kunt u wellicht beter deze URL's en IP-adressen testen voordat u de OVA-implementatie start. U kunt deze fouten beter herstellen, anders mislukt de implementatie van het systeem.

Dit zijn de vereiste gegevens voor uw systeem, op volgorde.

Veldnaam	Beschrijving	Waarde voor uw systeem
Openbaar VIP	IP-adres voor de URL van de WebEx-site (toegang voor sitegebruikers om vergaderingen te hosten en bij te wonen)	
Privé-VIP	• IP-adres voor de URL van de beheerwebsite (voor beheerders om het systeem te configureren, controleren en beheren.) • Het IP-adres voor de URL van de WebEx-site (alleen voor interne gebruikers, als u een DNS met split-horizon hebt).	
URL van WebEx-site	Beveiligde http-URL (met alleen kleine letters) voor gebruikers om vergaderingen te hosten en bij te wonen.	
URL WebEx-beheer	Beveiligde http-URL (met alleen kleine letters) voor beheerders om het systeem te configureren, controleren en beheren.	
FQDN voor de interne virtuele machines	Afhankelijk van de systeemgrootte die u hebt geselecteerd, de volledige domeinnaam van de virtuele mediamachines (met alleen kleine letters) en virtuele machines voor media en web.	
(alleen openbare toegang) FQDN voor de Reverse Proxy	Als u van plan bent openbare toegang toe te voegen, moet u de volledige domeinnaam (met alleen kleine letters) van de Reverse Proxy-virtuele machine opgeven.	

Wat moet u nog meer doen

Met deze informatie start u de implementatie van het systeem door de implementatie-URL in te voeren in een browservenster. (De implementatie-URL wordt weergegeven in het consolevenster voor de virtuele beheermachine.)

Opmerking Als het systeem opnieuw is opgestart voordat de configuratie is voltooid, wordt een nieuwe toegangscode gegenereerd en moet u de implementatie-URL gebruiken met de nieuwe toegangscode.

Het OVA-bestand van de VMware vSphere-client implementeren

Voordat u uw systeem implementeert, moet u de VMware vSphere-client gebruiken om de virtuele beheermachine voor uw systeem te implementeren.

Opmerking De volgende procedure wordt verstrekt als algemene handleiding. Welke schermen precies worden weergegeven tijdens de OVA-implementatie, is afhankelijk van uw vCenter-, opslag- en netwerkconfiguratie. Dit kan enigszins afwijken van deze procedure. Bekijk uw VMware vSphere-documentatie voor volledige informatie over de OVA-wizard.

Voordat u begint

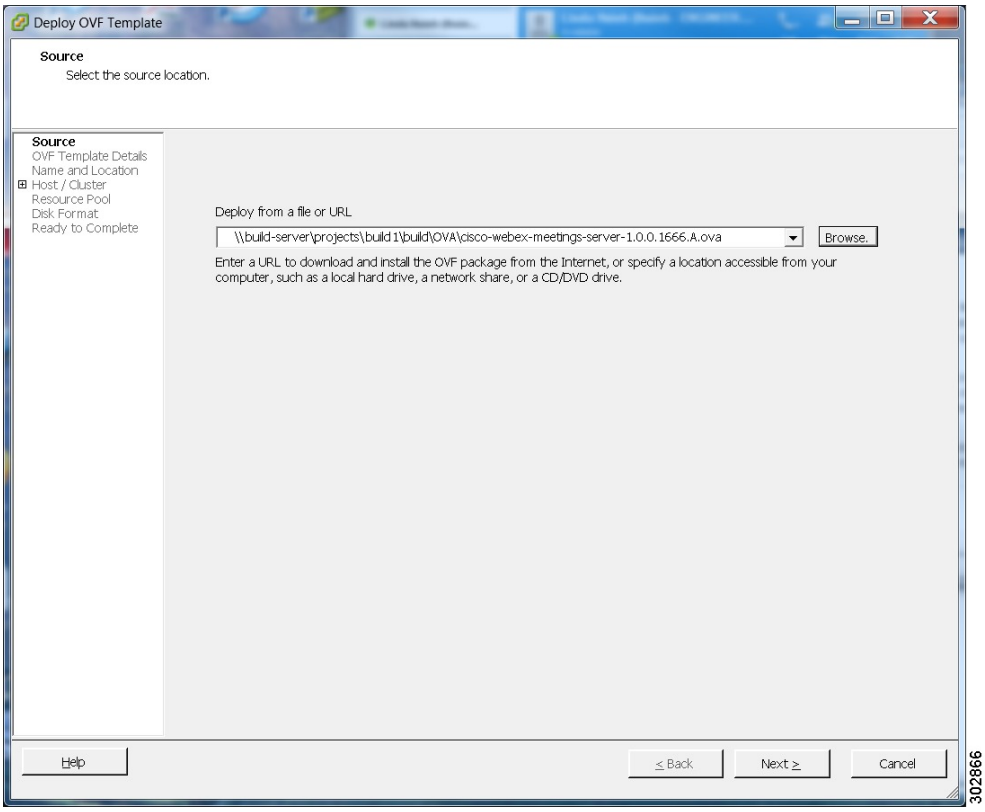
Verkrijg het OVA-bestand van de Cisco WebEx-vergaderingsserver voor uw systeem en plaats het in een locatie die toegankelijk is vanaf VMware vSphere.

U moet VMware vCenter gebruiken voor het beheren van ESXi-hosts waar het Cisco WebEx Meetings Server-systeem op is geïmplementeerd. Gebruik de vSphere-client om u aan te melden bij vCenter en implementeer het OVA-bestand voor de virtuele beheermachine.

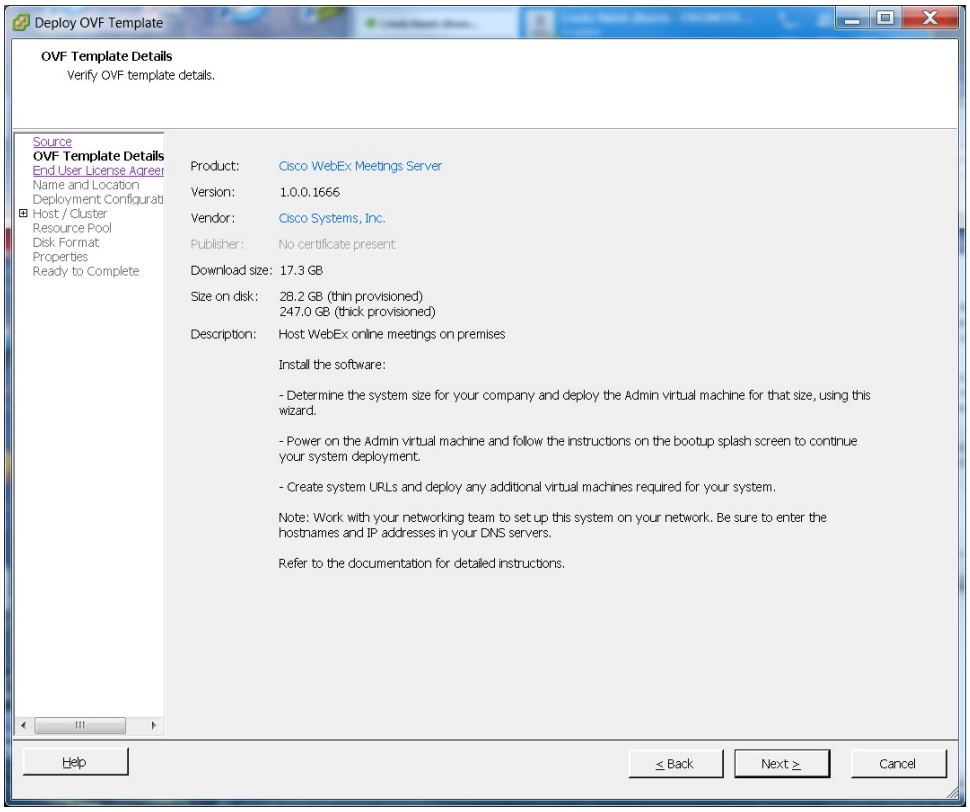
Procedure

Stap 1 Meld u aan bij uw VMware vSphere-client.
Zorg dat u zich als gebruiker met beheerdersrechten aanmeldt: om virtuele machines te gebruiken, configureren, in- of uit te schakelen en te verwijderen.

Stap 2 Selecteer **File** > **Deploy OVF Template...**



Stap 3 Selecteer **Bladeren** om naar de locatie van het OVA-bestand te navigeren. Selecteer **Volgende**.
U kunt op de koppeling **Cisco WebEx Meetings Server** klikken om naar een webpagina met uitgebreide informatie over dit systeem te gaan.



Stap 4 Lees de licentieovereenkomst voor eindgebruikers en selecteer **Accept** en dan **Next**.

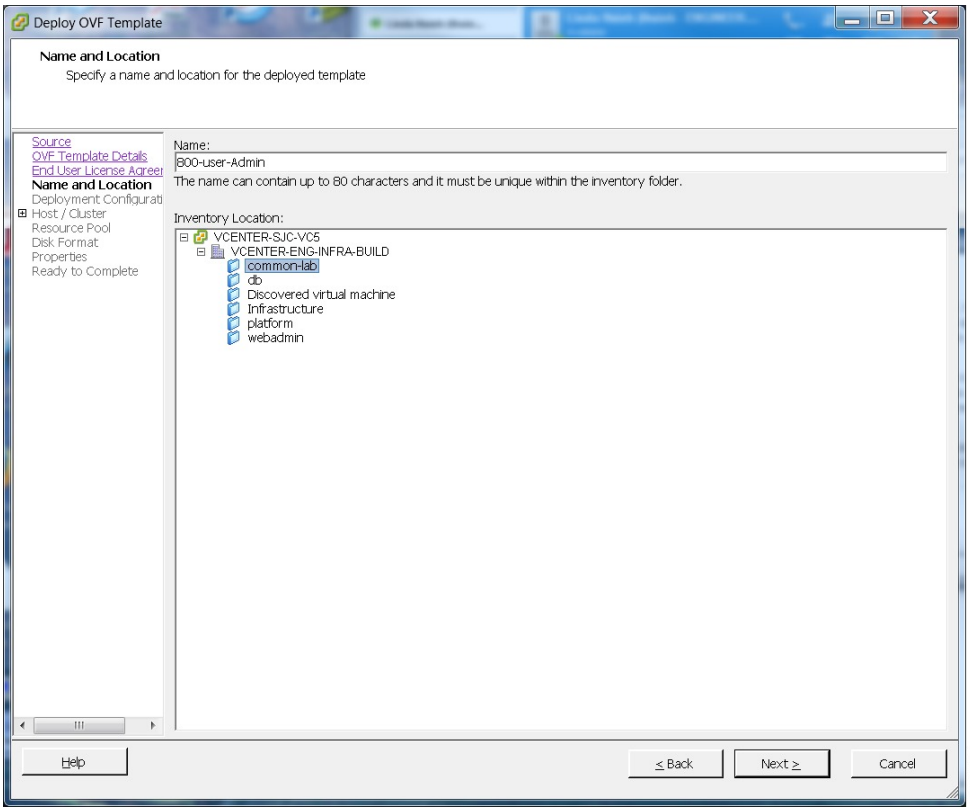
Stap 5 Navigeer in het vCenter-overzicht naar de locatie waar u de virtuele beheermachine wilt plaatsen en selecteer deze locatie.

Stap 6 Voer de naam van de virtuele beheermachine in voor uw systeemgrootte en selecteer **Next**. Zie Systeemgroottes voor meer informatie over het selecteren van de juiste omvang voor uw bedrijf.

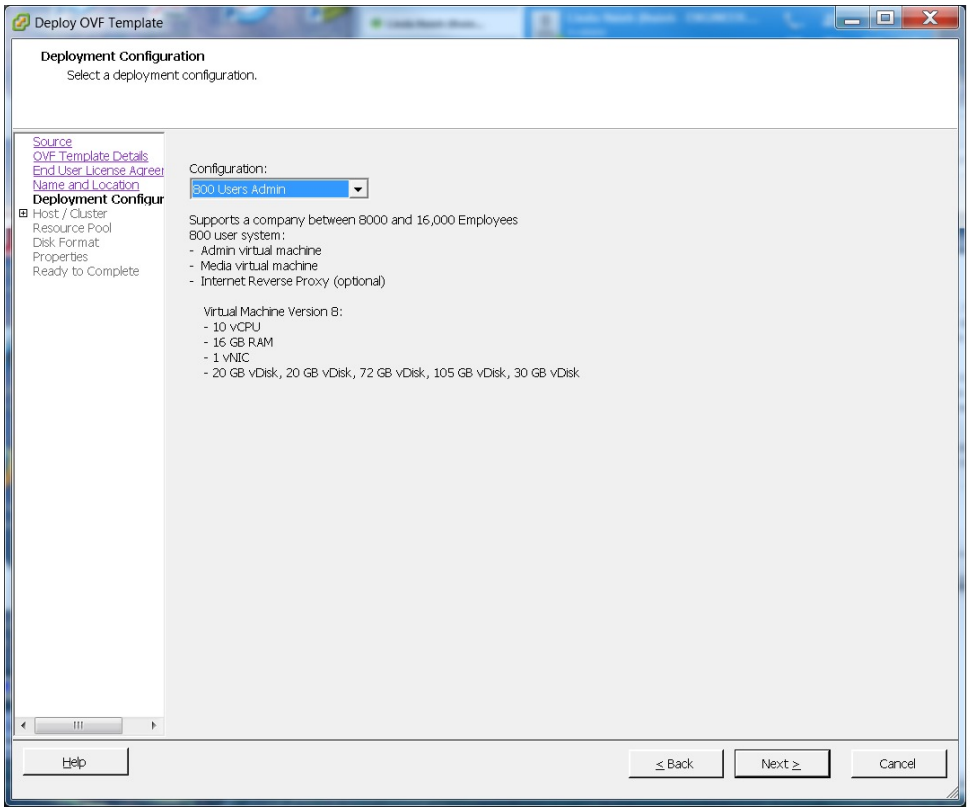
Opmerking U moet de virtuele beheermachine implementeren voordat u de andere virtuele machines implementeert. Als u automatische implementatie selecteert (aanbevolen), implementeren wij de andere virtuele machines voor u. Als u voor handmatige implementatie kiest (verplicht voor systemen met 2000 gelijktijdige gebruikers), moet u met deze wizard de andere virtuele machines implementeren nadat u de virtuele beheermachine hebt geïmplementeerd.

Cisco raadt aan om in de naam van de virtuele machine het type machine te gebruiken (bijvoorbeeld 'beheer' in de naam van de virtuele beheermachine), zodat de machine goed te herkennen is in het vCenter-overzicht.

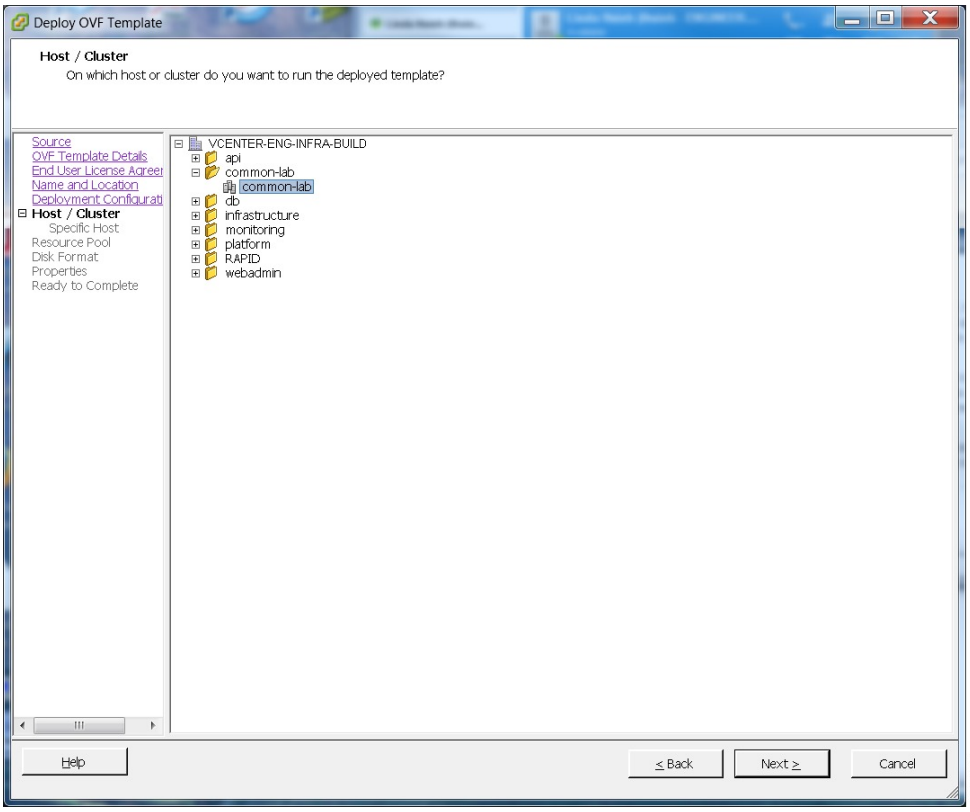
Opmerking Alle interne virtuele machines voor uw systeem moeten zich in hetzelfde subnet bevinden als de virtuele beheermachines. (Afhankelijk van de geselecteerde systeemomvang hebt u mogelijk een of meer interne virtuele machines nodig voor media en het web.)



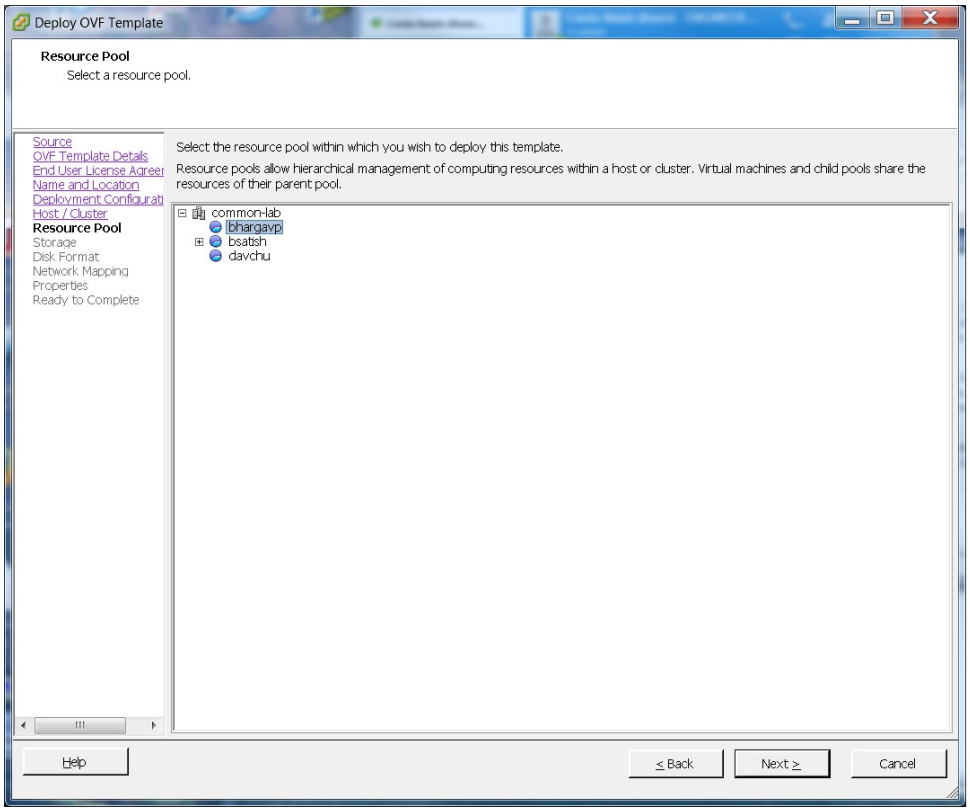
Stap 7 Selecteer in de vervolgkeuzelijst de virtuele machine voor uw systeemomvang en selecteer **Volgende**.
Zorg ervoor dat u de virtuele beheermachine vóór alle andere virtuele machines in uw systeem implementeert.



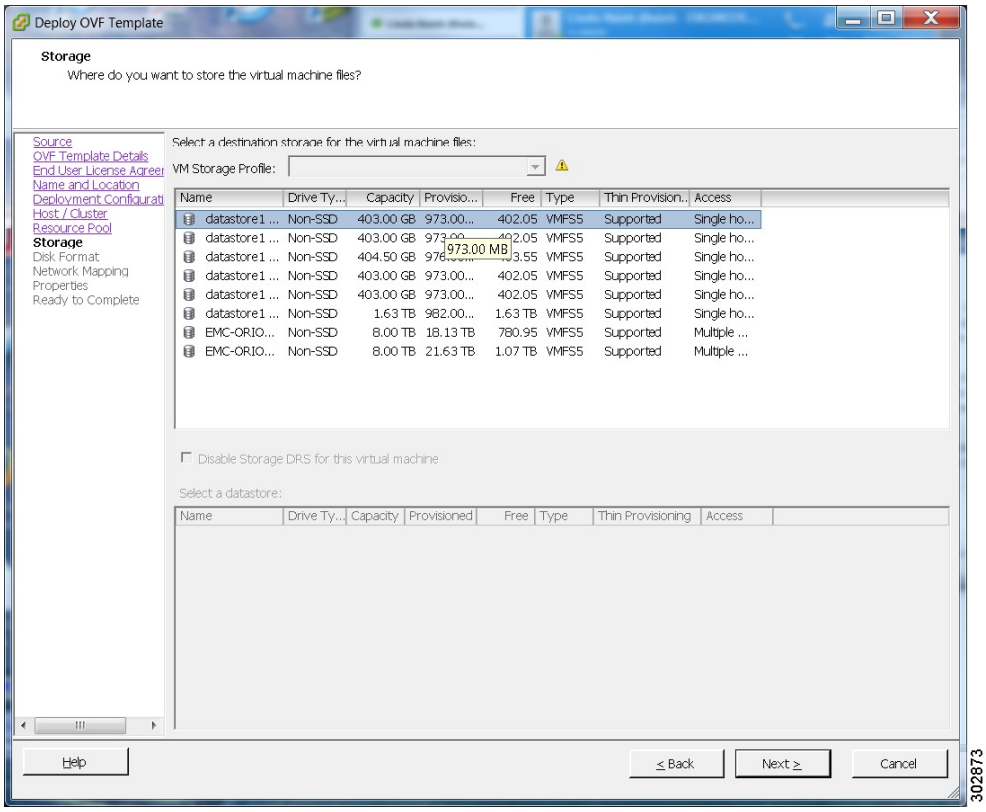
Stap 8 Navigeer door het vCenter-overzicht en selecteer de ESXi-host of het cluster waar u de virtuele machines voor uw systeem wilt implementeren. Selecteer **Volgende**.

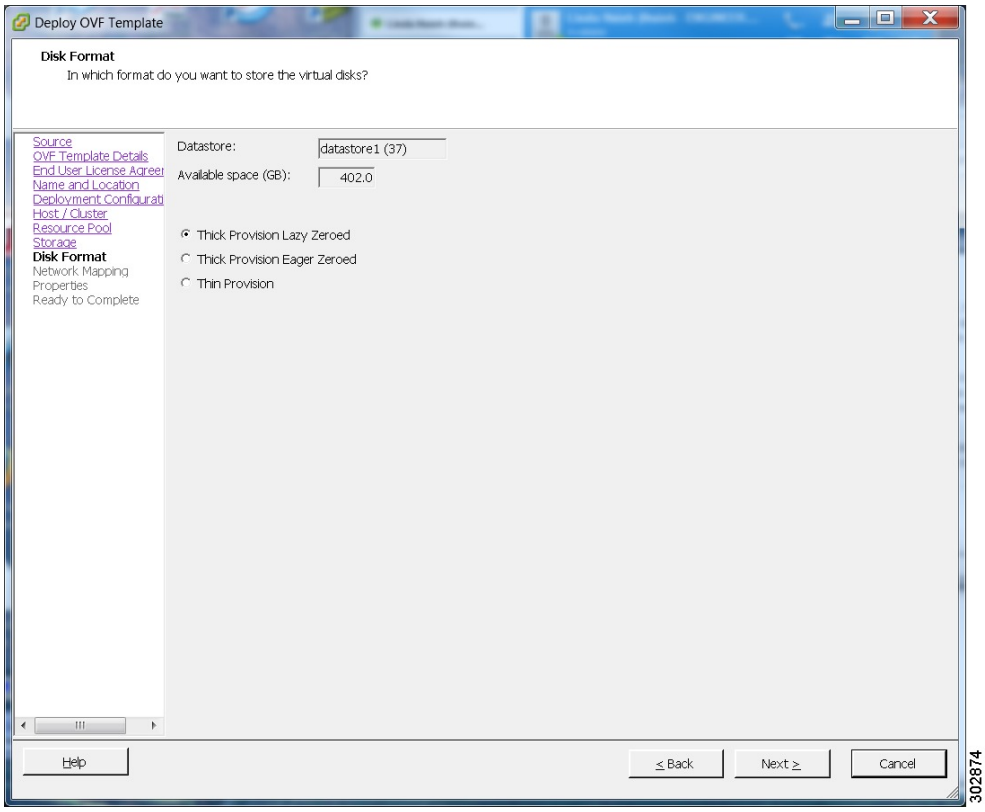


Stap 9 Als het cluster een resource-pool bevat, selecteert u de resource-pool waar u de OVA-sjabloon wilt implementeren en selecteert u **Volgende**.
Resource-pools delen CPU- en geheugenbronnen voor VMware-functies als DRS of vMotion. Resource-pools moeten aan één ESXi-host worden toegewezen. Het is niet raadzaam om resource-pools van VMware te gebruiken met Cisco WebEx Meetings Server.



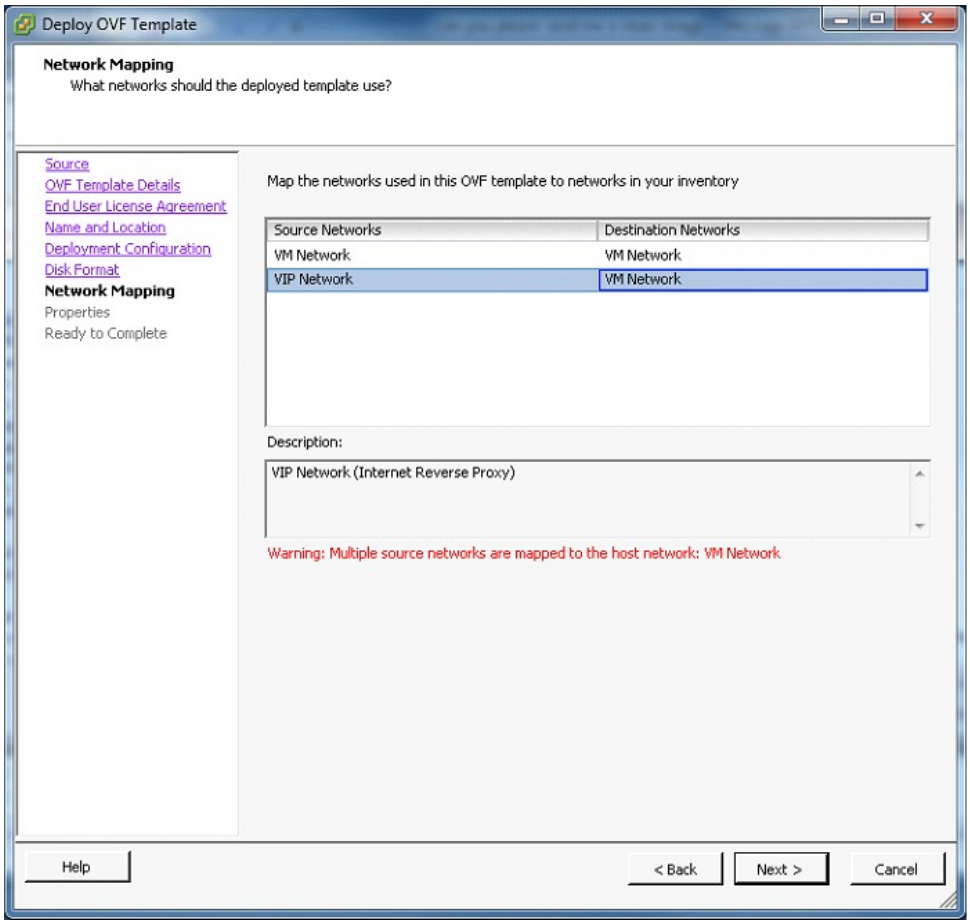
Stap 10 Selecteer de gegevensopslag en het soort provisioning voor uw virtuele machine.
U moet **Thick provisioning** selecteren en ervoor zorgen dat de maximaal vereiste virtuele schijfruimte voor uw systeem beschikbaar is. Met thin provisioning wijst VMware de ruimte van het bestandssysteem toe *op basis van behoefte*. Dit kan tot slechte prestaties leiden. Lazy zero is voldoende en eager zero acceptabel, maar het duurt langer voordat eager zero is voltooid.


Deploy OVF Template
Storage
Where do you want to store the virtual machine files?
Source
OVF Template Details
End User License Agreer
Name and Location
Deployment Configurati
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Select a destination storage for the virtual machine files:
VM Storage Profile:
Name
Drive Ty...
Capacity
Provisio...
Free
Type
Thin Provision...
Access
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 404.50 GB 976.00... 403.55 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 1.63 TB 982.00... 1.63 TB VMFS5 Supported Single ho...
EMC-ORIO... Non-SSD 8.00 TB 18.13 TB 780.95 VMFS5 Supported Multiple ...
EMC-ORIO... Non-SSD 8.00 TB 21.63 TB 1.07 TB VMFS5 Supported Multiple ...
973.00 MB
Disable Storage DRS for this virtual machine
Select a datastore:
Name
Drive Ty...
Capacity
Provisioned
Free
Type
Thin Provisioning
Access
Help
< Back
Next >
Cancel
302873



Stap 11 Netwerktoewijzing instellen. Selecteer een doelnetwerk voor elk bronnetwerk in de vervolgkeuzelijst in de kolom **Destination Networks**. Selecteer **Volgende**.

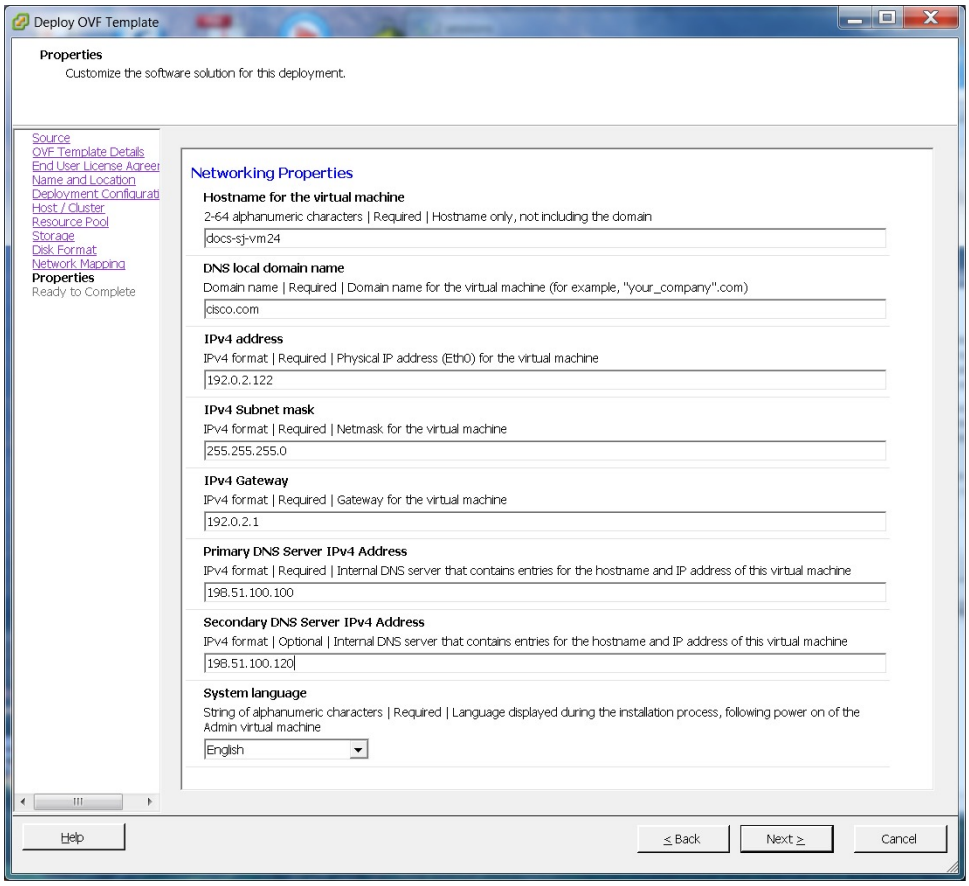
Opmerking Het VM-netwerk en het VIP-netwerk moeten aan dezelfde waarde in de kolom Netwerk worden toegewezen. U kunt het waarschuwingsbericht negeren over netwerken met meerdere bronnen gemapt aan hetzelfde hostnetwerk.



Stap 12 Voer de volgende informatie in voor de virtuele machine en selecteer **Next**:

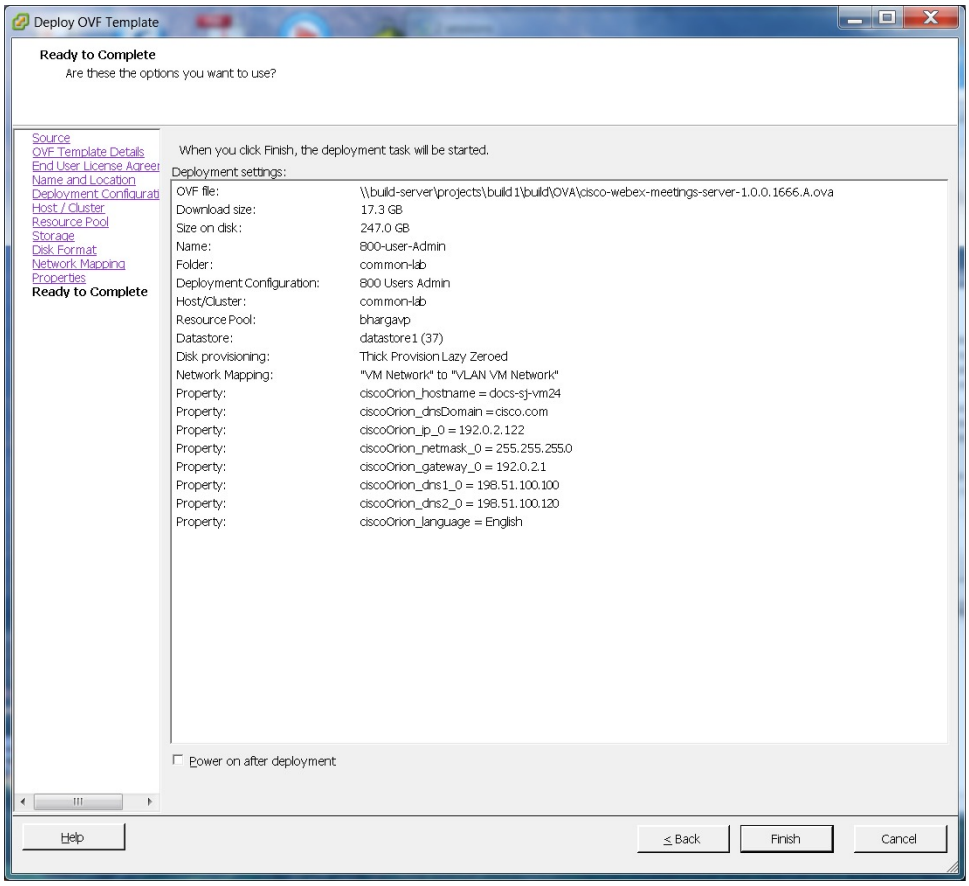
- Hostnaam van de virtuele machine (gebruik hier niet het domein)
- Domein voor de virtuele machine
- IPv4-adres (Eth0) van de virtuele machine
- Subnetmasker van de virtuele machine
- Gateway-IP-adres
- Primaire DNS-server die vermeldingen voor de hostnaam en het IP-adres van deze virtuele machine bevat
- Secundaire DNS-server die vermeldingen voor de hostnaam en het IP-adres van deze virtuele machine bevat
- De taal die tijdens het installatieproces wordt gebruikt nadat de virtuele beheermachine is ingeschakeld

Opmerking Om DNS-problemen te voorkomen, kunt u de URL's en IP-adressen testen voordat u de OVA-implementatie start. Als er fouten optreden, mislukt de implementatie.



Stap 13 Bevestig de informatie die u hebt ingevoerd. Hebt u zich vergist? Selecteer dan **Vorige** en wijzig de waarden.

Stap 14 Schakel het selectievakje **Inschakelen na implementatie** in en selecteer vervolgens **Voltooien**.



Stap 15 Als u een virtuele beheermachine implementeert, gaat u naar vCenter en opent u een consolevenster voor de virtuele machine. Zodra het wordt ingeschakeld, controleren we de netwerkinformatie die u hebt ingevoerd tijdens de OVA-implementatie.

- Als we de verbinding kunnen bevestigen, wordt een groen vinkje weergegeven.
- Als er een probleem optreedt, wordt een rode X weergegeven. Herstel de fout en probeer de OVA-implementatie opnieuw uit te voeren.

Stap 16 Wanneer alle informatie is bevestigd, noteert u de hoofdlettergevoelige URL die in het consolevenster wordt weergegeven.
Een softwarebeheerder typt deze URL in een webbrowser en gaat verder met de systeemimplementatie.

Opmerking Als het systeem opnieuw wordt opgestart voordat de configuratie is voltooid, wordt een nieuwe toegangscode gegenereerd en moet u de URL met de nieuwe toegangscode gebruiken.

Volgende stappen

Als u een handmatige implementatie uitvoert, raadt Cisco u aan om de resterende virtuele machines voor uw systeem op dit moment te implementeren. Hiermee voorkomt u problemen als time-outs bij het inschakelen van virtuele machines.

Als de implementatie is geslaagd, gaat u verder met de systeemimplementatie in een browservenster.

Zie Uw netwerkconfiguratie controleren na een mislukte OVA-implementatie als de implementatie is mislukt.

Uw netwerkconfiguratie controleren na een mislukte OVA-implementatie

Bevestig de netwerkwaarden voor de virtuele machine.

Belangrijk Gebruik niet **Edit Settings...** voor de virtuele machines in uw systeem, behalve na een mislukte implementatie. Zodra het systeem operationeel is, dient u de WebEx-beheerwebsite te gebruiken om verdere wijzigingen aan de instellingen van de virtuele machine door te voeren. Als u gebruikmaakt van uw vSphere Client, worden deze wijzigingen niet aanvaard door het systeem.

Opmerking Raadpleeg uw VMware vSphere-documenten voor gedetailleerde stappen.

Procedure

Stap 1 Selecteer in de vSphere client **Power** > **Shut Down Guest** op de virtuele machine.

Stap 2 Zoek de virtuele machine in de inventaris en klik met de rechtermuisknop op **Edit Settings...**.

Stap 3 Selecteer het tabblad **Options**.

Stap 4 Selecteer **Properties** en bevestig dat alle netwerkinformatie correct is ingevoerd. Als er veranderingen nodig zijn, dient u de OVA opnieuw te implementeren met de juiste instellingen.
Een mogelijke reden van een netwerkprobleem is dat de VLAN-routering niet correct is ingesteld voor de ESXi-host. Omdat de virtuele machine op die VLAN staat, zal de virtuele machine geen netwerkverbinding hebben. Via het netwerk waar de ESXi-host zich bevindt, moet u het IP-adres van de standaard gateway kunnen pingen van de VLAN die u gaat gebruiken voor de virtuele machines in uw systeem.

Uw taal voor installatie selecteren

Bepaal uw voorkeurstaal voor het instellen van het systeem.

Opmerking Sluit dit browservenster niet totdat de systeemimplementatie is voltooid. Als u de browser te vroeg sluit, moet u de implementatie mogelijk opnieuw starten.

Voordat u begint

Zorg dat u de virtuele beheermachine van VMware vCenter hebt geïmplementeerd. Zie Het OVA-bestand van de VMware vSphere-client implementeren, op pagina 16

Procedure

Stap 1 Selecteer de taal in het vervolgkeuzemenu.

Stap 2 Selecteer **Volgende**.

De implementatie bevestigen

Procedure

Stap 1 Geef aan of u een nieuw systeem implementeert of een bestaand systeem uitbreidt.

Stap 2 Selecteer **Volgende**.

De grootte van uw systeem bevestigen

U hebt de grootte van uw systeem geselecteerd toen u de virtuele beheermachine hebt geïmplementeerd met gebruik van het OVA-bestand.

- Bevestig dat de systeemgrootte die u hebt geselecteerd tijdens de OVA-implementatie juist is.
  - Als de systeemgrootte die u hebt geselecteerd juist is, selecteert u **Next**.
  - Als de systeemgrootte die u hebt geselecteerd onjuist is, selecteert u **I want to change System Size**.

a) Selecteer **Power** > **Shut Down Guest** met gebruik van uw VMware vSphere-client voor de virtuele beheermachine met de onjuiste systeemgrootte.
b) Klik met uw rechtermuisknop op de virtuele machine en selecteer **Deleting from Disk**.
c) Implementeer het OVA-bestand opnieuw en selecteer de virtuele beheermachine voor de juiste systeemgrootte.

Kiezen welk systeem u moet installeren

Procedure

Stap 1 Bepaal het type installatie.

- Als u dit systeem voor de eerste keer installeert, kiest u **Install a primary system**.
- Als u al een primair systeem hebt geïnstalleerd en een redundant systeem met hoge beschikbaarheid wilt, kiest u **Create a High Availability (HA) redundant system**.

Opmerking U dient geen HA-systeem te installeren alvorens het primaire systeem te installeren, daar u het HA-systeem niet kunt gebruiken totdat het primaire systeem geïnstalleerd is.

Stap 2 Selecteer **Volgende**.

Het type systeemimplementatie kiezen

Bepaal hoe u elke andere virtuele machine wilt implementeren die vereist is voor uw systeem. Als u een systeem voor 2000 gebruikers hebt geselecteerd, moet u een handmatige implementatie selecteren.

Procedure

Stap 1 Selecteer of u de virtuele machines zelf wilt implementeren of dat wij ze voor u implementeren.

- **Automatisch**: Dit is de snelste installatiemethode. Wij implementeren alle virtuele machines die vereist zijn voor uw systeem.
  Cisco raadt u aan **Automatic** te selecteren tenzij u een systeem met 2000 gebruikers implementeert, wat een handmatige implementatie vereist.

  Opmerking Door Cisco WebEx-beheer te gebruiken, kunt u nog steeds wijzigingen aanbrengen aan uw systeem, na de implementatie.
- **Handmatig**: U moet elke virtuele machine handmatig implementeren met VMware vCenter. Nadat u nog een aantal vragen over uw systeem hebt beantwoord, geven wij een lijst met virtuele machines die vereist zijn voor uw systeem.

Uw beslissing wat betreft automatische of handmatige implementatie hangt af van het volgende:

- Als u tijdsdruk hebt, is een automatische implementatie sneller dan een handmatige implementatie.
- Als u de voorkeur geeft aan stapsgewijze instructies, selecteert u een automatische implementatie.
- Als u bekend bent met VMware vCenter en uw vCenter-gegevens niet wilt verschaffen, selecteer dan handmatige implementatie.

Stap 2 Selecteer **Volgende**.

Openbare toegang toevoegen

Als u openbare toegang toevoegt, kunnen gebruikers vergaderingen hosten of bijwonen via internet of mobiele apparaten. Voor aanvullende informatie over het instellen hiervan voor uw bedrijf, raadpleegt u de *Planningshandleiding van Cisco WebEx-vergaderingsserver*.

Opmerking U kunt deze optie altijd wijzigen via de WebEx-beheerwebsite.

Procedure

Stap 1 Kies of externe gebruikers vergaderingen kunnen hosten of bijwonen.

- Als u openbare toegang wilt toevoegen, bevestigt u dat het selectievakje **Create an Internet Reverse Proxy virtual machine** is geselecteerd.
- Als u wilt dat alleen interne gebruikers (achter uw bedrijfsfirewall) vergaderingen hosten of bijwonen, schakelt u het selectievakje **Create an Internet Reverse Proxy virtual machine** uit.

Stap 2 Selecteer **Volgende**.

Volgende stappen

- Met openbare toegang: vCenter-instellingen voor uw Reverse Proxy kiezen, op pagina 32
- Zonder openbare toegang: Het privé-VIP-adres invoeren, op pagina 34

Het openbare VIP-adres invoeren

- Dit openbaar VIP-adres moet zichtbaar zijn van zowel het Internet als het interne netwerk (enkel split-horizon DNS).
- Het openbare VIP-adres moet zich op hetzelfde subnet bevinden als de Reverse Proxy-virtuele machine.
- Als u geen split-horizon DNS hebt, gebruiken alle gebruikers het openbare VIP-adres om vergaderingen te hosten en bij te wonen.
- Als u een split-horizon DNS hebt en openbare toegang hebt toegevoegd, gebruiken externe gebruikers het openbare VIP-adres om vergaderingen te hosten en bij te wonen.

Voor meer informatie over DNS zonder split-horizon en met split-horizon en publieke toegang, raadpleegt u de *Planningshandleiding van Cisco WebEx-vergaderingsserver*.

Opmerking Als u een systeem met hoge beschikbaarheid (HA – high availability) maakt, hoeft u deze informatie niet opnieuw in te voeren, omdat we de informatie gebruiken die u voor het primaire systeem hebt ingevoerd.

- Voer het openbare VIP IPv4-adres in en selecteer **Next**.

Het privé-VIP-adres invoeren

Beheerders configureren, controleren en onderhouden het systeem via de URL van de beheerwebsite die wordt gekoppeld aan het persoonlijke VIP-adres.

Opmerking Als u een split horizon DNS hebt, gebruiken interne gebruikers het persoonlijke VIP-adres om vergaderingen te hosten en bij te wonen.

Opmerking Als u een systeem met hoge beschikbaarheid (HA – high availability) toevoegt, hoeft u deze informatie niet opnieuw in te voeren, omdat we de informatie gebruiken die u voor het primaire systeem hebt ingevoerd.

Voordat u begint

Het privé virtuele IP (VIP)-adres moet zich op hetzelfde subnet bevinden als uw interne (beheer en media, indien van toepassing) virtuele machines.

- Voer het openbare privé-VIP-adres van IPv4 in en selecteer **Next**.

URL's van WebEx-site en WebEx-beheer

URL van WebEx-site

Eindgebruikers hebben toegang tot de URL van de WebEx-site om vergaderingen te hosten of bij te wonen. Deze URL verwijst naar het privé-VIP-adres of het openbare VIP-adres, afhankelijk of u wel of niet een split-horizon DNS gebruikt.

- Verwijst naar het openbare VIP-adres voor alle gebruikers, als u geen split-horizon DNS hebt.
- Verwijst naar het openbare VIP-adres voor externe gebruikers als u split-horizon DNS hebt.
- Verwijst naar het privé-VIP-adres voor interne gebruikers als u split-horizon DNS hebt.

URL WebEx-beheer

Beheerders hebben toegang tot de URL van WebEx-beheer om het systeem te configureren, te beheren en te controleren. Deze URL verwijst naar het privé VIP-adres.

Namen voor de URL's van de WebEx-site en WebEx-beheer

U kunt bijna alle namen voor deze URL's kiezen; deze dienen wel uit kleine letters te bestaan. De volgende namen kunt u echter niet als hostnaam in de site-URL's gebruiken:

- dezelfde naam als de hostnamen voor de virtuele machines die deel uitmaken van het systeem
- Verificatie
- client
- bedrijfslogo
- verzender
- Documenten
- elm-admin

- elm-client-services
- E-mailberichten
- Onderhoud
- Manager
- orion
- oriondata
- oriontemp
- NBR
- npp
- probe
- Herinnering
- Root
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- Versie
- WBXService
- WebEx

De URL's van de WebEx-site en –Beheer invoeren

- U kunt de hostnamen van de virtuele machines in uw systeem niet hergebruiken in het hostnaamgedeelte van de URL's van het Beheer of de WebEx-site
- De URL van de WebEx-site Site moet verschillen van de URL van het WebEx-beheer.

Opmerking Als u een systeem met hoge beschikbaarheid (HA – high availability) toevoegt, hoeft u deze informatie niet opnieuw in te voeren, omdat we de informatie gebruiken die u voor het primaire systeem hebt ingevoerd.

- Voer de volgende beveiligde (https) URL's in en selecteer **Next**.
  - URL van de WebEx-site voor gebruikers om vergaderingen te hosten en bij te wonen
  - URL van WebEx-beheer voor systeembeheerders om uw systeem te beheren

Bevestigen dat uw netwerk op de juiste manier is geconfigureerd

Dit scherm bevat koppelingen naar online Help voor de netwerkwijzigingen die vereist zijn voor uw systeem. De online Help bevat informatie over DNS-serverwijziging en firewallinstellingen.

Opmerking U moet de nodige aanpassingen aan uw DNS-server en firewall uitvoeren, omdat wij de netwerkverbinding in de volgende stap zullen testen.

- Als u dit nog niet hebt gedaan, voltooit u de netwerkconfiguratie en selecteert u **Next**.
  Zodra u **Next** selecteert:
  - Automatische implementatie: Wij beginnen met het implementeren van de virtuele machines die vereist zijn voor uw systeem.
  - Handmatige implementatie: Op het volgende scherm voert u de hostnamen in voor uw virtuele machines en implementeert u ze, als u dat nog niet gedaan hebt. Als u ze al hebt geïmplementeerd, schakelt u ze in en controleert u of alle virtuele machines goed opstarten.

Uw virtuele machines implementeren

Nadat u informatie over de virtuele machines in het systeem hebt verstrekt, proberen we verbinding te maken met elke virtuele machine die is geïmplementeerd voor uw systeem.

Opmerking Verlaat deze pagina niet totdat het systeem is verbonden met alle virtuele machines of als de verbinding is mislukt en er foutberichten worden weergegeven die het probleem aanduiden.

Procedure

Stap 1 Voer de fully qualified domain names (FSDN's) in voor enige extra virtuele machines vereist voor uw systeem. (U hebt de FQDN van de virtuele beheermachine eerder ingevoerd, toen u het van het OVA-bestand hebt geïmplementeerd.)

Stap 2 Indien u dit nog niet hebt gedaan, moet u alle aanvullende virtuele machines implementeren die vereist zijn voor uw systeem met behulp van VMware vCenter.

Stap 3 Schakel al deze virtuele machines in en controleer of ze allemaal ingeschakeld zijn. Selecteer vervolgens **Detect virtual machines**.
We proberen verbinding te maken met deze virtuele machines. Dit kan enkele minuten in beslag nemen.

Stap 4 Wacht totdat de status **Connected** voor alle virtuele machines wordt weergegeven en voltooi een van de volgende

- Als er geen fouten zijn, toont de status allemaal groene vinkjes. Als u tevreden bent, selecteert u **Next**. U kunt ook nog steeds de FQDN's van de virtuele machines wijzigen, selecteer vervolgens **Detect virtual machines** opnieuw.
- Als u fouten ziet, herstelt u de fouten en selecteert u **Volgende**.

Opmerking Mogelijk wilt u **Logbestand downloaden** selecteren om het logbestand voor deze implementatie te verkrijgen. Hiermee krijgt u een opname van de implementatie, die u kunt gebruiken om problemen bij een mislukte implementatie op te lossen.

- Als er andere problemen zijn met een of meer van uw virtuele machines, schakelt u deze virtuele machines uit vanaf VMware vCenter en verwijdert u ze handmatig. Implementeer na het verhelpen van de problemen de virtuele machines opnieuw vanaf het OVA-bestand en selecteer **Detect virtual machines**.

  Opmerking Voordat u de implementatie opnieuw uitvoert, moet u virtuele machines met problemen uitschakelen. Anders worden er mogelijk foutberichten over bestaande virtuele machines weergegeven.

Uw systeem controleren

Gebaseerd op de informatie die u eerder hebt ingevoerd, controleren wij de configuratie van uw systeem. We bevestigen dat de virtuele machines de vereiste minimale configuratie hebben en we valideren de URL's van de WebEx-site en het WebEx-beheer.

Opmerking De systeemcontrole duurt een paar minuten om te voltooien. Verlaat deze pagina niet totdat alle controles zijn voltooid of de systeemcontrole is mislukt, met foutberichten die het probleem aangeven.

Opmerking Als u de pagina opnieuw laadt voordat de controles zijn voltooid, wordt u terugverwezen naar de eerste pagina van deze systeemimplementatie. Als de controles echter zijn voltooid, wordt u naar de eerste pagina van basisconfiguratie gebracht (waar u de mailserver en een beheerder instelt).

Opmerking De beheersite-URL die wordt gebruikt tijdens het implementatieproces is de hostnaam van de virtuele beheermachine. Tijdens de basisconfiguratie wordt de hostnaam echter vervangen door de daadwerkelijke URL van de beheersite. Als gevolg hiervan is het mogelijk dat het systeem u vraagt de certificaatuitzondering te accepteren wanneer u zich voor de eerste keer aanmeldt bij de beheersite.

- Voltooi een van de volgende opties:
  - Als er geen fouten zijn en de status allemaal groene vinkjes toont, selecteert u **Next**. Doorgaan met De mailserver voor uw systeem instellen, op pagina 65.
  - Als er een probleem is met de netwerkverbinding, controleert u of de URL's van uw WebEx-site en –beheer en de IP-adressen juist zijn ingevoerd. Controleer of deze sites zich in het juiste subnet bevinden en juist in uw DNS-servers zijn ingevoerd.
  - Als er problemen zijn met uw systeem bij het voldoen aan de minimale systeemcapaciteit, hebt u twee opties.

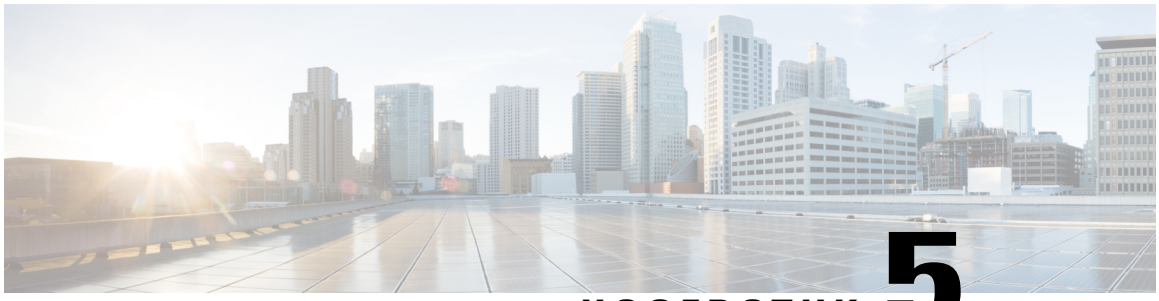
- We raden u aan alle virtuele machines van VMware vCenter uit te schakelen en deze handmatig te verwijderen. Probeer vervolgens de systeemimplementatie op een systeem met hulpbronnen die voldoen aan de minimale vereisten of ze overschrijden.
- U kunt ervoor kiezen om verder te gaan met uw huidige installatie. Als u doorgaat, erkent u dat u afstand doet van het recht op technische ondersteuning van Cisco. Bevestig door het selectievakje in het foutbericht aan te vinken en selecteer **Next**.

- Als er andere problemen zijn met een of meer van uw virtuele machines, schakelt u deze virtuele machines uit vanaf VMware vCenter en verwijdert u ze handmatig. Probeer vervolgens de systeemimplementatie opnieuw nadat de problemen zijn opgelost.

Opmerking Voordat u de implementatie opnieuw uitvoert, moet u virtuele machines met problemen uitschakelen. Anders ziet u mogelijk foutberichten over bestaande virtuele machines wanneer u de systeemimplementatie opnieuw uitvoert.

- In zeldzame gevallen kunt u **Not tested** zien.
  Dit betekent niet dat er een probleem is met uw virtuele machines. Dit zegt gewoon dat we de systeemcontroles niet voltooid hebben; bijvoorbeeld vanwege een tijdelijk verlies van netwerkverbinding. Zodra u de implementatie voltooid hebt, kunt u zich aanmelden op de Beheersite en deze bronnen controleren.

- Selecteer **Continue** om naar de eerste pagina van de basisconfiguratie te gaan (waar u de mailserver en een beheerder instelt). Indien een andere beheerder de basisconfiguratie doet, schrijft u deze URL op en verzendt u deze naar de softwarebeheerder.



HOOFDSTUK 5

Uw mailserver, tijdzone en landinstellingen configureren

- De mailserver voor uw systeem instellen, pagina 65
- De tijdzone en landinstelling voor het systeem instellen, pagina 66
- De mailserver, tijdzone en landinstellingen bevestigen, pagina 66
- Het eerste beheerdersaccount voor uw systeem instellen, pagina 66
- Het systeem testen, pagina 67

De mailserver voor uw systeem instellen

Door deze mailserver in te stellen, kan het systeem uw bedrijfsmailserver gebruiken om e-mails te verzenden naar beheerders (meldingen, alarmen, rapporten, enzovoort) en naar gebruikers (uitnodigingen voor vergaderingen, herstellen van wachtwoord, enzovoort).

Voordat u begint

U moet de implementatie van de virtuele machines die vereist zijn voor uw systeem voltooid hebben.

Procedure

Stap 1 Voer de volledige domeinnaam (FQDN) van een mailserver in die het systeem gebruikt om e-mails te verzenden.

Stap 2 Als u **TLS geactiveerd** wilt, vinkt u dit selectievakje aan.

Stap 3 U kunt het veld **Poort** bewerken als u niet de standaardwaarde wilt gebruiken.
Het standaard SMTP-poortnummer is 25 of 465 (beveiligd SMTP-poortnummer).

Opmerking De knooppunten Web en Beheer verzenden SMTP-verzoeken aan de geconfigureerde mailserver. Als zich tussen de interne virtuele web- en beheermachines en de mailserver een firewall bevindt, kan het SMTP-verkeer worden geblokkeerd. Zorg dat poort 25, of poort 465 (beveiligde SMTP-poort), tussen de mailserver en de virtuele web- en beheermachines open staat voor een goede werking van de mailserverconfiguratie en de e-mailmeldingen.

Stap 4 Als u mailserververificatie wilt inschakelen, vinkt u het selectievakje **Verificatie server geactiveerd** aan.

Als u serververificatie inschakelt, worden de velden **Gebruikersnaam** en **Wachtwoord** weergegeven.

Stap 5 Als deze worden weergegeven, voert u de gegevens **Gebruikersnaam** en **Wachtwoord** voor het systeem in voor toegang tot uw bedrijfsmailserver.
E-mails van het systeem worden verzonden door admin@<WebEx-site-URL>. Zorg ervoor dat de mailserver deze gebruiker herkent.

Stap 6 Selecteer **Volgende**.

De tijdzone en landinstelling voor het systeem instellen

Voordat u begint

Als u Windows 7 gebruikt en uw Cisco WebEx-site hebt geopend in Internet Explorer 10, kan het handig zijn de standaardinstellingen van Internet Explorer 10 voor documenten te selecteren om ervoor te zorgen dat alle knoppen in de toepassing correct werken.

- Selecteer **Hulpmiddelen** > **Ontwikkelhulpprogramma's**.
- Boven in het venster Ontwikkelhulpprogramma's selecteert u **Documentmodus: Standaardinstellingen voor IE7** > **Standaardinstellingen voor Internet Explorer 10**.

Procedure

Stap 1 Selecteer de lokale tijdzone voor uw systeem in de vervolgkeuzelijst.

Stap 2 Selecteer de landinstelling voor uw systeem in de vervolgkeuzelijst.

Stap 3 Selecteer **Volgende**.

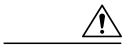
De mailserver, tijdzone en landinstellingen bevestigen

U hebt deze instellingen op de vorige schermen ingevoerd.

- Controleer de informatie die u eerder hebt ingevoerd. Als er fouten zijn, selecteert u **Terug**. Anders selecteert u **Volgende**.

Het eerste beheerdersaccount voor uw systeem instellen

Het systeem maakt één beheerdersaccount als onderdeel van het implementatieproces.



Voorzichtig Deze beheerder moet zich aanmelden bij het systeem, een wachtwoord maken en extra beheerders en gebruikers toevoegen. Anders heeft geen andere gebruiker toegang tot het systeem.

Voordat u begint

U moet een mailserver voor het systeem juist hebben ingesteld om e-mails te verzenden naar beheerders en gebruikers.

Procedure

Stap 1 Voer de voor- en achternamen van de beheerders in.

Stap 2 Voer het volledige e-mailadres van de beheerder in en bevestig dit adres door het opnieuw in te voeren.

Stap 3 Selecteer **Volgende** om een wachtwoord aan te maken.

Stap 4 Voer uw wachtwoord in en bevestig dit wachtwoord door het opnieuw in te voeren.

Stap 5 Selecteer **Verzenden** om u aan te melden bij de WebEx-beheerwebsite.

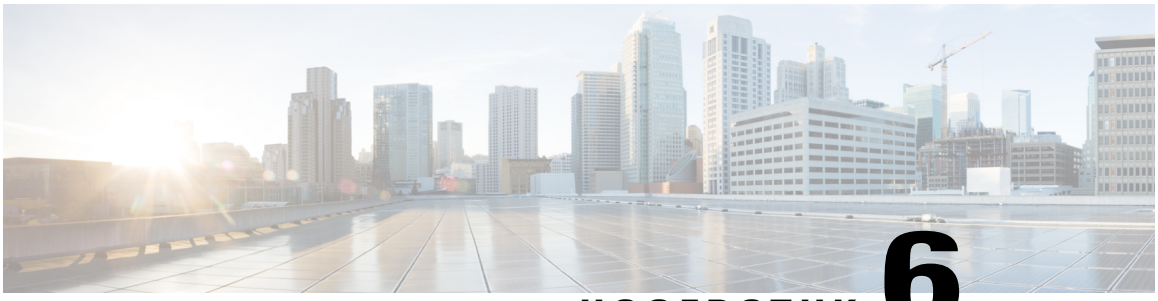
Stap 6 U moet zich aanmelden bij het systeem en extra gebruikers toevoegen. Wanneer de nieuwe gebruiker is gemaakt, verzendt het systeem een e–mail naar elke gebruiker met een welkomstbericht en de vraag of de gebruiker zich wil aanmelden en een wachtwoord wil maken.
Bij de eerste aanmelding heeft iedere beheerder de gelegenheid om een zelfstudie over het systeem te bekijken. De beheerders kunnen de zelfstudie direct bekijken of besluiten om deze later te bekijken.

Het systeem testen

Een aantal van de aanbevolen tests om uit te voeren op het systeem, worden in dit gedeelte vermeld. U kunt deze tests uitvoeren en uw systeem valideren door twee diagnostische hulpmiddelen te gebruiken die u op de ondersteuningspagina's voor dit product vindt: de vergaderingstest en de systeembronnentest.

Wanneer u een geüpgraded systeem test, kunt u het bestaande systeem houden totdat u klaar bent met het testen van het geüpgradede systeem (u kunt beide systemen echter niet gelijktijdig inschakelen). Zodra u tevreden bent met de testresultaten voor het geüpgradede systeem, kunt u het bestaande systeem (voorgoed) verwijderen. Zorg ervoor dat het geüpgradede systeem wordt uitgevoerd wanneer u het bestaande systeem verwijdert of wist. Hiermee voorkomt u dat het VMDK-bestand, waartoe het geüpgradede systeem toegang heeft, onbedoeld wordt verwijderd.

- Gebruikers toevoegen, bewerken, activeren en deactiveren.
- Een vergadering plannen en starten
- Een bestaande vergadering opnieuw plannen.
- Een aantal vergaderingen of een toekomstige vergadering verwijderen.
- Een vergaderingsbijlage openen.
- Een opname van een vergadering afspelen.



HOOFDSTUK 6

Het systeem na de installatie wijzigen

Dit hoofdstuk vermeldt de verschillende systeemwijzigende procedures voor na de initiële implementatie van uw systeem.

- Hoge beschikbaarheid toevoegen, bijwerken, upgraden of het systeem uitbreiden., pagina 69
- Voorbereiden op een systeemwijzigende procedure, pagina 70

Hoge beschikbaarheid toevoegen, bijwerken, upgraden of het systeem uitbreiden.

De volgende procedures worden beschouwd als 'systeemwijzigend' en vereisen voorbereiding door de beheerder:

- Een systeem met hoge beschikbaarheid (HA) toevoegen of verwijderen
- Het systeem bijwerken naar een nieuwere versie door een ISO-updatebestand te gebruiken
- Het systeem upgraden door het systeem opnieuw te implementeren vanuit een OVA-bestand voor de upgradeversie
- De systeemgrootte uitbreiden van de huidige grootte naar een groter formaat

U moet het systeem ook in onderhoudsmodus zetten wanneer u deze procedures uitvoert. Om deze reden wilt u mogelijk een aantal van deze procedures samen plannen; bijvoorbeeld het uitbreiden en bijwerken van het systeem tijdens hetzelfde onderhoudsvenster.

Houd rekening met de volgende beperkingen:

- Als u al hoge beschikbaarheid aan uw systeem hebt toegevoegd en u wilt het systeem uitbreiden of upgraden, moet u het HA-systeem opnieuw implementeren nadat u de upgrade hebt uitgevoerd.

  Systeemuitbreidingen of -upgrades vereisen de implementatie van een nieuw systeem, met de overdracht van de systeemgegevens naar het uitgebreide of bijgewerkte systeem. Wanneer u een nieuw systeem implementeert, wordt u gevraagd te kiezen tussen het implementeren van een primair systeem of het HA-systeem - u kunt ze niet allebei tegelijk implementeren. Daarom moet u eerst het primaire systeem met het OVA-bestand implementeren en dan het HA-systeem met hetzelfde OVA-bestand dat u hebt gebruikt voor het primaire systeem.

- Als u van plan bent een HA-systeem toe te voegen en het bij te werken (met een ISO-updatebestand), raden wij u aan eerst het HA-systeem toe te voegen en dan het gecombineerde (primaire en HA)-systeem bij te werken.

  De updateprocedure werkt het gehele systeem bij, met of zonder een HA-systeem. Als u eerst het systeem bijwerkt en dan HA toevoegt, moet u eerst het HA-systeem implementeren en dan het HA-systeem bijwerken (dus zowel de primaire als de HA-systemen staan op dezelfde versie). Als u eerst HA toevoegt, wordt het gecombineerde primaire en HA-systeem op hetzelfde moment bijgewerkt door de updateprocedure.

- De updateprocedure werkt het gehele systeem bij, met of zonder een Reverse Proxy-server.

Voorbereiden op een systeemwijzigende procedure

Dit gedeelte beschrijft hoe u zich voorbereidt op een grote systeemomvattende procedure: uw systeem uitbreiden, een systeem met hoge beschikbaarheid toevoegen, publieke toegang inschakelen, uw systeem bijwerken of upgraden, enzovoort, door een back-up van uw systeem te maken.

Hoewel u ervoor kunt kiezen om dit wel te doen, hoeft u geen back-up te maken bij een uitbreiding of upgrade van uw systeem. Tijdens een uitbreiding of upgrade implementeert u een nieuw systeem, waarbij u gegevens van uw bestaande systeem naar het nieuwe systeem overbrengt. Als bij de uitbreiding of upgrade een probleem optreedt, kunt u het nieuwe systeem uitschakelen en uw bestaande systeem blijven gebruiken.

Voorzichtig Omdat deze procedure exclusieve toegang tot het systeem vereist, hebben gebruikers geen toegang tot het systeem voor vergaderingen. Zorg ervoor dat u deze procedure plant wanneer het uw gebruikers zo min mogelijk stoort.

Andere systeembeheerders mogen het systeem niet openen tijdens deze procedure. Als dit het geval is, worden de wijzigingen niet opgeslagen en is het resultaat mogelijk onvoorspelbaar. Ze moeten wachten totdat deze procedure is voltooid en zich vervolgens aanmelden bij Cisco WebEx-beheer om hun taak te voltooien.

Opmerking Zorg dat u afspreekt met andere systeembeheerders voordat u een systeemomvattende procedure begint.

Let op Als u geen back-up moet maken van uw virtuele machines, moet u deze procedure niet voltooien. Als een beste praktijk, echter, raadt Cisco aan een back-up te maken. Dankzij back-ups kunt u het systeem herstellen, indien de procedure mislukt is.

Procedure

Stap 1 Meld u aan bij de Cisco WebEx-beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen**.

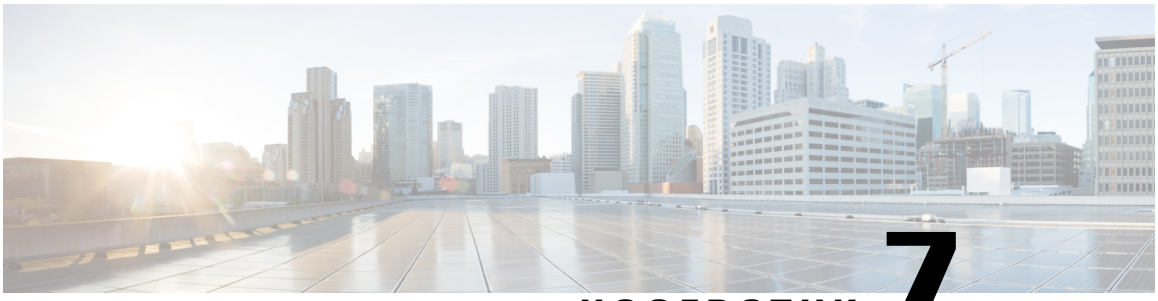
Stap 3 Met VMware-gegevensherstel (vanaf vSphere-release 5.1 VMware vSphere-gegevensbeveiliging genoemd) kunt u een back-up maken van elke virtuele machine.
Met een back-up kunt u uw virtuele machine herstellen naar de staat van vóór de systeemwijzigende procedure. Zie Een back-up maken met VMware vCenter, op pagina 4 voor meer informatie. Zie de *beheerhandleiding*

van VMware-gegevensherstel of de *beheerhandleiding van vSphere-gegevensbeveiliging* voor de complete informatie over deze back-up.

Opmerking Als u een uitbreiding of upgrade voorbereidt, verwijder dan alle VMware-momentopnamen op het bestaande systeem. Hiermee voorkomt u dat het VMDK-basisbestand op harde schijf 4, waartoe het uitgebreide of bijgewerkte systeem toegang heeft, onbedoeld wordt verwijderd.

Stap 4 Meld u weer aan bij de Cisco WebEx-beheersite, maar schakel de onderhoudsmodus niet uit.

Stap 5 Ga door met de systeemwijzigende procedure.



HOOFDSTUK 7

Een systeem met hoge beschikbaarheid toevoegen

- Een systeem met hoge beschikbaarheid toevoegen met automatische implementatie, pagina 73
- Een systeem met hoge beschikbaarheid toevoegen met handmatige implementatie, pagina 76
- Bevestigen dat uw primair systeem en uw HA-systeem dezelfde versie hebben, pagina 78
- Een systeem met hoge beschikbaarheid toevoegen, pagina 79
- Het systeem testen, pagina 80

Een systeem met hoge beschikbaarheid toevoegen met automatische implementatie

Voordat u begint

- U moet het primaire systeem geïmplementeerd hebben.
- Het primaire systeem bevindt zich in de onderhoudsmodus.
- Een back-up maken van zowel de primaire systemen als systemen met hoge beschikbaarheid. Zie Een back-up maken met VMware vCenter, op pagina 4.

Overwegingen voordat u een systeem met hoge beschikbaarheid toevoegt

Een systeem met hoge beschikbaarheid is een redundant systeem dat is toegevoegd aan en deel uitmaakt van uw systeem. Het biedt hoge beschikbaarheid indien er een probleem is met een virtuele machine.

Het systeem met hoge beschikbaarheid bevat de volgende beperkingen

- Het systeem met hoge beschikbaarheid moet dezelfde versie hebben als het primaire systeem.

  Als u het primaire systeem bijgewerkt hebt, moet u ook voor het systeem met hoge beschikbaarheid bijwerken.

- Als u hiertoe gemachtigd bent (met het juiste servicecontract), beveelt Cisco aan dat u het systeem met hoge beschikbaarheid implementeert met het OVA-bestand die dezelfde basisversie is (voor patches) als het primaire systeem.
- De grootte van het systeem met hoge beschikbaarheid moet hetzelfde zijn als het primaire systeem.
- Als u openbare toegang hebt toegevoegd aan het primaire systeem, moet u dit ook toevoegen aan het systeem met hoge beschikbaarheid.
- De interne virtuele machines van het systeem met hoge beschikbaarheid moeten op hetzelfde subnet zitten als de interne virtuele machines van het primaire systeem.
- Als u openbare toegang hebt toegevoegd, moet de Reverse Proxy virtuele machine van het systeem met hoge beschikbaarheid op hetzelfde subnet zitten als de Reverse Proxy virtuele machine van het primaire systeem.
- Aangezien dit proces virtuele machines aan uw systeem toevoegt, wordt uw huidige beveiligingscertificaat ongeldig en is een update nodig, tenzij u een zelfondertekend certificaat gebruikt.
- Als u eerder een systeem met hoge beschikbaarheid hebt gehad, dit hebt verwijderd en een nieuw systeem met hoge beschikbaarheid implementeert, kunt u de virtuele machines in het vorige systeem met hoge beschikbaarheid hergebruiken. U moet een nieuw systeem met hoge beschikbaarheid implementeren met nieuwe virtuele machines.

Opsomming van stappen voor het toevoegen van een systeem met hoge beschikbaarheid met automatische implementatie

Voer deze taken in de aangegeven volgorde uit.

Taak	Beschrijving	Zie
1	Implementeer met de VMware vSphere-client de virtuele beheermachine voor het systeem met hoge beschikbaarheid.	Het OVA-bestand van de VMware vSphere-client implementeren, op pagina 16
2	Schakel de virtuele beheermachine van het systeem met hoge beschikbaar in en schrijf de implementatie-URL op.	
3	Geef de URL op in een webbrowser en ga verder met de implementatie van uw systeem met hoge beschikbaarheid.	
4	Selecteer uw voorkeurstaal voor de implementatie van het systeem met hoge beschikbaar.	Uw taal voor installatie selecteren, op pagina 28
5	Bevestig de systeemgrootte voor het systeem met hoge beschikbaarheid. (Deze systeemgrootte moet overeenkomen met het primaire systeem.)	De grootte van uw systeem bevestigen, op pagina 29
6	Selecteer **Een redundant systeem met hoge beschikbaarheid maken**.	Kiezen welk systeem u moet installeren, op pagina 29
7	Selecteer een automatische implementatie. (Voor het gemak raad Cisco aan om dezelfde selectie te maken als voor uw primaire systeem.)	Het type systeemimplementatie kiezen, op pagina 30

Taak	Beschrijving	Zie
8	Geef uw vCenter-gegevens op zodat we de virtuele machines van het systeem met hoge beschikbaarheid voor u kunnen implementeren.	VMware vCenter-gebruikersgegevens opgeven, op pagina 30
9	Selecteer de ESXi-host, gegevensopslag en de poortgroep voor virtuele machines voor de virtuele mediamachine van het systeem met hoge beschikbaarheid. **Opmerking** Kies dezelfde poortgroep voor virtuele machines als voor het primaire systeem.	vCenter-instellingen voor uw virtuele mediamachine selecteren, op pagina 31
10	Geef indien nodig de volledige domeinnaam op van de virtuele mediamachine van het systeem met hoge beschikbaarheid. (Als u uw DNS-server al hebt bijgewerkt met invoer voor het systeem met hoge beschikbaarheid, zoeken we het IP-adres voor u op.)	Netwerkinformatie voor de virtuele mediamachine invoeren, op pagina 31
11	Als u openbare toegang hebt toegevoegd voor uw primaire systeem, moet u controleren of het selectievakje **Een Reverse Proxy virtuele machine maken** is ingeschakeld. Als u geen openbare toegang hebt toegevoegd, moet u dit selectievakje uitschakelen. **Opmerking** Als u geen openbare toegang hebt ingeschakeld, kunt u verdergaan met Stap 14.	Openbare toegang toevoegen, op pagina 32
12	Als u openbare toegang hebt toegevoegd, moet u de ESXi-host, gegevensopslag en poortgroep voor virtuele machines voor de Reverse Proxy-virtuele machine van het systeem met hoge beschikbaarheid selecteren. **Opmerking** Kies dezelfde poortgroep voor virtuele machines als voor het primaire systeem.	vCenter-instellingen voor uw Reverse Proxy kiezen, op pagina 32
13	Geef de hostnaam en de netwerkinformatie voor de Reverse Proxy-virtuele machine op.	De netwerkinformatie voor de Reverse Proxy-virtuele machine invoeren, op pagina 33
14	Controleer of u alle wijzigingen aan het netwerk, DNS-server en firewallconfiguratie hebt aangebracht die vereist zijn voor uw systeem met hoge beschikbaarheid.	Bevestigen dat uw netwerk op de juiste manier is geconfigureerd, op pagina 36
15	Zodat de virtuele machines van uw systeem met hoge beschikbaarheid zijn geïmplementeerd, moet u **Volgende** selecteren om verder te gaan met de controle van het systeem met hoge beschikbaarheid.	Uw virtuele machines implementeren, op pagina 36
16	Als de controle van het systeem met hoge beschikbaarheid zonder problemen voltooid is, selecteert u **Volgende**.	Uw systeem controleren, op pagina 37

Taak	Beschrijving	Zie
17	Bevestig dat het primaire systeem en het systeem met hoge beschikbaarheid dezelfde versie bevatten. Als dit niet het geval is, moet u het systeem met hoge beschikbaarheid bijwerken.	Bevestigen dat uw primair systeem en uw HA-systeem dezelfde versie hebben, op pagina 78
18	Voeg dit systeem met hoge beschikbaarheid toe aan het primaire systeem in Cisco WebEx-beheer.	Een systeem met hoge beschikbaarheid toevoegen, op pagina 79

Een systeem met hoge beschikbaarheid toevoegen met handmatige implementatie

Voordat u begint

- U moet het primaire systeem geïmplementeerd hebben.
- Het primaire systeem bevindt zich in de onderhoudsmodus.
- Een back-up maken van zowel de primaire systemen als systemen met hoge beschikbaarheid. Zie Een back-up maken met VMware vCenter, op pagina 4.

Overwegingen voordat u een systeem met hoge beschikbaarheid toevoegt

Een systeem met hoge beschikbaarheid is een redundant systeem dat is toegevoegd aan en deel uitmaakt van uw systeem. Het biedt hoge beschikbaarheid indien er een probleem is met een virtuele machine.

Het systeem met hoge beschikbaarheid bevat de volgende beperkingen

- Het systeem met hoge beschikbaarheid moet dezelfde versie hebben als het primaire systeem.

  Als u het primaire systeem bijgewerkt hebt, moet u ook voor het systeem met hoge beschikbaarheid bijwerken.
- Als u hiertoe gemachtigd bent (met het juiste servicecontract), beveelt Cisco aan dat u het systeem met hoge beschikbaarheid implementeert met het OVA-bestand die dezelfde basisversie is (voor patches) als het primaire systeem.
- De grootte van het systeem met hoge beschikbaarheid moet hetzelfde zijn als het primaire systeem.
- Als u openbare toegang hebt toegevoegd aan het primaire systeem, moet u dit ook toevoegen aan het systeem met hoge beschikbaarheid.
- De interne virtuele machines van het systeem met hoge beschikbaarheid moeten op hetzelfde subnet zitten als de interne virtuele machines van het primaire systeem.
- Als u openbare toegang hebt toegevoegd, moet de Reverse Proxy virtuele machine van het systeem met hoge beschikbaarheid op hetzelfde subnet zitten als de Reverse Proxy virtuele machine van het primaire systeem.
- Aangezien dit proces virtuele machines aan uw systeem toevoegt, wordt uw huidige beveiligingscertificaat ongeldig en is een update nodig, tenzij u een zelfondertekend certificaat gebruikt.

- Als u eerder een systeem met hoge beschikbaarheid hebt gehad, dit hebt verwijderd en een nieuw systeem met hoge beschikbaarheid implementeert, kunt u de virtuele machines in het vorige systeem met hoge beschikbaarheid hergebruiken. U moet een nieuw systeem met hoge beschikbaarheid implementeren met nieuwe virtuele machines.

Opsomming van stappen voor het toevoegen van een systeem met hoge beschikbaarheid met handmatige implementatie

Voer deze taken in de aangegeven volgorde uit.

Taak	Beschrijving	Zie
1	Implementeer met de VMware vSphere-client de virtuele beheermachine voor het systeem met hoge beschikbaarheid.	Het OVA-bestand van de VMware vSphere-client implementeren, op pagina 16
2	Schakel de virtuele beheermachine van het systeem met hoge beschikbaar in en schrijf de implementatie-URL op.	
3	Geef de URL op in een webbrowser en ga verder met de implementatie van uw systeem met hoge beschikbaarheid.	
4	Selecteer uw voorkeurstaal voor de implementatie van het systeem met hoge beschikbaar.	Uw taal voor installatie selecteren, op pagina 28
5	Bevestig de systeemgrootte voor het systeem met hoge beschikbaarheid. (Deze systeemgrootte moet overeenkomen met het primaire systeem.)	De grootte van uw systeem bevestigen, op pagina 29
6	Selecteer **Een redundant systeem met hoge beschikbaarheid maken**.	Kiezen welk systeem u moet installeren, op pagina 29
7	Selecteer handmatige implementatie. (Voor het gemak raad Cisco aan om dezelfde selectie te maken als voor uw primaire systeem.)	Het type systeemimplementatie kiezen, op pagina 30
8	Als u openbare toegang hebt toegevoegd voor uw primaire systeem, moet u controleren of het selectievakje **Een Reverse Proxy virtuele machine maken** is ingeschakeld. Als u geen openbare toegang hebt toegevoegd, moet u dit selectievakje uitschakelen.	Openbare toegang toevoegen, op pagina 32
9	Controleer of u alle wijzigingen aan het netwerk, DNS-server en firewallconfiguratie hebt aangebracht die vereist zijn voor uw systeem met hoge beschikbaarheid.	Bevestigen dat uw netwerk op de juiste manier is geconfigureerd, op pagina 36
10	Zodat de virtuele machines van uw systeem met hoge beschikbaarheid zijn geïmplementeerd, moet u **Volgende** selecteren om verder te gaan met de controle van het systeem met hoge beschikbaarheid.	Uw virtuele machines implementeren, op pagina 61
11	Als de controle van het systeem met hoge beschikbaarheid zonder problemen voltooid is, selecteert u **Volgende**.	Uw systeem controleren, op pagina 37

Taak	Beschrijving	Zie
12	Bevestig dat het primaire systeem en het systeem met hoge beschikbaarheid dezelfde versie bevatten. Als dit niet het geval is, moet u het systeem met hoge beschikbaarheid bijwerken.	Bevestigen dat uw primair systeem en uw HA-systeem dezelfde versie hebben, op pagina 78
13	Voeg dit systeem met hoge beschikbaarheid toe aan het primaire systeem in Cisco WebEx-beheer.	Een systeem met hoge beschikbaarheid toevoegen, op pagina 79

Bevestigen dat uw primair systeem en uw HA-systeem dezelfde versie hebben

Het systeem met hoge beschikbaarheid (HA) moet precies dezelfde release zijn als uw primaire systeem. De versie van het systeem met hoge beschikbaarheid wordt op de browserpagina vermeld. Ga als volgt te werk op het primaire systeem om de versie ervan te controleren:

Procedure

Stap 1 Meld u in een afzonderlijk browservenster aan bij de WebEx-beheersite op het primaire systeem.

Stap 2 Controleer op het tabblad **Dashboard** in het deelvenster **Systeem** het versienummer van het primaire systeem.

Stap 3 Als het primaire systeem een nieuwere versie heeft dan het systeem met hoge beschikbaarheid, moet u het systeem met hoge beschikbaarheid bijwerken of opnieuw implementeren met een nieuwer OVA-bestand (voor een nieuwere softwareversie).

Opmerking Maak eerst een back-up van de virtuele machines als u het systeem met hoge beschikbaarheid wilt bijwerken. Zie Een back-up maken met VMware vCenter voor meer informatie.

Stap 4 Als een systeem met hoge beschikbaarheid moet worden bijgewerkt, selecteer dan na het implementeren van dit systeem de optie **Bijwerken** in de browser die met het systeem is verbonden.

Stap 5 Download het desbetreffende updatebestand van Cisco:
Software downloaden

Plaats het updatebestand op een lokale schijf of een gegevensopslag die beschikbaar is voor het HA-systeem.

Stap 6 Selecteer **Doorgaan** in de browser verbonden met het HA-systeem.

Stap 7 Koppel het cd/dvd-station met het ISO-updatebestand in de virtuele beheermachine van het HA-systeem. Zie Verbinding maken met een ISO-image op het cd/dvd-station.

Stap 8 Schakel het selectievakje **Ik heb verbinding gemaakt met het ISO-bestand en ben klaar om door te gaan** in en selecteer **Doorgaan**.

Voorzichtig Zodra u **Doorgaan** selecteert, kunt u de updateprocedure niet stoppen. Als er zich tijdens de updateprocedure een probleem voordoet en de procedure niet wordt voltooid, moet u back-upbestanden gebruiken om het systeem te herstellen.

De updateprocedure kan tot een uur duren. Sluit dit browservenster niet, omdat u dan niet kunt terugkeren naar deze pagina.

Nadat de update is voltooid, wordt een nieuw dialoogvenster weergegeven waarin wordt bevestigd dat de update is geslaagd.

Stap 9 Selecteer **Opnieuw opstarten**.

Nadat het systeem opnieuw is opgestart, wordt de systeempagina weergegeven die door het systeem met hoge beschikbaarheid is gemaakt, waarop wordt aangegeven dat de update is geslaagd.

Volgende stappen

Voeg dit systeem met hoge beschikbaarheid toe aan het primaire systeem in Cisco WebEx-beheer.

Een systeem met hoge beschikbaarheid toevoegen

Opmerking De meeste functies op uw systeem met hoge beschikbaarheid zijn verboden. Zo hebt u bijvoorbeeld geen toegang tot upgrades, SNMP-configuratie, opslagtoegang en e-mailservers op uw systeem met hoge beschikbaarheid. U kunt de systeemeigenschappen bekijken, maar kunt geen wijzigingen aanbrengen.

Opmerking Voltooi de volgende procedure op het primaire systeem.

Voordat u begint

- Installeer Cisco WebEx op een tweede virtuele machine vanuit een OVA-bestand, die u wilt gebruiken als uw systeem met hoge beschikbaarheid.

  Opmerking De grootte van uw systeem met hoge beschikbaarheid moet hetzelfde zijn als het primaire systeem.

- Uw systeem met hoge beschikbaarheid moet worden geconfigureerd met dezelfde OVA en patch als uw primaire systeem. Indien de versies van uw primaire systeem en uw systeem met hoge beschikbaarheid niet overeenstemmen, wordt u gevraagd bij te werken naar het hoogste versieniveau.
- Kopieer de volledige domeinnaam (FQDN) van de virtuele machine met hoge beschikbaarheid. U moet de FQDN hebben om uw systeem met hoge beschikbaarheid toe te voegen.
- Controleer of alle virtuele machines normaal werken. Bepaal de status van de virtuele machine door de systeemmonitor te bekijken zoals beschreven in Informatie over uw dashboard, op pagina 115.
- We raden u aan een momentopname te maken op de virtuele machines met hoge beschikbaarheid voordat u deze procedure uitvoert. Herhaal de procedure vanaf de momentopname indien er een fout optreedt.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen**.

Stap 3 Selecteer de koppeling **Meer weergeven** op het primaire systeem, in de Systeemsectie.

Stap 4 Selecteer **Systeem met hoge beschikbaarheid toevoegen**.

Stap 5 Volg de instructies op de pagina **Systeemeigenschappen** om dit HA-systeem toe te voegen.

Stap 6 Voer de FQDN van de virtuele machine van de beheersite in van de machine met hoge beschikbaarheid en selecteer **Doorgaan**.
We zullen de gereedheid van zowel het primaire systeem als het HA-systeem valideren voor deze HA-toevoeging.

- Als beide systemen klaar zijn, ziet u een groene knop **Toevoegen**. Selecteer niets totdat u uw systeem in de onderhoudsmodus hebt geplaatst.
- Als een systeem niet klaar is, ziet u een foutbericht. Herstel de fout en probeer de procedure voor hoge beschikbaarheid nogmaals toe te voegen.

Stap 7 Selecteer **Toevoegen**.

Opmerking Als de fout 'Foutcode: Database-64' wordt weergegeven, herhaalt u deze procedure met gebruik van de momentopname van de virtuele machines met hoge beschikbaarheid.

Uw systeem met hoge beschikbaarheid wordt toegevoegd en automatisch geconfigureerd om te werken als back-up indien het primaire systeem uitvalt.

Stap 8 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem wordt opnieuw opgestart nadat u de onderhoudsmodus hebt uitgeschakeld. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

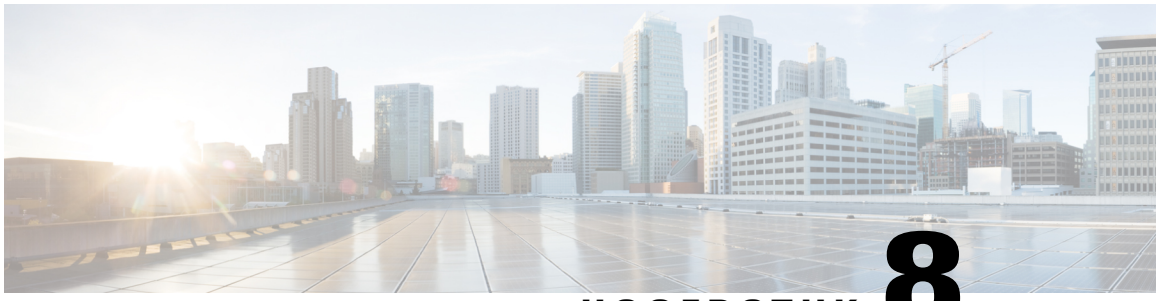
Het systeem testen

Een aantal van de aanbevolen tests om uit te voeren op het systeem, worden in dit gedeelte vermeld. U kunt deze tests uitvoeren en uw systeem valideren door twee diagnostische hulpmiddelen te gebruiken die u op de ondersteuningspagina's voor dit product vindt: de vergaderingstest en de systeembronnentest.

Wanneer u een geüpgraded systeem test, kunt u het bestaande systeem houden totdat u klaar bent met het testen van het geüpgradede systeem (u kunt beide systemen echter niet gelijktijdig inschakelen). Zodra u tevreden bent met de testresultaten voor het geüpgradede systeem, kunt u het bestaande systeem (voorgoed) verwijderen. Zorg ervoor dat het geüpgradede systeem wordt uitgevoerd wanneer u het bestaande systeem verwijdert of wist. Hiermee voorkomt u dat het VMDK-bestand, waartoe het geüpgradede systeem toegang heeft, onbedoeld wordt verwijderd.

- Gebruikers toevoegen, bewerken, activeren en deactiveren.
- Een vergadering plannen en starten
- Een bestaande vergadering opnieuw plannen.
- Een aantal vergaderingen of een toekomstige vergadering verwijderen.

- Een vergaderingsbijlage openen.
- Een opname van een vergadering afspelen.



HOOFDSTUK 8

Uw systeem uitbreiden naar een groter systeemformaat

- Voorbereiden op systeemuitbreiding, pagina 83
- Voorbereiden op een systeemwijzigende procedure, pagina 84
- Het systeem uitbreiden met automatische implementatie, pagina 85
- Het systeem uitbreiden met handmatige implementatie, pagina 89
- Het systeem testen, pagina 94

Voorbereiden op systeemuitbreiding

In dit gedeelte worden de vereisten voor een systeemuitbreiding beschreven.

Voor het uitbreiden van een systeem moeten de bestaande systeemlicenties opnieuw worden geconfigureerd op het uitgebreide systeem. (Zie Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding.)

De omvang van het nieuwe systeem vaststellen

Houd rekening met het volgende:

- Een budget voor aanvullende hardware
- Het verwachte aantal gelijktijdige vergaderingen en de gemiddelde omvang daarvan gedurende de komende paar maanden

De vereiste informatie voor uw systeemuitbreiding verkrijgen

- Verkrijg het OVA-bestand dat is gebruikt om de huidige versie van het systeem te installeren.
- Voltooi de uitbreidingscontrolelijst.

Veldnaam	Huidige waarde voor uw systeem
URL van WebEx-site	

Veldnaam	Huidige waarde voor uw systeem
URL van beheerwebsite	
Persoonlijk VIP-adres	
Openbaar VIP-adres	

Voorbereiden op een systeemwijzigende procedure

Dit gedeelte beschrijft hoe u zich voorbereidt op een grote systeemomvattende procedure: uw systeem uitbreiden, een systeem met hoge beschikbaarheid toevoegen, publieke toegang inschakelen, uw systeem bijwerken of upgraden, enzovoort, door een back-up van uw systeem te maken.

Hoewel u ervoor kunt kiezen om dit wel te doen, hoeft u geen back-up te maken bij een uitbreiding of upgrade van uw systeem. Tijdens een uitbreiding of upgrade implementeert u een nieuw systeem, waarbij u gegevens van uw bestaande systeem naar het nieuwe systeem overbrengt. Als bij de uitbreiding of upgrade een probleem optreedt, kunt u het nieuwe systeem uitschakelen en uw bestaande systeem blijven gebruiken.

Voorzichtig Omdat deze procedure exclusieve toegang tot het systeem vereist, hebben gebruikers geen toegang tot het systeem voor vergaderingen. Zorg ervoor dat u deze procedure plant wanneer het uw gebruikers zo min mogelijk stoort.

Andere systeembeheerders mogen het systeem niet openen tijdens deze procedure. Als dit het geval is, worden de wijzigingen niet opgeslagen en is het resultaat mogelijk onvoorspelbaar. Ze moeten wachten totdat deze procedure is voltooid en zich vervolgens aanmelden bij Cisco WebEx-beheer om hun taak te voltooien.

Opmerking Zorg dat u afspreekt met andere systeembeheerders voordat u een systeemomvattende procedure begint.

Let op Als u geen back-up moet maken van uw virtuele machines, moet u deze procedure niet voltooien. Als een beste praktijk, echter, raadt Cisco aan een back-up te maken. Dankzij back-ups kunt u het systeem herstellen, indien de procedure mislukt is.

Procedure

Stap 1 Meld u aan bij de Cisco WebEx-beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen**.

Stap 3 Met VMware-gegevensherstel (vanaf vSphere-release 5.1 VMware vSphere-gegevensbeveiliging genoemd) kunt u een back-up maken van elke virtuele machine.
Met een back-up kunt u uw virtuele machine herstellen naar de staat van vóór de systeemwijzigende procedure. Zie Een back-up maken met VMware vCenter, op pagina 4 voor meer informatie. Zie de *beheerhandleiding van VMware-gegevensherstel* of de *beheerhandleiding van vSphere-gegevensbeveiliging* voor de complete informatie over deze back-up.

Opmerking Als u een uitbreiding of upgrade voorbereidt, verwijder dan alle VMware-momentopnamen op het bestaande systeem. Hiermee voorkomt u dat het VMDK-basisbestand op harde schijf 4, waartoe het uitgebreide of bijgewerkte systeem toegang heeft, onbedoeld wordt verwijderd.

Stap 4 Meld u weer aan bij de Cisco WebEx-beheersite, maar schakel de onderhoudsmodus niet uit.

Stap 5 Ga door met de systeemwijzigende procedure.

Het systeem uitbreiden met automatische implementatie

Voordat u begint

Opmerking Het systeem vóór de uitbreiding wordt het *originele* systeem genoemd. Het systeem na de uitbreiding is het *uitgebreide* systeem.

Plan een tijd om de systeemuitbreiding uit te voeren waarop het uw gebruikers zo min mogelijk stoort.

Plaats het primaire systeem in onderhoudsmodus voordat u de systeemuitbreiding start.

Voorzichtig Omdat deze procedure exclusieve toegang tot het systeem vereist, hebben gebruikers geen toegang tot het systeem voor vergaderingen. Zorg ervoor dat u deze procedure plant wanneer het uw gebruikers zo min mogelijk stoort.

Coördineer procedures waarbij het systeem wordt gewijzigd vooraf met andere systeembeheerders. Andere systeembeheerders mogen het systeem niet openen tijdens deze procedure. Als u dit niet doet, worden de wijzigingen van de andere beheerders niet opgeslagen, wat tot onvoorspelbare resultaten kan leiden.

Overwegingen vóór uitbreiding van het systeem

- Verwijder alle VMware-momentopnamen van uw originele systeem voordat u de uitbreidingsprocedure start.
- U kunt de hostnamen en IP-adressen van de originele virtuele machines opnieuw gebruiken in het uitgebreide systeem. Er kan echter altijd slechts één systeem, het originele of het uitgebreide, zijn ingeschakeld. De beide systemen kunnen niet tegelijk worden ingeschakeld en uitgevoerd.
- Als het originele systeem een hoge beschikbaarheid had, moet u na de implementatie van het uitgebreide systeem hoge beschikbaarheid aan het uitgebreide systeem toevoegen. U kunt het systeem met hoge beschikbaarheid niet opnieuw gebruiken, omdat het niet behouden blijft bij de uitbreiding.
- U kunt het originele systeem bewaren tot u het testen van het uitgebreide systeem hebt voltooid. Zodra het testen is voltooid en u tevreden bent met het uitgebreide systeem, kunt u het originele systeem (het systeem van vóór de uitbreiding) verwijderen.
- De interne virtuele machines van het originele systeem en het uitgebreide systeem moeten zich op hetzelfde subnet bevinden.
- Als u openbare toegang hebt ingeschakeld, moeten de virtuele Internet Reverse Proxy-machines van het originele systeem en het uitgebreide systeem zich op hetzelfde subnet bevinden.

- Aangezien dit proces virtuele machines aan uw systeem toevoegt, worden uw huidige beveiligingscertificaat, publieke codes en privécodes ongeldig en is een update nodig, tenzij u een zelfondertekend certificaat gebruikt.

  Bij de certificaten zijn de hostnamen en URL's inbegrepen. Het certificaat en de codes worden ongeldig, omdat daarin de nieuwe virtuele machine niet is opgenomen. Zie Certificaten beheren voor uitgebreide informatie over certificaten en sleutels.

- Zorg ervoor dat het uitgebreide systeem toegang heeft tot de schijven van de originele virtuele beheermachine. U kopieert harde schijf 4 naar het uitgebreide systeem.
- Zorg ervoor dat uw uitgebreide systeem actief is wanneer u uw originele systeem verwijdert of wist. Hiermee voorkomt u dat het VMDK-basisbestand op harde schijf 4, waartoe het uitgebreide systeem toegang heeft, onbedoeld kan worden verwijderd.

Het systeem uitbreiden

De algemene taken om het systeem uit te breiden zijn:

1. Maak een back-up van het originele systeem.
2. Gebruik hetzelfde OVA-bestand dat u hebt gebruikt om uw originele systeem te implementeren en implementeer de virtuele beheermachine voor de omvang van het nieuwe systeem.
3. Kopieer de gegevens van uw originele systeem naar de virtuele beheermachine van het uitgebreide systeem.
4. Implementeer zo nodig aanvullende virtuele machines voor de nieuwe systeemgrootte.
5. Test het uitgebreide systeem.
6. Configureer de licenties opnieuw.

Overzicht van de taken om het systeem uit te breiden met een automatische implementatie

Opmerking Deze tabel omvat koppelingen naar andere gedeelten van de beheerhandleiding voor *Cisco WebEx Meetings Server*. Elk van deze gedeelten biedt uitgebreide informatie over de betreffende taak. U dient na voltooiing van elke taak weer terug te gaan naar deze tabel om de volgende taak uit te voeren. (U kunt met Vorige weergave en Volgende weergave in Adobe Acrobat eenvoudig tussen deze tabel en de afzonderlijke taakprocedures schakelen.)

Taak	Beschrijving	Zie
1	Maak het originele systeem gereed voor de uitbreiding.	U hebt deze taak eerder in dit hoofdstuk uitgevoerd. Deze is voor de volledigheid in deze tabel opgenomen.
2	Bereid het systeem voor op een systeemwijzigende procedure.	U hebt deze taak eerder in dit hoofdstuk uitgevoerd. Deze is voor de volledigheid in deze tabel opgenomen.
3	Start de uitbreidingsprocedure vanaf de beheerwebsite van het originele systeem.	Het systeem vergroten

Taak	Beschrijving	Zie
4	Selecteer **In-/uitschakelen** > **Gast afmelden** op de virtuele machines van het bestaande systeem met de VMware vSphere-client.	
5	Implementeer de virtuele beheermachine voor de nieuwe systeemgrootte met de vSphere-client.	Het OVA-bestand van de VMware vSphere-client implementeren, op pagina 16
6	Voeg **harde schijf 4** van de virtuele beheermachine van het originele systeem toe aan de virtuele beheermachine van het uitgebreide systeem.	Een bestaand VMDK-bestand aan een nieuwe virtuele machine koppelen, op pagina 6
7	Schakel de virtuele beheermachine voor het uitgebreide systeem in en noteer de implementatie-URL.	
9	Geef de implementatie-URL op in een webbrowser en ga verder met de implementatie van uw uitgebreide systeem.	
10	Selecteer uw voorkeurstaal voor de implementatie van het uitgebreide systeem.	Uw taal voor installatie selecteren, op pagina 28
11	Bevestig de systeemgrootte. (Dit systeem moet minstens even groot zijn als het originele systeem.)	De grootte van uw systeem bevestigen, op pagina 29
13	Selecteer **Installeer een primair systeem**.	Kiezen welk systeem u moet installeren, op pagina 29
14	Selecteer een automatische implementatie.	Het type systeemimplementatie kiezen, op pagina 30
15	Geef uw vCenter-gegevens op zodat we de virtuele machines voor u kunnen implementeren.	VMware vCenter-gebruikersgegevens opgeven, op pagina 30
16	Selecteer de ESXi-host, gegevensopslag en poortgroep van de virtuele machines voor uw virtuele mediamachine.	vCenter-instellingen voor uw virtuele mediamachine selecteren, op pagina 31
17	Voer de volledige domeinnaam in voor de virtuele mediamachine. (Als u uw DNS-server al hebt bijgewerkt met invoer voor het uitgebreide systeem, zoeken we het IP-adres voor u op.)	Netwerkinformatie voor de virtuele mediamachine invoeren, op pagina 31
18	Als u openbare toegang wilt voor uw uitgebreide systeem, moet u controleren of het selectievakje **Een Reverse Proxy-virtuele machine maken** is ingeschakeld. Als u geen openbare toegang hebt toegevoegd, moet u dit selectievakje uitschakelen. **Opmerking** Ga door naar taak 19 als u geen openbare toegang hebt ingeschakeld.	Openbare toegang toevoegen, op pagina 32

Taak	Beschrijving	Zie
19	Als u openbare toegang hebt ingeschakeld, selecteert u de ESXi-host, de gegevensopslag en de poortgroep van de virtuele machine voor de virtuele Internet Reverse Proxy-machine.	vCenter-instellingen voor uw Reverse Proxy kiezen, op pagina 32
20	Geef de hostnaam en de netwerkinformatie voor de Reverse Proxy-virtuele machine op.	De netwerkinformatie voor de Reverse Proxy-virtuele machine invoeren, op pagina 33
21	Voer het openbare VIP-adres voor de URL van de WebEx-site in. **Opmerking** U kunt hetzelfde openbare VIP-adres invoeren als u voor uw originele systeem gebruikt of een nieuw IP-adres gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server.	Het openbare VIP-adres invoeren, op pagina 33
22	Voer het privé-VIP-adres in voor de URL van WebEx-beheer. **Opmerking** U kunt hetzelfde privé-VIP-adres invoeren als u voor uw originele systeem gebruikt of een nieuw IP-adres gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server.	Het privé-VIP-adres invoeren, op pagina 34
23	Voer de URL van de WebEx-site in. Deelnemers openen deze URL om vergaderingen te hosten en bij te wonen. (Deze URL verwijst naar het persoonlijke VIP-adres of het openbare VIP-adres, afhankelijk of u wel of niet een split-horizon DNS gebruikt.) **Opmerking** U kunt dezelfde site-URL voor WebEx invoeren als u voor uw originele systeem gebruikt of een nieuwe URL gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server. Zorg dat u de URL van uw oorspronkelijke site op de DNS-server behoudt. Leid de URL van de oorspronkelijke site om naar de URL van de nieuwe site. Indien gebruikers de oorspronkelijke URL proberen te gebruiken en u deze niet hebt omgeleid naar de nieuwe URL, kunnen zij geen vergaderingen hosten of bijwonen.	De URL's van de WebEx-site en –Beheer invoeren, op pagina 36

Taak	Beschrijving	Zie
24	Voer de URL van WebEx-beheer in waarmee beheerders Cisco WebEx-beheer kunnen openen en interne deelnemers vergaderingen kunnen hosten of bijwonen (alleen met een split-horizon DNS). (Deze URL verwijst naar het privé-VIP-adres.) **Opmerking** U kunt dezelfde beheer-URL voor WebEx invoeren als u voor uw originele systeem gebruikt of een nieuwe URL gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server.	De URL's van de WebEx-site en –Beheer invoeren, op pagina 36
25	Controleer of u alle wijzigingen aan het netwerk, de DNS-server en de firewallconfiguratie hebt aangebracht die vereist zijn voor uw systeem.	Bevestigen dat uw netwerk op de juiste manier is geconfigureerd, op pagina 36
26	Zodra uw virtuele machines zijn geïmplementeerd, selecteert u **Volgende** om verder te gaan met de controle van het systeem.	Uw virtuele machines implementeren
27	Tijdens de systeemcontrole werken we het uitgebreide systeem bij met eventuele benodigde updates om het systeem af te stemmen op de softwareversie van het originele systeem (het systeem van vóór het uitbreiden). (Deze updates kunnen tot een uur duren.) Als de update voltooid is, start het systeem opnieuw op.	Uw systeem controleren
28	Meld u aan bij Cisco WebEx-beheer.	
29	Test het uitgebreide systeem. Als de uitbreiding niet is geslaagd, schakel dan het uitgebreide systeem uit en het originele systeem in. Neem contact op met de Cisco TAC voor hulp.	Het systeem testen
30	Configureer de licenties opnieuw voor het uitgebreide systeem.	Over licentiesLicenties opnieuw configureren na een software-upgrade of systeemuitbreiding

Het systeem uitbreiden met handmatige implementatie

Voordat u begint

Opmerking Het systeem vóór de uitbreiding wordt het *originele* systeem genoemd. Het systeem na de uitbreiding is het *uitgebreide* systeem.

Plan een tijd om de systeemuitbreiding uit te voeren waarop het uw gebruikers zo min mogelijk stoort.

Plaats het primaire systeem in onderhoudsmodus voordat u de systeemuitbreiding start.

Voorzichtig Omdat deze procedure exclusieve toegang tot het systeem vereist, hebben gebruikers geen toegang tot het systeem voor vergaderingen. Zorg ervoor dat u deze procedure plant wanneer het uw gebruikers zo min mogelijk stoort.

Coördineer procedures waarbij het systeem wordt gewijzigd vooraf met andere systeembeheerders. Andere systeembeheerders mogen het systeem niet openen tijdens deze procedure. Als u dit niet doet, worden de wijzigingen van de andere beheerders niet opgeslagen, wat tot onvoorspelbare resultaten kan leiden.

Overwegingen vóór uitbreiding van het systeem

- Verwijder alle VMware-momentopnamen van uw originele systeem voordat u de uitbreidingsprocedure start.
- U kunt de hostnamen en IP-adressen van de originele virtuele machines opnieuw gebruiken in het uitgebreide systeem. Er kan echter altijd slechts één systeem, het originele of het uitgebreide, zijn ingeschakeld. Beide systemen kunnen niet tegelijk worden ingeschakeld en uitgevoerd.
- Als u al een systeem met hoge beschikbaarheid aan uw originele systeem hebt toegevoegd, moet u na de implementatie van het uitgebreide systeem een nieuw systeem met hoge beschikbaarheid toevoegen. U kunt het originele systeem met hoge beschikbaarheid niet opnieuw gebruiken, omdat het niet behouden blijft bij de uitbreiding.
- Mogelijk wilt u het originele systeem houden tot u het testen van het uitgebreide systeem hebt voltooid. Zodra het testen is voltooid en u tevreden bent met het uitgebreide systeem, kunt u het originele systeem (het systeem van vóór de uitbreiding) verwijderen.
- De interne virtuele machines van het originele systeem en het uitgebreide systeem moeten zich op hetzelfde subnet bevinden.
- Als u openbare toegang hebt ingeschakeld, moeten de virtuele Internet Reverse Proxy-machines van het originele systeem en het uitgebreide systeem zich op hetzelfde subnet bevinden.
- Aangezien dit proces virtuele machines aan uw systeem toevoegt, worden uw huidige beveiligingscertificaat, publieke codes en privécodes ongeldig en is een update nodig, tenzij u een zelfondertekend certificaat gebruikt.

  Bij de certificaten zijn de hostnamen en URL's inbegrepen. Het certificaat en de codes worden ongeldig, omdat daarin de nieuwe virtuele machine niet is opgenomen. Zie Certificaten beheren, op pagina 226 voor de complete informatie over certificaten en codes.
- Zorg ervoor dat het uitgebreide systeem toegang heeft tot de schijven van de virtuele beheermachine van het originele systeem. U kopieert harde schijf 4 naar het uitgebreide systeem.
- Zorg ervoor dat uw uitgebreide systeem actief is wanneer u uw originele systeem verwijdert of wist. Hiermee voorkomt u dat het VMDK-basisbestand op harde schijf 4, waartoe het uitgebreide systeem toegang heeft, onbedoeld wordt verwijderd.

Het systeem uitbreiden

De algemene taken om het systeem uit te breiden zijn:

1. Maak een back-up van uw originele systeem.
2. Gebruik hetzelfde OVA-bestand dat u hebt gebruikt om uw originele systeem te implementeren en implementeer de virtuele beheermachine voor de omvang van het nieuwe systeem.

3 Kopieer de gegevens van uw originele systeem naar de virtuele beheermachine van het uitgebreide systeem.

4 Implementeer met behulp van de OVA extra virtuele machines voor de nieuwe systeemgrootte.

5 Test het uitgebreide systeem.

6 Configureer de licenties opnieuw.

Samenvatting van taken om het systeem uit te breiden met behulp van een handmatige implementatie

Opmerking Deze tabel omvat koppelingen naar andere gedeelten van de beheerhandleiding voor *Cisco WebEx Meetings Server*. Elk van deze gedeelten biedt uitgebreide informatie over de betreffende taak. U dient na voltooiing van elke taak weer terug te gaan naar deze tabel om de volgende taak uit te voeren. (U kunt met Vorige weergave en Volgende weergave in Adobe Acrobat eenvoudig tussen deze tabel en de afzonderlijke taakprocedures schakelen.)

Taak	Beschrijving	Zie
1	Maak het originele systeem gereed voor de uitbreiding.	U hebt deze taak eerder in dit hoofdstuk uitgevoerd. Deze is voor de volledigheid in deze tabel opgenomen.
2	Bereid het systeem voor op een systeemwijzigende procedure.	U hebt deze taak eerder in dit hoofdstuk uitgevoerd. Deze is voor de volledigheid in deze tabel opgenomen.
3	Start de uitbreidingsprocedure vanaf de beheerwebsite van het originele systeem.	Het systeem vergroten
4	Selecteer **In-/uitschakelen** > **Gast afmelden** op de virtuele machines van het bestaande systeem met de VMware vSphere-client.	
5	Implementeer de virtuele beheermachine voor de nieuwe systeemgrootte met de vSphere-client. **Opmerking** Op dit tijdstip kunt u tevens de overige virtuele machines voor uw systeem maken.	Het OVA-bestand van de VMware vSphere-client implementeren, op pagina 16
6	Voeg **harde schijf 4** van de virtuele beheermachine van het originele systeem toe aan de virtuele beheermachine van het uitgebreide systeem.	Een bestaand VMDK-bestand aan een nieuwe virtuele machine koppelen, op pagina 6
7	Schakel de virtuele beheermachine voor het uitgebreide systeem in en noteer de implementatie-URL. **Opmerking** Op dit tijdstip kunt u tevens de overige virtuele machines in uw systeem inschakelen. Zorg ervoor dat alle virtuele machines zijn ingeschakeld.	

Taak	Beschrijving	Zie
9	Geef de implementatie-URL op in een webbrowser en ga verder met de implementatie van uw uitgebreide systeem.	
10	Selecteer uw voorkeurstaal voor de implementatie van het uitgebreide systeem.	Uw taal voor installatie selecteren, op pagina 28
11	Bevestig de systeemgrootte. (Dit systeem moet minstens even groot zijn als het originele systeem.)	De grootte van uw systeem bevestigen, op pagina 29
12	Selecteer **Installeer een primair systeem**.	Kiezen welk systeem u moet installeren, op pagina 29
13	Selecteer handmatige implementatie.	Het type systeemimplementatie kiezen, op pagina 30
14	Als u openbare toegang wilt voor uw uitgebreide systeem, moet u controleren of het selectievakje **Een Reverse Proxy-virtuele machine maken** is ingeschakeld. Als u geen openbare toegang hebt toegevoegd, moet u dit selectievakje uitschakelen.	Openbare toegang toevoegen, op pagina 32
15	Voer het openbare VIP-adres voor de URL van de WebEx-site in. **Opmerking** U kunt hetzelfde openbare VIP-adres invoeren als u voor uw originele systeem gebruikt of een nieuwe IP-adres gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server.	Het openbare VIP-adres invoeren, op pagina 33
16	Voer het privé-VIP-adres in voor de URL van WebEx-beheer. **Opmerking** U kunt hetzelfde privé VIP-adres invoeren als u voor uw originele systeem gebruikt of een nieuwe IP-adres gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server.	Het privé-VIP-adres invoeren, op pagina 34

Taak	Beschrijving	Zie
17	Voer de URL van de WebEx-site in. Deelnemers openen deze URL om vergaderingen te hosten en bij te wonen. (Deze URL verwijst naar het persoonlijke VIP-adres of het openbare VIP-adres, afhankelijk of u wel of niet een split-horizon DNS gebruikt.) **Opmerking** U kunt dezelfde site-URL voor WebEx invoeren als u voor uw originele systeem gebruikt of een nieuwe URL gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server. Zorg dat u de URL van uw oorspronkelijke site op de DNS-server behoudt. Leid de URL van de oorspronkelijke site om naar de URL van de nieuwe site. Indien gebruikers de oorspronkelijke URL proberen te gebruiken en u deze niet hebt omgeleid naar de nieuwe URL, kunnen zij geen vergaderingen hosten of bijwonen.	De URL's van de WebEx-site en –Beheer invoeren, op pagina 36
18	Voer de URL van WebEx-beheer in waarmee beheerders Cisco WebEx-beheer kunnen openen en interne deelnemers vergaderingen kunnen hosten of bijwonen (alleen met een split-horizon DNS). (Deze URL verwijst naar het privé-VIP-adres.) **Opmerking** U kunt dezelfde beheer-URL voor WebEx invoeren als u voor uw originele systeem gebruikt of een nieuwe URL gebruiken. Als u het wijzigt, voert u de noodzakelijke updates uit aan de DNS-server.	De URL's van de WebEx-site en –Beheer invoeren, op pagina 36
19	Controleer of u alle wijzigingen aan het netwerk, de DNS-server en de firewallconfiguratie hebt aangebracht die vereist zijn voor uw systeem.	Bevestigen dat uw netwerk op de juiste manier is geconfigureerd, op pagina 36
20	Zodra uw virtuele machines zijn geïmplementeerd, selecteert u **Volgende** om verder te gaan met de controle van het systeem.	Uw virtuele machines implementeren
21	Tijdens de systeemcontrole werken we het uitgebreide systeem bij met eventuele benodigde updates om het systeem af te stemmen op de softwareversie van het originele systeem (het systeem van vóór het uitbreiden). (Deze updates kunnen tot een uur duren.) Als de update voltooid is, start het systeem opnieuw op.	Uw systeem controleren
22	Meld u aan bij Cisco WebEx-beheer.	

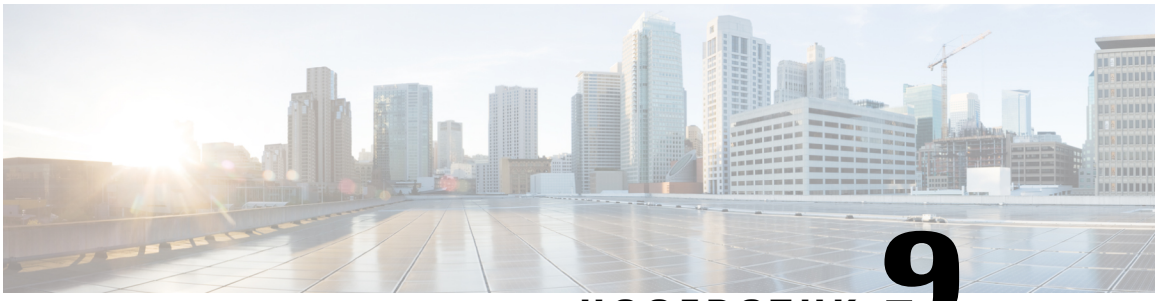
Taak	Beschrijving	Zie
23	Test het uitgebreide systeem. Als de uitbreiding niet is geslaagd, schakel dan het uitgebreide systeem uit en het originele systeem in. Neem contact op met de Cisco TAC voor hulp.	Het systeem testen
24	Configureer de licenties opnieuw voor het uitgebreide systeem.	Over licentiesLicenties opnieuw configureren na een software-upgrade of systeemuitbreiding

Het systeem testen

Een aantal van de aanbevolen tests om uit te voeren op het systeem, worden in dit gedeelte vermeld. U kunt deze tests uitvoeren en uw systeem valideren door twee diagnostische hulpmiddelen te gebruiken die u op de ondersteuningspagina's voor dit product vindt: de vergaderingstest en de systeembronnentest.

Wanneer u een geüpgraded systeem test, kunt u het bestaande systeem houden totdat u klaar bent met het testen van het geüpgradede systeem (u kunt beide systemen echter niet gelijktijdig inschakelen). Zodra u tevreden bent met de testresultaten voor het geüpgradede systeem, kunt u het bestaande systeem (voorgoed) verwijderen. Zorg ervoor dat het geüpgradede systeem wordt uitgevoerd wanneer u het bestaande systeem verwijdert of wist. Hiermee voorkomt u dat het VMDK-bestand, waartoe het geüpgradede systeem toegang heeft, onbedoeld wordt verwijderd.

- Gebruikers toevoegen, bewerken, activeren en deactiveren.
- Een vergadering plannen en starten
- Een bestaande vergadering opnieuw plannen.
- Een aantal vergaderingen of een toekomstige vergadering verwijderen.
- Een vergaderingsbijlage openen.
- Een opname van een vergadering afspelen.



HOOFDSTUK 9

Het systeem bijwerken

- Het systeem bijwerken, pagina 95
- Verbinding maken met een ISO-image op het cd/dvd-station, pagina 96
- Verdergaan met de updateprocedure, pagina 97
- De update voltooien, pagina 98

Het systeem bijwerken

Omdat de updateprocedure exclusieve toegang tot het systeem vereist, hebben gebruikers geen toegang tot het systeem voor vergaderingen. Zorg ervoor dat u de update plant wanneer het uw gebruikers zo min mogelijk stoort.

Andere systeembeheerders mogen het systeem niet openen tijdens deze procedure. Als ze dit wel doen, worden hun wijzigingen niet opgeslagen en is het resultaat onvoorspelbaar. Ze moeten wachten totdat deze procedure is voltooid voordat ze zich aanmelden bij de Cisco WebEx-beheersite.

De volledige updateprocedure, inclusief het maken van back-ups van uw virtuele machines, kan tot een uur duren, afhankelijk van de omvang van het systeem en de database.

Voordat u begint

Zorg dat u het recentste updatebestand van Cisco ontvangt:

Cisco-software downloaden (extern)

Het updatepakket voor uw systeem bevat een ISO-image. Het is niet mogelijk bepaalde versies van de software *over te slaan*. U moet bijvoorbeeld Cisco WebEx Meetings Server versie 1.1 (build 1.1.1.9.A) of versie 1.5 (build 1.5.1.6.A) installeren voordat u 1.5 MR2 toepast.

Procedure

Stap 1 Meld u aan bij de Cisco WebEx-beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen**.

Stap 3 Selecteer het tabblad **Systeem** en selecteer vervolgens **Upgraden**.

Stap 4 Selecteer **Bijwerken**.

Stap 5 Selecteer in de VMware vSphere-client **Power** > **Shut Down Guest** op elk van de virtuele machines in uw systeem.
Zie de VMware ESXi- en vCenter Server-documentatie voor een overzicht van het gebruik van vSphere.

Stap 6 Gebruik, wanneer de virtuele machines zijn uitgeschakeld, VMware Data Recovery (vanaf vSphere Release 5.1 wordt dit VMware vSphere Data Protection genoemd) om back-ups te maken van alle virtuele machines. Met een back-up wordt een virtuele machine indien nodig teruggezet naar de status ervan vóór de update. Zie Een back-up maken met VMware vCenter, op pagina 4 voor meer informatie. Zie de *beheerhandleiding van VMware-gegevensherstel* of de *beheerhandleiding van vSphere-gegevensbeveiliging* voor de complete informatie over deze back-up.

Opmerking U kunt ook een momentopname maken, maar u moet alle momentopnamen binnen ongeveer 24 uur verwijderen. Als u dat niet doet, presteren gegevens mogelijk niet goed. Zie Een momentopname maken met VMware vCenter voor meer informatie.

Voorzichtig Maak een back-up van elke virtuele machine, want de updateprocedure brengt wijzigingen aan in uw bestaande virtuele machines en u kunt de update niet ongedaan maken wanneer de procedure eenmaal is begonnen.

Stap 7 Schakel in de VMware vSphere-client elk van de virtuele machines in uw systeem in.

Stap 8 Meld u aan bij de Cisco WebEx-beheersite, maar schakel de onderhoudsmodus niet uit.

Stap 9 Selecteer het tabblad **Systeem** en selecteer vervolgens **Upgraden**.

Stap 10 Selecteer **bijwerken** om terug te gaan naar de pagina **Systeem bijwerken**.

Volgende stappen

Ga naar Verbinding maken met een ISO-image op het cd/dvd-station.

Verbinding maken met een ISO-image op het cd/dvd-station

Voor de snelste update raadt Cisco aan dat u de ISO-image onderbrengt in de vCenter-gegevensopslag. Als u echter het bestand op een lokale schijf van de vSphere-client plaatst, moet u er voor zorgen dat de vSphere-client via een kabelverbinding op uw bedrijfsintranet is aangesloten (en niet via VPN).

Ga als volgt te werk om de ISO-image in een vCenter-gegevensopslag te plaatsen en te verbinden met de cd/dvd:

Voordat u begint

Zorg dat u de benodigde ISO-image van Cisco ontvangt:

Software downloaden

Verifieer of u over de juiste toestemmingen beschikt.

Procedure

Stap 1 Selecteer de ESXi-host voor de virtuele beheermachine. Selecteer het tabblad **Samenvatting** en dubbelklik op de naam **gegevensopslag1** bij **Opslag**.

Stap 2 Selecteer in het venster **Datastore and Datastore clustersBrowse this datastore**.

Stap 3 Selecteer de groene pictogram pijl-omhoog (bestand uploaden) en laad het ISO-updatebestand.

Stap 4 Selecteer de virtuele beheermachine in de inventaris van VMware vCenter.

Stap 5 Selecteer het **cd/dvd**-pictogram van de virtuele beheermachine.

Stap 6 Selecteer op een lokale schijf of een gegevensopslag **Cd/dvd-station 1** > **Verbinden met ISO-image**.

Stap 7 Bevestig dat het cd/dvd-station is gekoppeld.

a) Klik met de rechter muisknop op de naam van de virtuele beheermachine in de vCenter inventaris en selecteer **Edit Settings...**
b) Selecteer in het tabblad **HardwareCD/DVD drive 1**.
c) Schakel het selectievakje **Verbonden** in als dit nog niet is ingeschakeld.
d) Selecteer **OK**.

Verdergaan met de updateprocedure

Voordat u begint

U bent klaar:

- Het systeem bijwerken, op pagina 95
- Verbinding maken met een ISO-image op het cd/dvd-station, op pagina 96

Procedure

Stap 1 Nadat u het ISO-bestand van de update hebt verbonden, selecteert u **Doorgaan** op de pagina **Systeem bijwerken** op de Cisco WebEx-beheerwebsite.

Stap 2 Selecteer het selectievakje **Ik ben verbonden met het ISO-bestand en klaar om door te gaan**.

Stap 3 Selecteer **Doorgaan**.

Voorzichtig Zodra u **Doorgaan** selecteert, kunt u de updateprocedure niet stoppen. Als er problemen optreden tijdens het updateproces en het wordt niet voltooid, moet u uw back-ups gebruiken om het systeem te herstellen.

De updateprocedure kan tot een uur duren. Sluit het browservenster niet, omdat u dan niet kunt terugkeren naar deze pagina.

Zodra de update is voltooid, wordt een nieuwe pagina weergegeven die de voltooiing van de update bevestigt.

Opmerking Er bestaat een regelmatig voorkomend probleem waarbij de update wordt voltooid, maar u de tekst **Systeem bijgewerkt** en de knop **Opnieuw opstarten** niet ziet. Als de update niet is voltooid en het heeft al langer dan een uur geduurd, kunt u proberen om de onderhoudsmodus uit te schakelen. Als u de onderhoudsmodus niet kunt uitschakelen, is de update nog steeds bezig. Start alle virtual machines van vCenter zodra de update voltooid is. Wacht totdat de virtual machines online komen en verifieer de systeemversie op het dashboard.

Stap 4 Selecteer **Opnieuw opstarten** om het systeem opnieuw op te starten.
Deze pagina bevat een standaardwaarde voor time-out van 90 minuten Zorg ervoor dat u het systeem binnen deze tijd opnieuw hebt opgestart; wijzig anders de standaardwaarde voor time-out in een langere periode.

Volgende stappen

Doorgaan met De update voltooien, op pagina 98.

De update voltooien

Voordat u begint

Dit is een voortzetting van Verdergaan met de updateprocedure, op pagina 97.

Procedure

Stap 1 Zodra de update is voltooid, selecteert u **Opnieuw starten**.
Zodra het systeem opnieuw is gestart, wordt de aanmeldpagina van de Cisco WebEx-beheersite weergegeven.

Stap 2 Meld u aan bij Cisco WebEx-beheer. De bijgewerkte versie is te zien op het dashboard.

Stap 3 Controleer de release-opmerkingen voor deze update en bepaal of post-updatetaken vereist zijn. Als er extra taken vereist zijn, voltooit u deze voordat u het systeem uit de onderhoudsmodus haalt.

Stap 4 Nadat u een post-updateconfiguratie hebt voltooid, selecteert u **Onderhoudsmodus uitschakelen**.

Stap 5 Het systeem testen en controleren. U kunt deze tests uitvoeren en uw systeem valideren door twee diagnostische hulpmiddelen te gebruiken die u op de ondersteuningspagina's voor dit product vindt: de vergaderingstest en de systeembronnentest.

- Gebruikers toevoegen, bewerken, activeren en deactiveren.
- Een vergadering plannen en starten
- Een bestaande vergadering opnieuw plannen.
- Een aantal vergaderingen of een toekomstige vergadering verwijderen.
- Een vergaderingsbijlage openen.
- Een opname van een vergadering afspelen.

Volgende stappen

- Als u problemen ondervindt, maak dan gebruik van VMware-gegevensherstel (vSphere-gegevensbeveiliging) of de momentopnamen van uw systeem om terug te keren naar uw vorige versie. Controleer de ISO-netwerkverbinding en zorg dat er geen problemen zijn.
- Als de update gelukt is, maak dan een tijd gebruik van het bijgewerkte systeem. Zodra u tevreden bent, zorgt u ervoor dat u de back-ups van de virtuele machines of de momentopnamen die u vóór de update hebt gemaakt, hebt verwijderd.

HOOFDSTUK 10

Het systeem bijwerken

- Een upgrade voorbereiden, pagina 101
- Het systeem automatisch upgraden, pagina 102
- Het systeem handmatig upgraden, pagina 105
- Het systeem testen, pagina 107
- Licenties opnieuw configureren en upgraden, pagina 108

Een upgrade voorbereiden

Uw systeem kan worden geüpgraded door het opnieuw te implementeren met een geüpgraded OVA-bestand (Virtual Server Template). Een *upgrade* wordt gedefinieerd als een vervanging van het systeem om belangrijke wijzigingen te implementeren die op het systeem zijn aanbracht. Een voorbeeld is het vervangen van versie 1.0 met versie 2.0 voor een systeem, waarin ondersteuning voor een nieuw besturingssysteem is opgenomen. Gebruik altijd de procedure Het systeem bijwerken als u het systeem bijwerkt naar een onderhoudsrelease of patch. Controleer in de release-opmerkingen welke procedure moet worden gebruikt. In beide gevallen worden alle gegevens van het bestaande systeem overgedragen naar het geüpgradede systeem.

Het systeem kan automatisch of handmatig worden geüpgraded. **We raden u aan het systeem te upgraden via het automatische proces.**

Tijdens het upgraden:

- kunt u een *upgrade* uitvoeren naar de volgende volledige versie van de toepassing. U *upgradet* uw systeem bijvoorbeeld van 1.5 naar 2.0. *Werk uw systeem bij* van 1.1 naar 1.5; probeer uw systeem niet te *upgraden* naar een incrementele release.
- Wanneer u een Cisco WebEx Meeting Server upgradet, worden de logboekregistraties die op het *bestaande* systeem zijn opgeslagen niet overgebracht naar het *geüpdatete* Cisco WebEx Meeting Server-systeem. Daarom moet u alle benodigde logboeken en logboekregistraties van het bestaande systeem vastleggen en downloaden voordat u begint met upgraden.
- Bij nieuwe installaties van Cisco WebEx Meetings Server versie 2.0 is 1,5 TB aan schijfruimte vereist voor de ESXi-hosts (Cisco UCS-server) met de virtuele beheermachine. Voor de ESXi-hosts (Cisco UCS-server) zonder een virtuele beheermachine is 1 TB aan schijfruimte vereist. Wanneer u van Cisco WebEx Meetings Server versie 1.x upgradet naar versie 2.0 met gebruik van uw huidige Cisco UCS-servers, is voor ESXi-hosts 1.118 GB aan vrije schijfruimte vereist als de UCS-server alleen de

virtuele beheermachine bevat (primair systeem of systeem met hoge beschikbaarheid), of 990 GB aan vrije schuifruimte als de UCS-server één virtuele beheermachine en één virtuele mediamachine bevat (primair systeem of systeem met hoge beschikbaarheid). De schijfruimte kan lokaal (DAS) of extern (SAN of NAS) zijn. De volledige informatie vindt u in het gedeelte 'Bronnen die worden verbruikt door Cisco WebEx Meetings Server en de ESXi-host' in de Systeemvereisten.

Opmerking In dit hoofdstuk verwijzen we naar het huidige systeem, voordat de upgrade wordt gestart, als het *bestaande* systeem. Het systeem dat met de upgrade wordt geïnstalleerd, wordt het *geüpgradede* systeem genoemd.

Voordat u een automatische of een handmatige upgrade start

Voordat een systeem automatisch of handmatig wordt geüpgraded, moet u rekening houden met het volgende:

- Verkrijg het OVA-bestand dat vereist is voor de upgrade.
- Maak een back-up voor elke virtuele machine in uw bestaande (huidige) systeem. (Raadpleeg Een back-up maken met VMware vCenter.)
- Plan een onderhoudsperiode. Tijdens het upgradeproces wordt het bestaande systeem in onderhoudsmodus geplaatst en is exclusieve toegang tot het systeem vereist. Gebruikers hebben tijdens deze periode geen toegang tot het systeem voor vergaderingen. Plan dit gedeelte van de upgrade op een tijdstip waarop uw gebruikers er zo weinig mogelijk hinder van ondervinden.
- Houd er rekening mee dat de omvang van de gegevensopslag toeneemt, want het bestaande en het geüpgradede systeem delen de gegevensopslag totdat het testen van het geüpgradede systeem is voltooid en het bestaande systeem is verwijderd.
- De hostnamen en IP-adressen van het bestaande systeem worden opnieuw gebruikt in het geüpgradede systeem. De interne virtuele machines van beide systemen zitten ook op hetzelfde subnet. Als u openbare toegang hebt toegevoegd, moeten de Reverse Proxy-virtuele machines voor het bestaande systeem en het bijgewerkte systeem op hetzelfde subnet zitten.

Het systeem automatisch upgraden

Voordat u een automatische upgrade start

Voordat een systeem automatisch wordt geüpgraded, moet u rekening houden met het volgende:

- Informeer andere systeembeheerders dat ze zich tijdens de upgrade geen toegang tot het bestaande systeem moeten verschaffen en geen wijzigingen tijdens de upgrade moeten aanbrengen. Deze wijzigingen kunnen onvoorspelbare resultaten opleveren.
- Lever en configureer één extra IP-adres dat tijdelijk wordt gebruikt voor het geüpgradede systeem.
- Schakel beide systemen niet handmatig in of uit.
- Controleer of het geüpgradede systeem toegang heeft tot de schijven voor de virtuele beheermachine van het bestaande systeem.

Automatisch upgraden

Deze tabel bevat een overzicht van belangrijke taken voor het voltooien van een automatische upgrade. De tabel bevat koppelingen naar gedeelten van de *Beheerhandleiding van Cisco WebEx Meetings Server* met de gedetailleerde stappen die moeten worden uitgevoerd om elke taak te voltooien. (U kunt in Adobe Acrobat Vorige weergave en Volgende weergave selecteren om eenvoudig tussen deze tabel en de afzonderlijke taken te schakelen.)

Taak	Beschrijving	Zie
1	Ga op het bestaande systeem naar License Manager (**Systeem** > **Meer weergeven** > **Licenties beheren**) en genereer een licentieverzoek. License Manager wordt in een nieuw tabblad geopend. Selecteer **Een licentieaanvraag maken**. Er wordt een pop-up weergegeven met de tekst van het licentieverzoek. Kopieer de tekst en sla het licentieverzoek op een handige locatie op, want misschien moet u de procedure voor het handmatig opnieuw configureren gebruiken om uw licenties opnieuw te claimen. Met deze informatie kan Cisco ook uw licenties vinden.	Licenties uitvoeren met License Manager
2	U kunt met de vSphere-client de virtuele beheermachine voor het geüpgradede systeem implementeren door de configuratie met het achtervoegsel **Automatisch upgraden** te selecteren, bijvoorbeeld **250 Beheergebruikers automatisch upgraden**.	
3	Schakel de virtuele beheermachine voor het geüpgradede systeem in en noteer de implementatie-URL die op de console van de virtuele machine wordt weergegeven.	
4	Voer in het URL-veld van een webbrowser de implementatie-URL in.	
5	Voer de beheer- en vCenter-URL's en -gegevens in, zodat de virtuele machines voor u kunnen worden geïmplementeerd.	VMware vCenter-gebruikersgegevens opgeven

Taak	Beschrijving	Zie
6	Als u extra virtuele machines wilt implementeren, selecteert u **Doorgaan**. (Totdat u met de installatie van het geüpgradede systeem begint en het bestaande systeem in onderhoudsmodus wordt gezet, kunnen gebruikers vergaderingen houden, maar mogen beheerders de virtuele machines van het bestaande systeem niet aanpassen.)	De voortgang van de upgrade wordt weergegeven in de implementatie-URL van het geüpgradede systeem en op de VMware-console waarmee de virtuele beheermachine van het primaire systeem is verbonden. Mocht het browservenster tijdens het upgradeproces per ongeluk worden afgesloten, kunt u de implementatie-URL van de VMware-console gebruiken.
7	Noteer de namen van de automatisch gemaakte virtuele machines die in vCenter worden vermeld. De indeling voor namen van virtuele machines is: CWMS_hostnaam_MMDDHHmm Waarbij mm=minuut Wanneer de upgrade is voltooid, worden de virtuele machines niet weergegeven. U kunt op basis van deze indeling een zoekopdracht uitvoeren om de virtuele machines te zoeken die als deel van de CWMS-upgrade zijn gemaakt.	
8	Als u het bestaande systeem automatisch in de onderhoudsmodus wilt plaatsen en u wilt beginnen met de installatie van het geüpgradede systeem, selecteert u **Doorgaan**. Er wordt een bericht weergegeven wanneer de onderhoudsmodus is ingeschakeld. Dit kan tot 30 minuten duren.	
9	Als u de bijgewerkte Cisco WebEx-beheersite wilt starten, selecteert u **Aanmelden bij Beheersite**.	
10	Schakel de onderhoudsmodus op het geüpgradede systeem uit. Het systeem wordt opnieuw opgestart.	Het kan een paar minuten duren voordat de vergaderservice beschikbaar is. Gebruikers kunnen weer vergaderingen starten als voor alle virtuele machines op de pagina **Systeemeigenschappen** de status Goed (groen) wordt weergeven. Zie De onderhoudsmodus in- of uitschakelen voor meer informatie.
11	Test het geüpgradede systeem. Als de upgrade niet is geslaagd, schakelt u het geüpgradede systeem uit, schakelt u het bestaande systeem in en neemt u contact op met Cisco TAC.	Het systeem testen

Taak	Beschrijving	Zie
12	Configureer de licentieversie opnieuw en werk deze bij voor het geüpgradede systeem. De licentievrije proefperiode verloopt binnen maximaal 180 dagen. Als het bestaande systeem over geldige licenties beschikte, moeten die binnen maximaal 180 dagen opnieuw worden geconfigureerd. Als het bestaande systeem in de licentievrije proefperiode werkte, worden de resterende dagen daarvan overgenomen door het geüpgradede systeem.	Over licentiesLicenties opnieuw configureren na een software-upgrade of systeemuitbreiding

Het systeem handmatig upgraden

Voordat u een handmatige upgrade start

Voordat een systeem wordt geüpgraded, moet u rekening houden met het volgende:

- Verwijder alle VMware-momentopnamen van het bestaande (huidige) systeem.
- U mag beide systemen niet gelijktijdig inschakelen en uitvoeren, omdat de hostnamen en IP-adressen van de virtuele machines van het bestaande systeem worden gebruikt in het geüpgradede systeem.
- Controleer of het geüpgradede systeem toegang heeft tot de schijven voor de virtuele beheermachine van het bestaande systeem. (Harde schijf 4 wordt van het bestaande systeem naar het geüpgradede systeem gekopieerd.)

Taken om het systeem handmatig te upgraden

Deze tabel bevat koppelingen naar andere gedeelten van de *Beheerhandleiding van Cisco WebEx Meetings Server*. Deze gedeelten bieden gedetailleerde informatie over die taak. (U kunt in Adobe Acrobat Vorige weergave en Volgende weergave selecteren om eenvoudig tussen deze tabel en de afzonderlijke taken te schakelen.)

Taak	Beschrijving	Zie
1	Ga op het bestaande systeem naar License Manager (**Systeem** > **Meer weergeven** > **Licenties beheren**) en genereer een licentieverzoek. License Manager wordt in een nieuw tabblad geopend. Selecteer **Een licentieaanvraag maken**. Er wordt een pop-up weergegeven met de tekst van het licentieverzoek. Kopieer de tekst en sla het licentieverzoek op een handige locatie op, want misschien moet u de procedure voor het handmatig opnieuw configureren gebruiken om uw licenties opnieuw te claimen. Met deze informatie kan Cisco ook uw licenties vinden.	Over licenties
2	Meld u aan op de beheersite van het bestaande systeem.	
3	Ga naar het tabblad Systeem en selecteer **Upgraden**.	

Taak	Beschrijving	Zie
4	Selecteer **Belangrijke upgrade**.	
5	Selecteer **Doorgaan** om de gegevens van het bestaande systeem te archiveren en het systeem in de onderhoudsmodus te plaatsen.	
6	Selecteer **In-/uitschakelen** > **Gast afmelden** op de virtuele machines van het bestaande systeem met de VMware vSphere-client.	
7	Implementeer alle geüpgradede virtuele machines, inclusief de virtuele machine met hoge beschikbaarheid en de virtuele Internet Reverse Proxy-machine.	Het OVA-bestand van de VMware vSphere-client implementeren
8	Kopieer de gegevens vanuit uw bestaande systeem naar de virtuele beheermachine voor het geüpgradede systeem.	Een bestaand VMDK-bestand aan een nieuwe virtuele machine koppelen
9	Schakel de geüpgradede virtuele beheermachine in en noteer de implementatie-URL die op de console van de virtuele machine wordt weergegeven. Heeft het systeem een hoge beschikbaarheid? Stel de virtuele machines met hoge beschikbaarheid dan niet in vanuit de beheerimplementatie met hoge beschikbaarheid, maar laat het upgradescript de virtuele machines met hoge beschikbaarheid detecteren. (Zie Een systeem met hoge beschikbaarheid configureren.)	
10	Schakel de overige geüpgradede virtuele machines in.	
11	Voer in het URL-veld van een webbrowser de implementatie-URL in.	
12	Selecteer **Doorgaan** om de installatie van het systeem te starten.	De voortgang van de upgrade wordt weergegeven in de implementatie-URL van het geüpgradede systeem en op de VMware-console waarmee de virtuele beheermachine van het primaire systeem is verbonden. Mocht het browservenster tijdens het upgradeproces per ongeluk worden afgesloten, kunt u de implementatie-URL van de VMware-console gebruiken.

Taak	Beschrijving	Zie
13	Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.	Het kan een paar minuten duren voordat de vergaderservice beschikbaar is. Gebruikers kunnen weer vergaderingen starten als voor alle virtuele machines op de pagina **Systeemeigenschappen** de status Goed (groen) wordt weergeven. Zie De onderhoudsmodus in- of uitschakelen voor meer informatie.
14	Wanneer de systeeminstallatie is voltooid, selecteert u **Aanmelden bij de beheersite**.	
15	Test het geüpgradede systeem. Wanneer uw geüpgradede systeem probleemloos werkt, kunt u uw bestaande systeem verwijderen om de oorspronkelijke systeembronnen vrij te maken. Zorg dat het geüpgradede systeem blijft draaien als u het bestaande systeem verwijdert, om te voorkomen dat het VMDK-basisbestand op harde schijf 4, waartoe het geüpgradede systeem toegang heeft, onbedoeld wordt verwijderd. Neem contact op met de technische ondersteuning van Cisco en schakel het geüpgradede systeem uit en het bestaande systeem in als de upgrade mislukt.	Het systeem testen
16	Configureer de licentieversie opnieuw en werk deze bij voor het geüpgradede systeem. De licentievrije proefperiode verloopt binnen maximaal 180 dagen. Als het bestaande systeem over geldige licenties beschikte, moeten die binnen maximaal 180 dagen opnieuw worden geconfigureerd. Als het bestaande systeem in de licentievrije proefperiode werkte, worden de resterende dagen daarvan overgenomen door het geüpgradede systeem.	Over licentiesLicenties opnieuw configureren na een software-upgrade of systeemuitbreiding

Het systeem testen

Een aantal van de aanbevolen tests om uit te voeren op het systeem, worden in dit gedeelte vermeld. U kunt deze tests uitvoeren en uw systeem valideren door twee diagnostische hulpmiddelen te gebruiken die u op de ondersteuningspagina's voor dit product vindt: de vergaderingstest en de systeembronnentest.

Wanneer u een geüpgraded systeem test, kunt u het bestaande systeem houden totdat u klaar bent met het testen van het geüpgradede systeem (u kunt beide systemen echter niet gelijktijdig inschakelen). Zodra u tevreden bent met de testresultaten voor het geüpgradede systeem, kunt u het bestaande systeem (voorgoed) verwijderen. Zorg ervoor dat het geüpgradede systeem wordt uitgevoerd wanneer u het bestaande systeem verwijdert of wist. Hiermee voorkomt u dat het VMDK-bestand, waartoe het geüpgradede systeem toegang heeft, onbedoeld wordt verwijderd.

- Gebruikers toevoegen, bewerken, activeren en deactiveren.
- Een vergadering plannen en starten
- Een bestaande vergadering opnieuw plannen.
- Een aantal vergaderingen of een toekomstige vergadering verwijderen.
- Een vergaderingsbijlage openen.
- Een opname van een vergadering afspelen.

Licenties opnieuw configureren en upgraden

Wanneer de licenties van het bestaande systeem opnieuw worden geconfigureerd, kunnen ze tijdelijk worden gebruikt op het geüpgradede systeem. Als de licenties niet opnieuw worden geconfigureerd, kunnen ze niet volledig worden geüpgraded. De proefperiode verloopt binnen maximaal 180 dagen. Na een software-upgrade:

- (Als het bestaande systeem zonder licenties en tijdens de licentievrije proefperiode werd gebruikt:) gaat het resterende aantal licentievrije dagen over op het geüpgradede systeem
- (Als het bestaande systeem over geldige licenties beschikte:) zijn de licenties van het originele systeem maximaal 180 dagen geldig voordat ze opnieuw moeten worden geconfigureerd (zie Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding) en bijgewerkt

Het GLO-aanvraagformulier openen

Ga naar de pagina voor het registreren van productlicenties (**https://tools.cisco.com/SWIFT/LicensingUI/Quickstart**) en selecteer Contact met ons opnemen om het GLO-aanvraagformulier (Global Licensing Operations) weer te geven. Selecteer **Aanvragen** op de pagina met contactgegevens van GLO-ondersteuning.

Voordat u begint

Zorg ervoor dat u de volgende gegevens bij de hand hebt:

- Uw contactgegevens
- Een omschrijving van het probleem
- De naam van het product en de status van de licentie (zoals een opnieuw verzonden licentie of een upgradelicentie)
- Informatie over rechten (zoals een serienummer van het product)

Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding

Nadat de CWMS-software is geüpgraded of uitgebreid en het testen is voltooid, moeten uw licenties opnieuw worden geconfigureerd. Opnieuw geconfigureerde licenties worden automatisch ongeldig op het bestaande systeem. Zorg er voordat u met het opnieuw configureren begint voor dat u over een licentieverzoek van het bestaande systeem beschikt, voor het geval u dit nodig hebt om de licenties opnieuw te configureren.

Het aantal licenties dat u opnieuw kunt configureren, is beperkt tot het aantal licenties op het bestaande systeem. De aanbevolen methode voor het opnieuw configureren van licenties is door middel van de portal voor het registreren van productlicenties.

Als het bestaande systeem over licenties beschikt, kunt u het geüpgradede systeem 180 dagen zonder licenties gebruiken. Hierdoor hebt u de tijd om het geüpgradede systeem te testen voordat u de originele licenties er opnieuw op configureert. U kunt licenties opnieuw configureren via de portal voor het registreren van productlicenties op http://cisco.com/go/license (zie Het GLO-aanvraagformulier openen). Als het bestaande systeem al in een proefperiode werd gebruikt, is de proefperiode van het geüpgradede systeem gelijk aan de resterende duur van de proefperiode van het bestaande systeem op het moment van bijwerken. Als het bestaande systeem vanwege ontbrekende licenties was vergrendeld, is het geüpgradede systeem ook vergrendeld.

Een licentieverzoek opslaan

Ga als volgt te werk om een licentieverzoek voor het bestaande systeem te verkrijgen:

Procedure

Stap 1 Ga op het bestaande systeem naar het venster Beheer en selecteer het venster **Systeem**.

Stap 2 Selecteer **(bij Licenties) Meer weergeven** > **Licenties beheren**.

Stap 3 Selecteer **Een licentieaanvraag maken**.

Stap 4 Sla het verzoek op in een lokale map van de computer.

Licenties registreren die opnieuw moeten worden geconfigureerd

Ga als volgt te werk om de portal voor het registreren van productlicenties te gebruiken:

Procedure

Stap 1 Meld u aan bij de portal voor het registreren van productlicenties op https://tools.cisco.com/SWIFT/LicensingUI/Quickstart.

Stap 2 Meld u aan met het cisco.com-account dat is gebruikt voor het uitvoeren van de licenties van uw bestaande systeem.
Als dit account niet beschikbaar is of als u zich aanmeldt en er geen licenties worden weergegeven die aan het account zijn gekoppeld, open dan een case bij Cisco (zie Het GLO-aanvraagformulier openen).

Stap 3 Selecteer **Licentie voor overdracht - starten** in het menu **Overdracht**. Het venster **Licentiebron opgeven** wordt weergegeven.

Stap 4 Schakel het selectievakje naast de UUID in van het systeem waarvan u licenties opnieuw wilt configureren, bijvoorbeeld de UUID van het 1.x-systeem. Als u over meerdere systemen beschikt en u de UUID van het systeem dat u opnieuw wilt configureren niet weet, ga dan terug naar het bestaande systeem en start License Manager. Zoek in het venster **Licenties** in de kolom **Bestandsnaam** een licentiestring, bijvoorbeeld

c8be79aeecaba5922955b53679527463_201311182150051080. De UUID bestaat uit de eerste tekens van de string, tot aan het liggende streepje (_).

Stap 5 Ga terug naar de portal voor het registreren van productlicenties.

Stap 6 Selecteer de licenties die u opnieuw wilt configureren en selecteer **Volgende**. Het venster **Doel en opties opgeven** wordt weergegeven.

Stap 7 Plak het licentieverzoek in het veld **Licentieverzoek** van het doelsysteem en selecteer **Volgende**. Het doelsysteem is het systeem waarnaar u licenties verplaatst. Als dit een software-upgrade is, is het doel het geüpgradede systeem. Als dit een systeemuitbreiding is, is het doel het vergrote systeem. Als dit een noodherstel is, is het doel het herstelde systeem.
Het venster **Controleren** wordt weergegeven.

Stap 8 Schakel het selectievakje **Ik ga akkoord met de voorwaarden van de licentieovereenkomst** in en klik op **Verzenden**.
U ontvangt een e-mail met uw opnieuw geconfigureerde licenties. Als u de licenties opnieuw configureert als onderdeel van een software-upgrade, moet u de 1.0-licenties opnieuw configureren en bijwerken op uw 2.0-systeem (zie Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding). Mogelijk wordt er op de beheersite van uw geüpgradede systeem een foutbericht weergegeven in de trant van **U gebruikt een ongeldig licentiebestand bij uw huidige implementatie**. Dit is verwacht gedrag. In het bericht wordt een vervaldatum genoemd waarop uw systeem zal worden uitgeschakeld. Upgrade uw licenties vóór de vervaldatum om te voorkomen dat uw systeem wordt uitgeschakeld.

Volgende stappen

Opnieuw geconfigureerde licenties die op het geüpgradede systeem zijn geïnstalleerd, zijn van dezelfde versie als de licenties op het bestaande systeem. Als u bijvoorbeeld upgradet van 1.x naar 2.0, ontvangt u 1.x-licenties die op het 2.0-systeem worden herkend. Als de licenties worden geïnstalleerd, wordt het volgende foutbericht weergegeven: **U gebruikt een ongeldig licentiebestand voor uw huidige implementatie. Als dit zo blijft, wordt uw systeem op *mm/dd/jj* uitgeschakeld.** Dit is verwacht gedrag. (Mogelijk wordt dit bericht ook per e-mail aan de systeembeheerder verzonden.)

Voltooi na het opnieuw configureren van de licenties de licentie-upgrade vóór de genoemde datum om ervoor te zorgen dat het gebruik van het systeem niet wordt onderbroken. (Zie Licenties uitvoeren met License Manager.)

Licenties upgraden na een software-upgrade

Na een software-upgrade worden licenties vanaf het bestaande systeem opnieuw geconfigureerd op het geüpgradede systeem. (Zie Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding voor meer informatie.) Nadat de licenties opnieuw zijn geconfigureerd, kunnen deze worden geüpgraded voor gebruik op het geüpgradede systeem.

Uw licenties upgraden met eFulfilment:

1. Vraag uw leverancier naar een PAK-code (Product Authorization Key).
2. Vanuit het venster **Systeem** selecteert u **(onder Licenties) meer weergeven**>**Licenties beheren**> **Licenties**> **Licenties installeren vanuit PAK**. Het venster **Licenties installeren vanuit PAK** wordt weergegeven.
3. Voer de PAK-code in en selecteer **Volgende**.
4. Meld u aan met uw cisco.com-gebruikersgegevens. Het venster **Licenties installeren vanuit PAK** wordt weergegeven.
5. Klik op de kolom Installeren om het aantal licenties te selecteren dat u wilt installeren.

6 Geef het aantal te installeren licenties op en selecteer **Opslaan**. De licenties worden als onderdeel van de eFulfilment van de PAK op het systeem geïnstalleerd.

Opmerking U kunt maximaal het aantal licenties uit de upgrade-PAK installeren. Het maximale aantal te installeren licenties mag ook het aantal opnieuw geconfigureerde licenties van het bestaande systeem niet overschrijden.

Uw licenties upgraden met behulp van een licentiebestand:

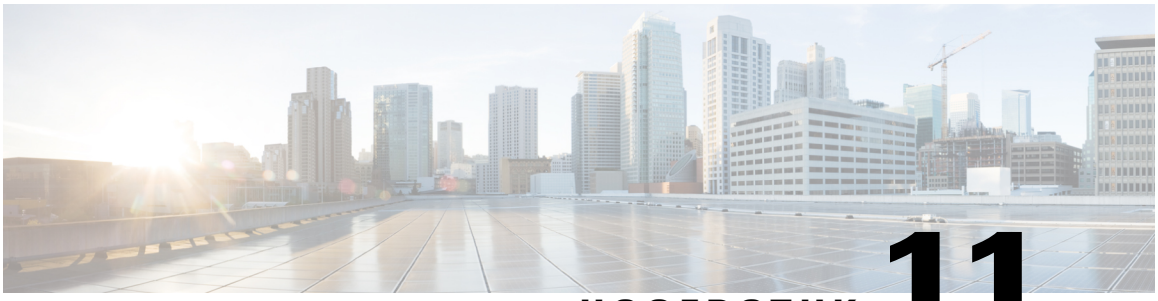
1 Verkrijg een licentiebestand van Cisco via **cisco.com/go/license**.
2 Vanuit het venster **Systeem** selecteert u **(onder Licenties) meer weergeven**>**Licenties beheren**> **Licenties**> **Licenties installeren vanuit bestand**. Het venster **Licentiebestand installeren** wordt weergegeven.
3 Blader door het licentiebestand. Het bestand wordt weergegeven in het venster **Licenties**.

De licenties worden automatisch bijgewerkt.

DEEL II

Configuratiehandleiding van Cisco WebEx Meetings Server

- Uw dashboard gebruiken, pagina 115
- Gebruikers beheren, pagina 131
- Uw systeem configureren, pagina 153
- Instellingen configureren, pagina 187
- Uw rapporten beheren, pagina 243
- De ondersteuningsfuncties gebruiken, pagina 251



HOOFDSTUK 11

Uw dashboard gebruiken

Deze module beschrijft de functies op uw Cisco WebEx-serverdashboard en hoe u deze moet gebruiken.

- Informatie over uw dashboard, pagina 115
- Alarmen weergeven en bewerken, pagina 117
- Uw Geschiedenis hulpmiddelen weergeven, pagina 119
- Trends vergadering weergeven, pagina 121
- De lijst Vergaderingen weergeven, pagina 122
- Een onderhoudsperiode plannen, pagina 123
- Een geplande onderhoudsperiode wijzigen, pagina 124
- Over de onderhoudsmodus, pagina 125
- De onderhoudsmodus in- of uitschakelen, pagina 128

Informatie over uw dashboard

Dit gedeelte beschrijft de functies op uw dashboard en hoe u ze moet gebruiken. Het dashboard, de startpagina van de beheersite, bevat verschillende parameters en belangrijke controlefuncties met grafieken.

Het dashboard bevat de volgende gedeelten:

- Systeemmonitor: geeft de systeemstatus en een tijdstempel weer. Bevat de volgende subsecties:
  - Vergaderingen en gebruikers: de status van actieve vergaderingen en het gebruik. Geeft het aantal vergaderingen weer dat momenteel actief is, en het aantal gebruikers dat aan vergaderingen deelneemt (het gebruik). Het statuslampje geeft aan of het aantal actieve vergaderingen en het gebruik hoger of lager zijn dan de geconfigureerde alarmdrempel. Bij een groen lampje liggen ze onder de geconfigureerde drempel en bij een rood lampje erboven. Zie Alarmen weergeven en bewerken, op pagina 117 voor meer informatie over het configureren van alarmen.
  - Alarmpictogram: selecteer het alarmpictogram om de geconfigureerde alarmdrempelinstellingen weer te geven en te bewerken. Alarmdrempels worden numeriek weergegeven op de pagina **Alarmen**. Alarmdrempels worden standaard in percentages weergegeven. Zie Alarmen weergeven en bewerken, op pagina 117 voor meer informatie over het configureren van alarmen.

U kunt alarmen configureren voor het volgende:

- Actieve vergaderingen—Geeft aan wanneer de huidige vergaderingen problemen ondervinden.
- Gebruik—Het totale aantal gebruikers dat momenteel het systeem gebruikt.
- CPU—Het CPU-gebruik van de virtuele machine met het hoogste CPU-gebruik van alle virtuele machines van het systeem.
- Geheugen—De hoeveelheid geheugen (bij benadering) die wordt gebruikt door de virtuele machine met de hoogste geheugenbelasting.

Opmerking Wanneer het lampje telkens kort rood oplicht, betekent dat niet dat het systeem zich in een kritieke toestand bevindt of onmiddellijk aandacht nodig heeft. Een hoog geheugengebruik kan een indicatie van andere systeemprestatieproblemen zijn. Als het geheugengebruik langdurig boven de 90% uitkomt, raden wij u aan om het geheugengebruik van vCenter en de CPU-statistieken te controleren. Als blijkt dat deze statistieken zich buiten de normale waarden bevinden, kijk dan of u het systeem zodanig kunt wijzigen dat de belasting lager is.

- Netwerk—De totale gebruikte bandbreedte van het systeem.
- Opslag—Gebruikte opslagruimte voor opnamen en back-ups van de database.

Opmerking Het opslagalarm wordt weergegeven als u een opslagserver hebt geconfigureerd. Zie Een opslagserver configureren, op pagina 164 voor meer informatie.

Opmerking De opnamefunctie voor vergaderingen wordt uitgeschakeld als het opslaggebruik boven de drempel ligt.

- CPU, Geheugen, Netwerk en Opslag—Geven het percentage en de werkelijke hoeveelheid gebruikte bronnen weer. Elke bron heeft een statuslampje. Bij een groen lampje liggen ze onder de geconfigureerde drempel en bij een rood lampje erboven. Zie Alarmen weergeven en bewerken, op pagina 117 voor meer informatie over het configureren van alarmen.

  Klik op de koppeling CPU, Geheugen, Netwerk of Opslag om de pagina **Geschiedenis systeembronnen** of **Opslaggeschiedenis** te openen.

- De grafiek Trend vergadering en de lijst Vergaderingen—Een grafiek met het aantal vergaderingen dat gedurende een opgegeven periode op uw systeem is gehouden. Gebruik de velden **Van** en **Tot** om de periode in te stellen voor de trendinformatie over vergaderingen en voor de vergaderingen in de lijst Vergaderingen. Als u op een punt in de grafiek Trend vergadering klikt, wordt een lijst weergegeven met de vergaderingen in de lijst Vergaderingen die plaatsvonden tijdens de periode die in de grafiek is opgegeven. Als u wilt weergeven welke vergaderingen op een specifiek tijdstip plaatsvonden, beweegt u de muis over de grafiek en selecteert u de gewenste tijd. In de lijst Vergaderingen wordt het totale aantal vergaderingen weergegeven dat tijdens de geselecteerde periode plaatsvond, evenals de onderwerpen, hosts, deelnemersaantallen en statussen van die vergaderingen. U kunt elke informatiekolom

in de lijst Vergaderingen sorteren. De vergaderingen worden op volgorde van status weergegeven: Bezig, Beëindigd en Niet gestart.

- Onderhoud—Hiermee kunt u een onderhoudsperiode plannen voor het configureren van uw systeem of het wijzigen van uw instellingen. Ook kunt u de onderhoudsmodus hiermee in- of uitschakelen. Zie Een onderhoudsperiode plannen, op pagina 123 en Over de onderhoudsmodus, op pagina 125 voor meer informatie.
- Laatste systeemback-up—De datum en tijd waarop voor het laatst een back-up is gemaakt, de bestandsnaam, omvang en locatie van die back-up en de datum en tijd van de volgende back-up. Het stelt u ook op de hoogte als de back-up is mislukt en geeft u de datum van de eerste poging van de back-up als deze nog niet is aangemaakt.

Opmerking Wordt alleen weergegeven als u een opslagserver hebt geconfigureerd.

- Systeem—Geeft het maximale aantal gebruikers weer dat tegelijkertijd aan vergaderingen kan deelnemen, evenals het versienummer, de product-URL, het aantal gebruikerslicenties, of openbare toegang is toegestaan en of het om een systeem met hoge beschikbaarheid gaat. Als u een gratis proefversie van Cisco WebEx Server gebruikt en de proefperiode nog dertig dagen of minder duurt, wordt in dit gedeelte ook aangegeven over hoeveel dagen de proefperiode verloopt. Selecteer **Meer weergeven** om naar Uw systeem configureren, op pagina 153 te gaan.
- Gebruikers—Geeft het totale aantal actieve gebruikers weer, evenals het geselecteerde verificatietype, of directory-integratie is geconfigureerd of niet en wanneer de volgende synchronisatie plaatsvindt (als deze is geconfigureerd). Selecteer **Meer weergeven** om naar Gebruikers bewerken, op pagina 138 te gaan.
- Instellingen—Geeft het maximale aantal deelnemers weer dat aan elke vergadering kan deelnemen, evenals het audiotype en of WebEx HQ-video is ingeschakeld. Selecteer **Meer weergeven** om naar Instellingen configureren, op pagina 187 te gaan.

Verwante onderwerpen

Uw Geschiedenis hulpmiddelen weergeven, op pagina 119

Het diagram Actieve vergaderingen gebruiken om vergaderingsproblemen te verhelpen, op pagina 120

Een onderhoudsperiode plannen, op pagina 123

De onderhoudsmodus in- of uitschakelen, op pagina 128

Alarmen weergeven en bewerken

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Dashboard** > **Alarmen**.
De pagina **Alarmen** wordt weergegeven en toont de huidige alarmdrempel.

Stap 3 Selecteer **Bewerken**.

De pagina **Alarmen bewerken** wordt weergegeven. Selecteer **Percentage %** om de alarmdrempel als een percentage weer te geven of **Nummer #** om de alarmdrempel als aantal weer te geven. De standaardinstelling is **Percentage %**.

Stap 4 Selecteer de selectievakjes voor de alarmen die u wilt inschakelen en selecteer het interval voor elk ingeschakeld alarm.

Optie	Beschrijving
Actieve vergaderingen	Geeft de drempel van actieve vergaderingen weer. • Indien ingesteld op **Percentage %**, beweegt u de schuifknop van 2 tot 99 procent. • Indien ingesteld op **Nummer #**, voert u een getal in van 2 tot 99 procent. **Standaard:** Geselecteerd met een interval van **een uur**.
Gebruik	Geeft de huidige systeemdrempel weer. • Indien ingesteld op **Percentage %**, beweegt u de schuifknop van 2 tot 99 procent. • Indien ingesteld op **Nummer #**, voert u het aantal gebruikers in. **Standaard:** Geselecteerd met een interval van **12 uur**.
CPU	Geeft de huidige CPU-drempel in MHz weer. • Indien ingesteld op **Percentage %**, beweegt u de schuifknop van 2 tot 99 procent. • Indien ingesteld op **Nummer #**, voert u het aantal MHz in. **Standaard:** Niet geselecteerd. Interval is **een uur**.
Geheugen	Geeft de huidige geheugendrempel in GB weer. • Indien ingesteld op **Percentage %**, beweegt u de schuifknop van 2 tot 99 procent. • Indien ingesteld op **Nummer #**, voert u het aantal GB in. **Standaard:** Niet geselecteerd. Interval is **een uur**. **Opmerking** De geheugenmeter geeft bij benadering aan hoeveel geheugen wordt gebruikt door de virtuele machine met de hoogste geheugenbelasting. Wanneer de meter gedurende een kortere periode in het rode gedeelte komt, is dit geen indicatie dat het systeem zich in een kritieke toestand bevindt of dat onmiddellijke aandacht is vereist. Een hoge geheugenbelasting kan erop wijzen dat er andere problemen op het gebied van systeemprestaties aanwezig zijn die aandacht vereisen. Als het geheugengebruik langdurig boven de 90% uitkomt, raden wij u aan om het geheugengebruik van vCenter en de CPU-statistieken te controleren. Als blijkt dat deze statistieken zich buiten de normale waarden bevinden, kijk dan of u het systeem zodanig kunt wijzigen dat de belasting lager is.

Optie	Beschrijving
Netwerk	Geeft de huidige netwerkbandbreedtedrempel in Mbps weer. • Indien ingesteld op **Percentage %**, beweegt u de schuifknop van 2 tot 99 procent. • Indien ingesteld op **Nummer #**, voer dan het aantal Mbps in. **Standaard:** Niet geselecteerd. Interval is **een uur**.
Opslag	Toont de huidige opslagdrempel in GB. De maximum opslagdrempel wordt berekend als (de totale ruimte – opnamebuffergrootte) waar opnamebuffergrootte 1 GB is voor micro, 5 GB voor kleine, 16 GB voor middelgrote en voor 40 GB grote. • Indien ingesteld op **Percentage %**, beweegt u de schuifknop van 2 tot 99 procent. • Indien ingesteld op **Nummer #**, voert u het aantal GB in. **Standaard:** Niet geselecteerd. Interval is **een uur**. **Opmerking** Deze rubriek wordt alleen weergegeven als u een opslagserver hebt geconfigureerd. Zie Een opslagserver configureren, op pagina 164 voor meer informatie.

Er wordt een e-mail verzonden naar de beheerders bij overschrijding van een alarmdrempel. Het interval wordt gebruikt om meerdere alarmen te onderdrukken binnen de opgegeven tijd, om te voorkomen dat er te veel e-mails voor hetzelfde probleem worden verzonden. Mogelijke intervallen voor elk alarm zijn:

- een uur
- Zes uur
- 12 uur
- 24 uur

Stap 5 Selecteer **Opslaan**.
Uw alarminstellingen zijn opgeslagen en de pagina **Alarmen** is bijgewerkt met uw wijzigingen.

Uw Geschiedenis hulpmiddelen weergeven

Uw geschiedenis hulpmiddelen bevat gedetailleerde grafieken voor elk alarm dat op uw systeem is geconfigureerd. De huidige waarden voor systeemstatus, vergaderingen, deelnemers en opslag worden weergegeven in de deelvensters aan de rechterkant. Zie Alarmen weergeven en bewerken voor meer informatie over de alarmen die u kunt configureren.

U kunt de geschiedenis van uw hulpmiddelen weergeven door een alarmkoppeling **CPU**, **Geheugen** of **Netwerk** te selecteren in het venster **Dashboard**. Als u bijvoorbeeld de CPU-koppeling selecteert, wordt het venster **Geschiedenis hulpmiddelen** weergegeven.

Als u een opslagserver hebt geconfigureerd, kunt u uw opslaggeschiedenis weergeven door de koppeling **Opslag** op het venster **Dashboard** te selecteren. Op de pagina **Opslaggeschiedenis** wordt weergegeven

hoeveel ruimte op uw opslagserver is gebruikt en wordt een grafiek weergegeven met de gebruikte opslagruimte in het afgelopen halfjaar. Beweeg met de muis over de blauwe gebruiksgrafiek om het percentage gebruikte ruimte op bepaalde dagen en tijden binnen het halve jaar weer te geven.

Het diagram Actieve vergaderingen gebruiken om vergaderingsproblemen te verhelpen

Wanneer u een e-mail ontvangt waarin staat vermeld dat er een probleem is met een vergadering, voert u de volgende stappen uit om de oorzaak vast te stellen.

Procedure

Stap 1 Selecteer de koppeling in de e-mail die u hebt ontvangen over het probleem.

Stap 2 Meld u aan bij de Beheersite.

Stap 3 Selecteer op het dashboard de koppeling **CPU, Geheugen** of **Netwerk**.
Geschiedenis hulpmiddelen wordt weergegeven.

Stap 4 Selecteer de koppeling **Actieve vergaderingen** in het deelvenster rechts van de hulpmiddelengrafiek.

Stap 5 Selecteer optioneel een **Weergave**-optie of het agendapictogram om vergaderingen voor een specifieke periode weer te geven.

Stap 6 Schakel optioneel het selectievakje **Geplande vergaderingen weergeven** in om toekomstige vergaderingen op te nemen in de lijst **Vergaderingen**.

Stap 7 Klik op een gegevenspunt in de grafiek **Deelnemers** of **Vergaderingen** om vergaderingsgegevens weer te geven.
U kunt de gedetailleerde informatie in deze tabel gebruiken om u te helpen bij het vaststellen van de oorzaak van het probleem dat wordt beschreven in de e-mail die u hebt ontvangen. In de lijst met vergaderingen vindt u informatie over vergaderingen die overeenkomen met het geselecteerde gegevenspunt. Vergaderingen met prestatieproblemen worden in de kolom Status in het rood of geel weergegeven.

Voer zoektermen in het veld boven de tabel in om de lijst met vergaderingen te filteren. De lijst met vergaderingen kan worden gesorteerd door de kop van de hoofdkolom te selecteren.

Stap 8 De huidige systeemstatus wordt weergegeven in de rechterkolom van de pagina. Selecteer deze regel om terug te keren naar het dashboard.
De systeemstatus kan als volgt zijn:

- Goed: alle services op uw systeem werken
- Buiten werking: geen van de processen op uw systeem wordt uitgevoerd. Neem contact op met Cisco Technical Assistance Center (TAC) voor ondersteuning. Zie De ondersteuningsfuncties gebruiken voor meer informatie.

Stap 9 Selecteer een alarmstatusvakje in de rechterkolom om de Geschiedenis hulpmiddelen voor de alarmen weer te geven. Raadpleeg Uw Geschiedenis hulpmiddelen weergeven voor meer informatie.

Stap 10 Als een opslagserver is geconfigureerd, wordt de hoeveelheid opslagruimte in de rechterkolom op de pagina weergegeven. Zie Alarmen weergeven en bewerken, op pagina 117 voor meer informatie.

Trends vergadering weergeven

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Dashboard**.

Stap 3 Stel boven de grafiek **Trend vergadering** een trendperiode in door bij **Van** en **Tot** een datum en tijd te selecteren.

- Vergaderingen die vóór middernacht zijn gepland en voortduren tot de volgende dag worden weergegeven op de grafiek met de startdatum van de vergadering.
- Als de verbinding van een vergadering wordt verbroken als gevolg van een systeemprobleem en opnieuw wordt verbonden, wordt dit twee keer geteld op de grafiek Trend vergadering.
- Trendgegevens van vergaderingen voor éénmaandelijkse en zesmaandelijkse weergaven zijn gebaseerd op Greenwich Mean Time (GMT) en worden bijgevolg niet nauwkeurig weergegeven over een periode van 24 uur. Als uw systeem bijvoorbeeld 200 vergaderingen host tijdens een bepaalde dag, neemt de database het aantal vergaderingen op basis van GMT op en niet op basis van de lokale tijd. Trendgegevens van vergaderingen voor ééndaagse en éénwekelijkse weergaven zijn gebaseerd op de tijdzone van de gebruiker.
- Actieve en beëindigde vergaderingen worden groen gemarkeerd. Toekomstige vergaderingen worden geel weergegeven.
- Als het geselecteerde tijdbereik 24 uur omvat, worden gegevenspunten voor afgeronde en actieve vergaderingen aangegeven in intervallen van vijf minuten en die voor toekomstige vergaderingen in intervallen van een uur.
- Als het geselecteerde tijdbereik langer dan een dag, maar korter dan of precies een week duurt, worden gegevenspunten voor afgeronde, actieve en toekomstige vergaderingen weergegeven in intervallen van een uur.
- Als het geselecteerde tijdbereik langer dan een week duurt, worden gegevenspunten voor afgeronde, actieve en toekomstige vergaderingen weergegeven in intervallen van een dag.

In de grafiek **Trend vergadering** wordt het totale aantal vergaderingen tijdens de geselecteerde periode weergegeven. In de lijst **Vergaderingen** onder de grafiek worden alle vergaderingen tijdens de geselecteerde trendperiode weergegeven.

Opmerking Sommige vergadertrendvermeldingen kunnen dubbel lijken, omdat ze dezelfde naam hebben. Telkens wanneer een vergadering wordt gestart, wordt er een vermelding gemaakt. Als een vergadering wordt gestart, beëindigd en opnieuw gestart, worden er dus meerdere vermeldingen met dezelfde naam weergegeven.

Stap 4 Ga als volgt te werk om een lijst weer te geven met vergaderingen op een bepaald tijdstip:

a) Klik op een bepaalde locatie in de grafiek **Trend vergadering** om de vergaderingen in de vijf minuten voor en na het geselecteerde tijdstip weer te geven in de lijst **Vergaderingen** onder de grafiek. Zie De lijst Vergaderingen weergeven, op pagina 122 voor meer informatie.

b) Selecteer het grafieksymbool onder de velden **Van** en **Tot** om een lijst weer te geven met datums en tijden waarop in de gekozen periode vergaderingen plaatsvonden. Selecteer vervolgens een datum in de vervolgkeuzelijst.

Opmerking De gegevenspunten in het vervolgkeuzemenu zijn gelijk aan die op de grafiek. Deze zijn voornamelijk toegankelijk gemaakt ten behoeve van gebruikers met een toetsenbord en schermlezer.

Opmerking Beweeg de muis over de grafiek om het totale aantal vergaderingen weer te geven dat op dat tijdstip plaatsvond.

De lijst Vergaderingen weergeven

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Dashboard**.

Stap 3 Stel boven de grafiek Trend vergadering een trendperiode in door bij **Van** en **Tot** een datum en tijd te selecteren. Zie Trends vergadering weergeven, op pagina 121 voor meer informatie.

Opmerking
- In de lijst Vergaderingen worden standaard de vergaderingen van de huidige periode van 24 uur weergegeven.
- Geplande vergaderingen die niet op de geplande tijd zijn begonnen, worden niet opgenomen in de grafiek Trend vergadering en de lijst Vergaderingen.

In de lijst Vergaderingen wordt het totale aantal vergaderingen weergegeven: alle geplande, actieve en beëindigde vergaderingen tijdens de geselecteerde trendperiode. De vergaderingen worden weergegeven in volgorde van status: Bezig, Beëindigd en Niet gestart. In de lijst Vergaderingen wordt onder andere de volgende informatie weergegeven:

- Het in de trendgrafiek geselecteerde tijdbereik
- Vergaderonderwerp
- Host
- Aantal deelnemers:
- De status van de vergadering: Bezig, Beëindigd of Niet gestart.

Opmerking In de eerste kolom voor vergaderingen met de status *Bezig* of *Beëindigd* staat een groen, geel of rood lampje, waarmee de staat van de vergadering wordt aangeduid: *goed*, *redelijk* of *slecht*. Een geel lampje (redelijk) geeft aan dat een audio- of videovertraging of jitter tijdens de vergadering een secundaire drempelwaarde heeft bereikt die moet worden gecontroleerd en waarvan de oorzaak moet worden vastgesteld. Een rood lampje (slecht) geeft aan dat een audio- of videovertraging of jitter tijdens de vergadering een primaire drempelwaarde heeft bereikt en dat de beheerder voor hulp contact moet opnemen met de technische ondersteuning van Cisco.

Stap 4 (Optioneel) Selecteer een kolomkop om de vergaderingen te sorteren.

Stap 5 Gebruik de functie voor paginering om de vorige of volgende pagina weer te geven.

Opmerking

- Per pagina worden maximaal tien vergaderingen weergegeven.
- Per trendperiode kunnen in totaal maximaal 125 vergaderingen worden weergegeven. Deel de trendperiode op in kortere perioden als een bepaalde periode te veel vergaderingen bevat.
- Mogelijk staan vergaderingen dubbel in de lijst Vergaderingen. Elke vergadering die wordt gestart, wordt aan de lijst toegevoegd. Als een vergadering wordt gestart, beëindigd en opnieuw gestart, worden er dus meerdere vergaderingen met dezelfde naam weergegeven in de lijst.

Een onderhoudsperiode plannen

Plan een onderhoudsperiode voordat u systeemonderhoud uitvoert. Als een onderhoudsperiode van kracht is, is de enige beperking dat gebruikers geen vergaderingen kunnen plannen die gedeeltelijk of geheel binnen de onderhoudsperiode vallen. Voorbeeld: een beheerder wil het systeem wegens onderhoud gedurende ongeveer een uur uitschakelen, van 5:00 tot 6:00 uur. In dat uur lijken er geen vergaderingen te zijn gepland. Als er wel vergaderingen zijn gepland, moet de beheerder contact opnemen met de hosts van alle vergaderingen om ze te vertellen dat er tijdens hun vergadering een onderhoudsperiode is gepland. Als een onderhoudsperiode is ingesteld, kunnen gebruikers tijdens die periode geen vergaderingen plannen. Gebruikers kunnen echter wel een directe vergadering starten via de functie **Nu vergaderen**.

Zodra de onderhoudsperiode is ingeschakeld, worden alle actieve vergaderingen beëindigd en is de functie Nu vergaderen niet meer beschikbaar. Stel dat u vaststelt dat het ongeveer twee uur zal duren om alle noodzakelijke systeemwijzigingen aan te brengen. Een van de taken die u moet uitvoeren is het uploaden van een nieuw certificaat van een certificeringsinstantie. Hiervoor moet het systeem mogelijk opnieuw worden opgestart nadat u de onderhoudsmodus hebt uitgeschakeld. U wilt rond 4:00 beginnen met het systeemonderhoud. U plant een onderhoudsperiode met een starttijd op 15 april 2014 om 3:30 uur met een duur van 3 uur en 30 minuten. Dit betekent dat de onderhoudsperiode plaatsvindt van 3:30 uur tot 7:00 uur. Voordat de beheerder wil beginnen met het systeemonderhoud, zijn er 30 minuten beschikbaar om alle vergaderingen te beëindigen. In deze 30 minuten kunnen er ook geen nieuwe vergaderingen worden gepland. In deze onderhoudsperiode is ook tijd opgenomen om het systeem, indien nodig, opnieuw op te starten en operationeel te kunnen laten worden na inschakeling van de onderhoudsmodus, en tijd waarin de beheerder een of meer directe vergaderingen kan starten om de gewijzigde instellingen te testen voordat de gebruikers vergaderingen kunnen plannen en hosten.

Voor bepaalde systeemonderhoudstaken hoeft u de onderhoudsmodus niet in te schakelen. Houd er echter rekening mee dat het systeem na taken waarvoor dat wél nodig is, extra tijd nodig heeft om opnieuw te starten of opnieuw op te starten nadat u de onderhoudsmodus hebt uitgeschakeld. Het *opnieuw starten* van het systeem duurt slechts een paar minuten (ongeveer drie tot vijf), maar het *opnieuw opstarten* van het systeem duurt ongeveer een half uur. Houd bij het plannen van de onderhoudsperiode rekening met deze extra tijd die uw systeem nodig heeft om volledig operationeel te worden. Zie De onderhoudsmodus in- of uitschakelen, op pagina 128 voor meer informatie.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoud plannen**

Het venster **Onderhoudsperiode plannen** wordt weergegeven.

Stap 3 Gebruik de agenda en het tijdvervolgkeuzemenu om de startdatum en -tijd voor de onderhoudsperiode te selecteren.

Stap 4 Voer de duur van de onderhoudsperiode in door het aantal uren en minuten op te geven.

Stap 5 Selecteer **Plannen**.
De startdatum en -tijd en de duur van de geplande onderhoudsperiode worden weergegeven in het deelvenster Onderhoud.

Opmerking Tijdens de onderhoudsperiode wordt er een foutbericht weergegeven als gebruikers een vergadering proberen te plannen die in de geplande onderhoudsperiode valt.

Volgende stappen

- Zie De onderhoudsmodus in- of uitschakelen voor informatie over het inschakelen van de onderhoudsmodus.
- In Gebruikers e-mailen leest u hoe u gebruikers op de hoogte brengt van systeemonderhoud.

Een geplande onderhoudsperiode wijzigen

U kunt de datum en tijd van een geplande onderhoudsperiode wijzigen of de onderhoudsperiode verwijderen.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Dashboard**.

Stap 3 Selecteer de datum en tijd van het weergegeven systeemonderhoud.

Stap 4 In het venster **Onderhoudsperiode plannen** kunt u het volgende doen:

- een andere begindatum en -tijd invoeren
- de tijdsduur in uren en minuten aanpassen
- **Verwijderen** selecteren om de onderhoudsperiode te verwijderen

Opmerking Als het systeemonderhoud eerder dan gepland is afgerond, kunt u de tijdsduur verkorten of **Verwijderen** selecteren in het venster **Onderhoudsperiode plannen**.

Volgende stappen

Vergeet niet de onderhoudsmodus in te schakelen voordat u systeemeigenschappen wijzigt. In Over de onderhoudsmodus, op pagina 125 leest u voor welke systeemeigenschappen de onderhoudsmodus moet worden ingeschakeld.

Over de onderhoudsmodus

Veel configuratiewijzigingen vereisen dat u uw systeem in onderhoudsmodus plaatst. In de onderhoudsmodus worden conferentieactiviteiten uitgeschakeld, zodat u uw onderhoudsperiode moet plannen om een minimale uitvaltijd voor uw gebruikers te garanderen. We adviseren u een onderhoudsperiode te plannen voordat u de onderhoudsmodus inschakelt, maar dit is niet verplicht. U kunt de onderhoudsmodus op elk gewenst moment inschakelen. De knop **Onderhoudsmodus inschakelen** bevindt zich op de pagina **Dashboard**.

Nadat u hebt bepaald wanneer u het systeemonderhoud wilt uitvoeren, gebruikt u de functie **Onderhoud plannen** op de pagina **Dashboard** om een onderhoudsperiode te plannen. Zie Een onderhoudsperiode plannen, op pagina 123 voor meer informatie. Vervolgens selecteert u de functie **Gebruikers e-mailen** om uw gebruikers vooraf te waarschuwen dat ze geen vergaderingen kunnen bijwonen of hosten tijdens de onderhoudsperiode. Zie Gebruikers e-mailen, op pagina 150 voor meer informatie.

Wanneer de onderhoudsmodus wordt ingeschakeld, wordt de situatie als volgt:

- Actieve vergaderingen worden beëindigd.
- Gebruikers kunnen geen nieuwe vergaderingen plannen of hosten.
- Gebruikers kunnen zich niet bij hun WebEx-site aanmelden vanaf webpagina's, de Microsoft Outlook-invoegtoepassing of mobiele toepassingen.
- Het systeem blijft automatische e-mailmeldingen verzenden aan gebruikers en beheerders.

Gebruik de volgende tabel om te bepalen voor welke taken u de onderhoudsmodus moet inschakelen en welke handeling uw systeem uitvoert nadat u de onderhoudsmodus hebt uitgeschakeld. Als u probeert deze taken uit te voeren terwijl de onderhoudsmodus niet is ingeschakeld, geeft het systeem berichten weer om u hieraan te herinneren.

Taak	Verwijzing	Onderhoudsmodus vereist	Na uitschakeling van de onderhoudsmodus wordt het systeem opnieuw opgestart of opnieuw gestart
Het toevoegen en verwijderen van systemen met hoge beschikbaarheid	Een systeem met hoge beschikbaarheid configureren, op pagina 154	J	Opnieuw opstarten
Openbare toegang toevoegen en verwijderen door een Internet Reverse Proxy te implementeren of te verwijderen	Openbare toegang aan uw systeem toevoegen, op pagina 158 en Openbare toegang uitschakelen, op pagina 160	J	Opnieuw starten
De standaardtaal van het systeem wijzigen	Uw bedrijfsgegevens configureren, op pagina 188	J	Opnieuw starten
De URL's van uw host- of beheerdersaccount wijzigen	Uw site-instellingen wijzigen, op pagina 161	J	Opnieuw starten

Taak	Verwijzing	Onderhoudsmodus vereist	Na uitschakeling van de onderhoudsmodus wordt het systeem opnieuw opgestart of opnieuw gestart
Uw mailserver wijzigen	Een mailserver configureren, op pagina 163	N	N.v.t.
Uw virtuele IP-adres wijzigen	Uw virtuele IP-adres wijzigen, op pagina 158	J	Opnieuw opstarten
Brandinginstellingen configureren en wijzigen	Uw brandinginstellingen configureren, op pagina 189	N	N.v.t.
Een groot deel van de audio-instellingen configureren en wijzigen	Over het configureren van uw audio-instellingen, op pagina 192	J	Opnieuw starten
De toegangsnummers voor de inbelfunctie, weergavenaam en audio-instellingen voor beller-ID configureren en wijzigen	Uw audio-instellingen configureren, op pagina 195	N	N.v.t.
Instellingen voor de servicekwaliteit configureren en wijzigen	Servicekwaliteit (Quality of Service – QoS) configureren, op pagina 198	N	N.v.t.
SNMP-instellingen configureren en wijzigen	Uw SNMP-instellingen configureren, op pagina 169	J	Opnieuw starten
Certificaten configureren	Certificaten beheren, op pagina 226	J	Opnieuw starten of opnieuw opstarten (bepaald door het systeem)
Instellingen voor noodherstel configureren	De noodherstelfunctie gebruiken, op pagina 166	J	Opnieuw starten
FIPS-compatibele codering configureren	FIPS-compatibele codering inschakelen, op pagina 242	J	Opnieuw starten
Opslagservers configureren	Een opslagserver configureren, op pagina 164	J	Opnieuw starten
De beveiliging van de virtuele machine configureren	Beveiliging van de virtuele machine configureren, op pagina 240	J	Opnieuw opstarten

Taak	Verwijzing	Onderhoudsmodus vereist	Na uitschakeling van de onderhoudsmodus wordt het systeem opnieuw opgestart of opnieuw gestart
Systeemgrootte uitbreiden	Het systeem vergroten, op pagina 160	J	Opnieuw starten
Kleine updates en grote upgrades uitvoeren en uw systeem uitbreiden	Het systeem bijwerken, op pagina 95	J	Opnieuw starten
Gedeelde sleutels bijwerken	Certificaten beheren, op pagina 226	J	Opnieuw starten
De systeembrontest gebruiken	De systeembrontest gebruiken, op pagina 254	J	Opnieuw starten

Al uw virtuele machines beschikken over een consolevenster dat aangeeft wanneer de machines zich in de onderhoudsmodus bevinden. U kunt de consolevensters in de overzichtsbalk van vCenter openen (voor navigatie). De consolevensters bevatten de URL van het systeem, het type systeem (primair, hoge beschikbaarheid of openbare toegang), het type implementatie (systeem voor 50, 250, 800 of 2000 gebruikers) en de huidige systeemstatus, die onder meer aangeeft of de onderhoudsmodus is in- of uitgeschakeld en de tijd en datum van de statuswijziging. De tijd die wordt weergegeven, wordt geconfigureerd in de instellingen voor Bedrijfsinfo. Zie Uw bedrijfsgegevens configureren, op pagina 188 voor meer informatie.

Systeemonderhoudstaken voltooien

Wanneer u klaar bent met het wijzigen van uw systeemconfiguratie kunt u de onderhoudsmodus uitschakelen. Afhankelijk van de taken die u hebt uitgevoerd:

- werkt het systeem snel weer normaal, omdat de onderhoudsmodus niet nodig was voor de wijzigingen.
- wordt het bericht weergegeven dat het systeem vanwege de aangebrachte wijzigingen *opnieuw moet worden gestart* en dat dit slechts een paar minuten duurt.
- wordt het bericht weergegeven dat het systeem vanwege de aangebrachte wijzigingen *opnieuw moet worden opgestart* en dat dit, afhankelijk van de omvang van uw systeem, ongeveer een half uur duurt.

Het opnieuw starten van het systeem duurt maar een paar minuten, maar het opnieuw opstarten van het systeem kan tot een halfuur duren. In deze periode zijn de conferentieactiviteiten niet beschikbaar. Het systeem stelt vast welke handeling moet worden uitgevoerd en maakt daar melding van wanneer u de onderhoudsmodus uitschakelt.

Wanneer de onderhoudsmodus is uitgeschakeld, wordt de pagina **Dashboard** vernieuwd. Gebruikers kunnen weer vergaderingen starten als voor alle virtuele machines op de pagina **Systeemeigenschappen** de status Goed (groen) wordt weergeven. Zie De onderhoudsmodus in- of uitschakelen, op pagina 128 voor meer informatie.

Als de onderhoudsmodus is uitgeschakeld maar de geplande onderhoudsperiode nog van kracht is, kunnen gebruikers eerder geplande vergaderingen hosten en bijwonen. Ze kunnen echter pas nieuwe vergaderingen plannen als de onderhoudsperiode is verstreken.

De onderhoudsmodus in- en uitschakelen voor een systeemupgrade

Als u uw systeem *handmatig* upgradet van Cisco WebEx Meetings Server versie 1.x naar versie 2.0, wordt na de implementatie van de virtuele machines voor uw geüpgradede systeem een bericht weergegeven dat het tijd is om de onderhoudsmodus in te schakelen. U moet de onderhoudsmodus handmatig inschakelen.

Als u het systeem *automatisch* upgradet, wordt de onderhoudsmodus automatisch op het juiste moment ingeschakeld en krijgt u een melding wanneer dit gebeurt.

Wanneer het handmatige of automatische upgradeproces is voltooid, schakelt u de onderhoudsmodus handmatig uit op het geüpgradede Cisco WebEx Meetings Server versie 2.0-systeem. Het kan een paar minuten duren voordat de vergaderservice beschikbaar is.

Verwante onderwerpen

Een onderhoudsperiode plannen, op pagina 123
De onderhoudsmodus in- of uitschakelen, op pagina 128

De onderhoudsmodus in- of uitschakelen

Voordat u uw systeemconfiguratie wijzigt, is het raadzaam een onderhoudsperiode te plannen en gebruikers te informeren over de geplande onderhoudstijd. Zie Een onderhoudsperiode plannen, op pagina 123 voor meer informatie.

Opmerking Wanneer de onderhoudsmodus is ingeschakeld, kunnen gebruikers geen vergaderingen plannen of hosten of aan vergaderingen deelnemen. Actieve vergaderingen worden beëindigd.

Voordat u begint

Bij het inschakelen van de onderhoudsmodus worden de conferentieactiviteiten beëindigd en kunnen gebruikers zich niet meer aanmelden bij uw WebEx-site, geen vergaderingen meer plannen of bijwonen en geen vergaderopnamen meer afspelen. Als u de onderhoudsmodus uitschakelt, bepaalt het systeem of *opnieuw starten* (duurt 3 tot 5 minuten) of *opnieuw opstarten* (duurt ongeveer een halfuur) nodig is en maakt het hier melding van. In Over de onderhoudsmodus leest u voor welke systeemtaken de onderhoudsmodus moet worden ingeschakeld.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen**.
Het dialoogvenster **Onderhoudsmodus inschakelen** wordt weergegeven. Lees de informatie over de status van uw systeem wanneer u de onderhoudsmodus inschakelt.

Stap 3 Selecteer **Doorgaan** als u klaar bent om het systeemonderhoud te starten.
Er wordt een bericht weergegeven dat uw systeem zich in de onderhoudsmodus bevindt. De knop **Onderhoudsmodus uitschakelen** wordt weergegeven.

Stap 4 (Optioneel) Maak een back-up van uw virtuele machines.

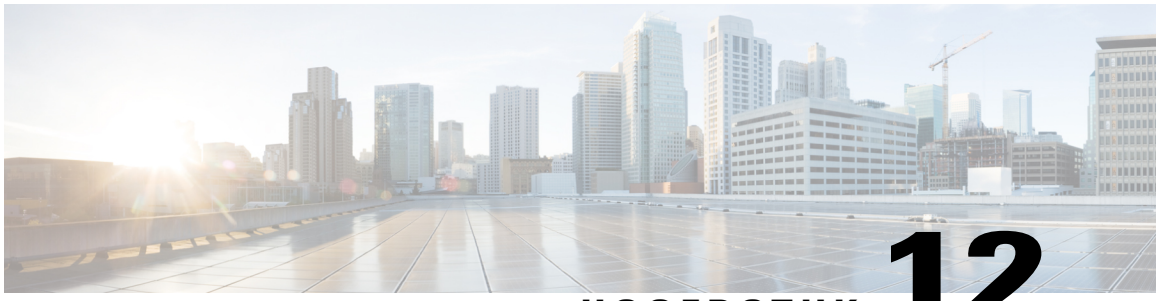
Stap 5 Selecteer **Onderhoudsmodus uitschakelen** wanneer u het configureren van uw systeem hebt voltooid.

Afhankelijk van de aangepaste systeemeigenschappen kan het een paar minuten of ongeveer een half uur duren voor gebruikers zich weer kunnen aanmelden en weer gebruik kunnen maken van de conferentiefuncties.

Stap 6 (Optioneel) Selecteer **Dashboard** > **Systeem** > **Meer weergeven** (in het gedeelte Systeem) om te bepalen of het systeem volledig operationeel is.
De conferentieactiviteiten kunnen worden hervat als de **Status** voor alle weergegeven virtuele machines **Goed** (groen) is.

Volgende stappen

Als de geplande onderhoudsperiode nog van kracht is nadat u de onderhoudsmodus hebt uitgeschakeld, en als uw systeem dan al opnieuw is gestart of opnieuw is opgestart, kunnen gebruikers een directe vergadering starten door **Nu vergaderen** op de pagina **Vergaderingen** te selecteren. Zie 'Een directe vergadering starten' in de *Gebruikershandleiding* op http://www.cisco.com/en/US/products/ps12732/tsd_products_support_maintain_and_operate.html.



HOOFDSTUK 12

Gebruikers beheren

Dit gedeelte beschrijft hoe u gebruikers op uw systeem moet beheren.

- Over het beheren van gebruikers, pagina 131
- Over door komma's en tabs gescheiden bestanden, pagina 132
- gebruikers toevoegen, pagina 138
- Gebruikers bewerken, pagina 138
- Gebruikers activeren, pagina 139
- Gebruikers deactiveren, pagina 139
- Gebruikers via Importeren deactiveren, pagina 140
- Gebruikers importeren, pagina 140
- Gebruikers exporteren, pagina 141
- Gebruikers importeren naar een nieuw systeem met een geëxporteerd bestand, pagina 141
- Traceercodes configureren, pagina 142
- Directory-integratie configureren, pagina 144
- Gebruikersgroepen synchroniseren, pagina 148
- CUCM gebruiken om AXL Web Service en directorysynchronisatie te configureren, pagina 149
- CUCM gebruiken om de LDAP-integratie en -verificatie te configureren, pagina 150
- Gebruikers e-mailen, pagina 150

Over het beheren van gebruikers

U kunt gebruikers individueel toevoegen of lijsten met gebruikers importeren die zijn opgeslagen in een door komma's of tabs gescheiden bestand.

U kunt gebruikersaccounts toevoegen en deactiveren, maar u kunt ze niet verwijderen. Met deactivering kunt u een gebruiker inactief maken en biedt u ook de mogelijkheid om de gebruiker later opnieuw te activeren,

indien nodig. Een opnieuw geactiveerde gebruikersaccount krijgt weer toegang tot vergaderingen, opnames en andere gegevens waar deze toegang tot had voordat deze werd gedeactiveerd.

Het systeem ondersteunt een limiet van 400.000 gebruikersaccounts. Dit aantal staat voor het totaal van zowel actieve als gedeactiveerde gebruikersaccounts. Deze limiet is groot genoeg om aan te passen aan verwachte groei in de gebruikersdatabase.

Om ongeautoriseerde aanmelding in het systeem te voorkomen, moet u ervoor zorgen dat u de gebruikers die uw organisatie verlaten, deactiveert. U kunt gebruikers op de volgende manieren deactiveren:

- Als uw systeem geen geïntegreerde SSO gebruikt, kunt u gebruikers individueel deactiveren of door middel van het importeren van een door komma's of tabs gescheiden bestand met het veld ACTIEF ingesteld op N voor elke gebruiker die u wilt deactiveren. Zie Gebruikers deactiveren, op pagina 139 en Over door komma's en tabs gescheiden bestanden, op pagina 132 voor meer informatie.
- Als uw systeem geïntegreerde SSO gebruikt, moet u gebruikers deactiveren door ze uit de bedrijfslijst in uw SAML 2.0 IdP te verwijderen. Deze procedure wordt niet uitgevoerd door dit product.
- Gebruik de wachtwoordconfiguratiefunctie om gebruikers na een opgegeven tijdsperiode te deactiveren. Zie Uw algemene wachtwoordinstellingen configureren, op pagina 200 voor meer informatie.

Over door komma's en tabs gescheiden bestanden

Als u een spreadsheettoepassing, zoals Microsoft Excel, wilt gebruiken om uw gebruikersgegevens te ordenen, kunt u de spreadsheet opslaan of exporteren als een door komma's of tabs gescheiden bestand (CSV). Uw systeem ondersteunt UCS Transformation Format—8 bit (UTF-8). De tekens die u in uw bestand opgeeft zijn beperkt tot de tekens die in UTF-8 zijn gespecificeerd. Als uw bestand non-ASCII-tekens bevat, controleert u of in het bestand een unicode komma- of tab-scheidingsteken wordt gebruikt.

Als u een door komma's of tabs gescheiden bestand wilt importeren, moeten alle velden in de tabel worden ingevuld. De veldwaarden mogen leeg zijn. Als er een veld ontbreekt, wordt er een foutbericht weergegeven. Bijvoorbeeld 'Onjuiste bestandsindeling. Custom10 is verplicht.'

U kunt maximaal tien **Traceercodegroepen** definiëren. Namen van traceercodegroepen moeten uniek zijn en mogen geen vooraf gedefinieerde veldnamen bevatten (GEBRUIKERS-ID, ACTIEF, VOORNAAM, ACHTERNAAM, E-MAIL, TAAL, HOSTRECHTEN, TIJDZONE).

Veldnaam	Beschrijving	Grootte en type waarde
GEBRUIKERS-ID	Gebruikers-id. **Opmerking** Dit veld wordt automatisch gegenereerd door het systeem en moet worden leeggelaten wanneer u een CSV-bestand importeert.	1 tot 19 alfanumerieke tekens
ACTIEF	Of deze gebruiker wel of niet actief is.	J of N
VOORNAAM	Voornaam van gebruiker.	Reeks met 1 tot 32 tekens

Veldnaam	Beschrijving	Grootte en type waarde
ACHTERNAAM	Achternaam van gebruiker.	Reeks met 1 tot 32 tekens
E-MAIL	Het e-mailadres van de gebruiker.	Reeks met 1 tot 192 alfanumerieke tekens
TAAL	Taal van de gebruiker. Zie Veldwaarden CSV-bestand voor meer informatie.	Reeks met 1 tot 64 tekens
HOSTRECHTEN	Hostrechten.	ADMN of HOST
TIJDZONE	De tijdzone waarin de gebruikers zich bevindt. Zie Veldwaarden CSV-bestand voor meer informatie.	Naam van tijdzone
DIVISIE	Divisie van gebruiker. Voor traceercodegroep 1. Dit veld kan worden ingesteld op de pagina Traceercodes. Zie Traceercodes configureren voor meer informatie.	Reeks met 1 tot 128 tekens
AFDELING	Afdeling van gebruiker. Voor traceercodegroep 2. Dit veld kan worden ingesteld op de pagina Traceercodes. Zie Traceercodes configureren voor meer informatie.	Reeks met 1 tot 128 tekens
PROJECT	Project van gebruiker. Voor traceercodegroep 3. Dit veld kan worden ingesteld op de pagina Traceercodes. Zie Traceercodes configureren voor meer informatie.	Reeks met 1 tot 128 tekens
OVERIGE	Overige informatie. Voor traceercodegroep 4. Dit veld kan worden ingesteld op de pagina Traceercodes. Zie Traceercodes configureren voor meer informatie.	Reeks met 1 tot 128 tekens
AANGEPAST 5	Aangepast veld 5.	Reeks met 1 tot 128 tekens
AANGEPAST 6	Aangepast veld 6.	Reeks met 1 tot 128 tekens
AANGEPAST 7	Aangepast veld 7.	Reeks met 1 tot 128 tekens
AANGEPAST 8	Aangepast veld 8.	Reeks met 1 tot 128 tekens
AANGEPAST 9	Aangepast veld 9.	Reeks met 1 tot 128 tekens
AANGEPAST 10	Aangepast veld 10.	Reeks met 1 tot 128 tekens

Veldwaarden CSV-bestand

Veldwaarden taal

Hier volgen voorbeelden van de landcodewaarden die u in een CSV-bestand kunt gebruiken.

Veldwaarde	Taal
en-us	Amerikaans Engels
zh-cn	Vereenvoudigd Chinees
zh-tw	Traditioneel Chinees
jp	Japans
ko	Koreaans
vr	Frans
de	Duits
it	Italiaans
es-me	Spaans (Castiliaans)
es	Latijns-Amerikaans Spaans
nl	Nederlands
pt-br	Portugees
ru	Russisch

Veldwaarden tijdzone

U kunt de volgende veldwaarden voor de tijdzone (TIMEZONE) instellen in een CSV-bestand.

Veldwaarde	GMT
Marshalleilanden	-12 uur
Samoa	-11 uur
Honolulu	-10 uur
Anchorage	-9 uur
San Francisco	-8 uur

Veldwaarde	GMT
Tijuana	-8 uur
Arizona	-7 uur
Denver	-7 uur
Chihuahua	-7 uur
Chicago	-6 uur
Mexico-Stad	-6 uur
Saskatchewan	-6 uur
Tegucigalpa	-6 uur
Bogota	-5 uur
Panama	-5 uur
New York	-5 uur
Indiana	-5 uur
Caracas	-4,5 uur
Santiago	-4 uur
Halifax	-4 uur
Newfoundland	-3,5 uur
Brasilia	-3 uur
Buenos Aires	-3 uur
Ontvangen	-3 uur
Nuuk	-3 uur
Midden-Atlantisch	-2 uur
Azoren	-1 uur
Reykjavik	0 uur
Londen	0 uur

Veldwaarde	GMT
Casablanca	0 uur
West-Afrika	1 uur
Amsterdam	1 uur
Berlijn	1 uur
Madrid	1 uur
Parijs	1 uur
Rome	1 uur
Stockholm	1 uur
Athene	2 uur
Caïro	2 uur
Pretoria	2 uur
Helsinki	2 uur
Tel Aviv	2 uur
Amman	2 uur
Istanbul	2 uur
Riyadh	3 uur
Nairobi	3 uur
Teheran	3,5 uur
Moskou	4 uur
Abu Dhabi	4 uur
Bakoe	4 uur
Kaboel	4,5 uur
Islamabad	5 uur
Mumbai	5,5 uur

Veldwaarde	GMT
Colombo	5,5 uur
Ekaterinburg	6 uur
Almaty	6 uur
Kathmandu	6,75 uur
Bangkok	7 uur
Beijing	8 uur
Perth	8 uur
Singapore	8 uur
Taipei	8 uur
Kuala Lumpur	8 uur
Tokio	9 uur
Seoul	9 uur
Adelaide	9,5 uur
Darwin	9,5 uur
Yakutsk	10 uur
Brisbane	10 uur
Sydney	10 uur
Guam	10 uur
Hobart	10 uur
Wladivostok	11 uur
Salomonseilanden	11 uur
Wellington	12 uur
Fiji	12 uur

gebruikers toevoegen

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers** > **Gebruiker toevoegen**.

Stap 3 Selecteer uw accounttype (**Host** of **Beheerder**).

Stap 4 Vul de gebruikersgegevens in de velden in. Velden gemarkeerd met * zijn altijd verplicht.

Stap 5 Selecteer **Opslaan**.
Cisco WebEx Meetings Server verzendt een e-mail met een koppeling **Wachtwoord maken** naar de gebruiker. Vóór aanmelding bij de WebEx-site moet de gebruiker een wachtwoord maken.

Opmerking De koppeling Wachtwoord maken verloopt na 72 uur.

Gebruikers bewerken

U kunt gebruikersinformatie wijzigen en gebruikersaccounts activeren of deactiveren met de functie voor gebruiker bewerken.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers**.
De lijst met gebruikers wordt weergegeven. Het standaard aantal gebruikers dat getoond wordt op elke pagina is 50. U kunt ook het vervolgkeuzemenu **Gebruikers per pagina** selecteren en de instelling wijzigen van **50** naar **100**.

Stap 3 Selecteer een gebruiker om te bewerken.

Stap 4 Maak wijzigingen in de velden die kunnen worden bewerkt. Velden gemarkeerd met * zijn altijd verplicht.

Stap 5 Selecteer eventueel het selectievakje **Deze gebruiker dwingen het wachtwoord te wijzigen bij de volgende aanmelding**.

Opmerking Als SSO is ingeschakeld op uw systeem, is deze functie niet van toepassing op hostaccounts.

Stap 6 U kunt ook een account activeren of deactiveren:

- Selecteer **Activeren** om een inactieve account opnieuw te activeren.
- Selecteer **Deactiveren** om een account te deactiveren.

Opmerking Een account activeren of deactiveren slaat geen andere wijzigingen op die u aan de account aangebracht hebt. U moet **Opslaan** selecteren om uw wijzigingen op te slaan.

Stap 7 Selecteer **Opslaan**. Hiermee slaat u uw wijzigen op zonder de status van het account te wijzigen.

Gebruikers activeren

Nadat u hostaccounts en beheerderaccounts hebt toegevoegd, worden deze standaard geactiveerd. Gebruik deze functie om inactieve gebruikers opnieuw te activeren.

U kunt ook een account activeren op de pagina **Gebruiker bewerken**. Zie Gebruikers bewerken, op pagina 138 voor meer informatie.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers**.

Stap 3 Schakel het selectievakje in voor inactieve gebruikers die u wilt activeren.

Stap 4 Selecteer **Acties** > **Activeren**.
De geselecteerde accounts zijn geactiveerd en de status voor elke account moet nu "Actief" zijn.

Gebruikers deactiveren

U kunt accounts van hosts en beheerders deactiveren. Door een account te deactiveren, kan de eigenaar van die accounts het volgende niet doen:

- Aanmelden vanaf webpagina's, de Outlook-invoegtoepassing en mobiele toepassingen.
- Vergaderingen hosten of bijwonen
- Het beheer van het systeem (als de gebruiker een beheerder was)

U kunt ook een account deactiveren op de pagina **Gebruiker bewerken**. Zie Gebruikers bewerken, op pagina 138 voor meer informatie.

Opmerking Beheerders kunnen hun eigen accounts niet deactiveren.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers**.

Stap 3 Schakel het selectievakje in voor actieve gebruikers die u wilt deactiveren.

Stap 4 Selecteer **Acties** > **Deactiveren** en bevestig door te klikken op **OK**.
De geselecteerde accounts zijn gedeactiveerd en de status voor elke account moet nu "Inactief" zijn.

Gebruikers via Importeren deactiveren

U kunt met de functie Importeren gebruikersaccounts deactiveren.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers** > **Gebruikers importeren/exporteren** > **Exporteren**.
Wacht enkele ogenblikken tot de koppeling **Geëxporteerd csv-bestand downloaden** wordt weergegeven.

Stap 3 Selecteer **Geëxporteerd csv-bestand downloaden** en sla dit bestand op uw harde schijf op.

Stap 4 Open het CSV-bestand. In de kolom ACTIVE en breng de volgende wijzigingen aan:

a) Voer N in voor elke gebruiker die u wilt deactiveren.

b) Verwijder alle gegevens van de gebruikers die u niet wilt wijzigen.

Stap 5 Selecteer **Gebruikers** > **Gebruikers importeren/exporteren** > **Importeren**.

Stap 6 Selecteer **Bladeren**, selecteer uw bijgewerkte CSV-bestand, selecteer **Komma** en vervolgens **Importeren**.
De gegevens van de bijgewerkte gebruiker worden overschreven en de account van de geselecteerde gebruiker wordt gedeactiveerd.

Gebruikers importeren

Voordat u begint

Bereid een door komma's of tabs gescheiden bestand voor met de informatie van uw gebruikers. Zie Over door komma's en tabs gescheiden bestanden, op pagina 132 voor meer informatie.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers** > **Gebruikers importeren/exporteren**.
De pagina Gebruikers importeren/exporteren wordt weergegeven.

Stap 3 Selecteer **Importeren**.
De pagina Gebruikers importeren wordt weergegeven.

Stap 4 Selecteer **Bladeren** en selecteer vervolgens het door komma's of tabs gescheiden traceercodebestand dat u wilt importeren.

Stap 5 Selecteer het keuzerondje **Komma** of **Tab** om aan te geven welk bestandstype u importeert.

Stap 6 Selecteer **Importeren**.

Uw bestand is geïmporteerd. Nadat het importeren is voltooid, verstuurt het systeem een e-mail waarin staat hoeveel records zijn geïmporteerd en hoeveel zijn mislukt.

Volgende stappen

Selecteer **Gebruikers** om de gebruikers in uw systeem weer te geven. Zorg ervoor dat uw gebruikers juist zijn geïmporteerd.

Gebruikers exporteren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers** > **Gebruikers importeren/exporteren**.

Stap 3 Selecteer **Exporteren**.
Uw gebruikersgegevens worden geëxporteerd als een CSV-bestand. Het systeem stuur een e-mail naar de beheerder met een koppeling om het geëxporteerde bestand te downloaden.

Gebruikers importeren naar een nieuw systeem met een geëxporteerd bestand

Voer de volgende stappen uit om gebruikers te importeren naar een nieuw systeem met een geëxporteerd bestand.

Procedure

Stap 1 Meld u aan bij de Beheersite van het systeem waaruit u gebruikers wilt exporteren.

Stap 2 Selecteer **Gebruikers** > **Gebruikers importeren/exporteren**.

Stap 3 Selecteer **Exporteren**.
Uw gebruikersgegevens zijn geëxporteerd als een door komma's of tabs gescheiden bestand.

Stap 4 Open het geëxporteerde bestand, verwijder alle gebruikers-id's uit het bestand en sla het bestand opnieuw op.

Stap 5 Meld u aan bij de Beheersite van het systeem waaruit u gebruikers wilt importeren.

Stap 6 Selecteer **Gebruikers** > **Gebruikers importeren/exporteren**.
De pagina Gebruikers importeren/exporteren wordt weergegeven.

Stap 7 Selecteer **Importeren**.
De pagina Gebruikers importeren wordt weergegeven.

Stap 8 Selecteer **Bladeren** en selecteer het bestand dat u hierboven hebt geëxporteerd.

Stap 9 Selecteer het keuzerondje **Komma** of **Tab** om aan te geven welk bestandstype u importeert.

Stap 10 Selecteer **Importeren**.

Uw bestand is geïmporteerd. Nadat het importeren is voltooid, verstuurt het systeem een e-mail waarin staat hoeveel records zijn geïmporteerd en hoeveel zijn mislukt.

Volgende stappen

Selecteer **Gebruikers** om de gebruikers in uw systeem weer te geven. Zorg ervoor dat uw gebruikers juist zijn geïmporteerd.

Traceercodes configureren

U kunt traceercodes configureren om hostgebruik in bepaalde groepen bij te houden. U kunt bijvoorbeeld traceercodes configureren voor projecten of afdelingen. De traceercodes die u configureert, verschijnen als opties wanneer u gebruikers toevoegt of bewerkt.

U moet de volgende zaken configureren voor elke traceercode:

- Traceercodegroep: Configureer uw traceercodegroepen. Traceercodegroepen worden gebruikt wanneer u gebruikers toevoegt en bewerkt. Standaard is dit Divisie, Afdeling, Project, Overig en Aangepast5 tot en met Aangepast10.

Opmerking Namen van traceercodegroepen moeten uniek zijn en mogen geen vooraf gedefinieerde veldnamen bevatten (GEBRUIKERS-ID, ACTIEF, VOORNAAM, ACHTERNAAM, E-MAIL, TAAL, HOSTRECHTEN, TIJDZONE).

- Invoermodus: Selecteer **Tekstveld** of **Vervolgkeuzemenu**.
- Gebruik: Selecteer **Niet gebruikt**, **Optioneel**, of **Verplicht.**

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers** > **Traceercodes**.

Stap 3 Voer optioneel de naam in van elke traceergroep die u wilt configureren in de kolom **Traceercodegroep**. U hoeft de velden niet aan te passen indien u de standaardwaarden wilt gebruiken.

Stap 4 Selecteer **Tekstinvoer** of **Vervolgkeuzemenu** in de kolom **Invoermodus** voor elke traceercode. Indien u **Tekstinvoer** selecteert, voert u uw traceercode in een tekstveld in. Indien u **Vervolgkeuzemenu** selecteert, verschijnt een koppeling **Lijst bewerken** naast uw veld **Invoermodus**. Selecteer de koppeling **Lijst bewerken** om de waarden in het vervolgkeuzemenu te selecteren voor die traceercode. Zie Traceercodes bewerken, op pagina 143 voor meer informatie.

Opmerking Als u **Vervolgkeuzemenu** selecteert voor één van uw traceercodegroepen, moet u **Lijst bewerken** selecteren en een of meer opties selecteren voor het bijhorend vervolgkeuzemenu.

Stap 5 Selecteer **Niet gebruikt**, **Optioneel**, of **Verplicht** in de kolom **Gebruik** voor elke traceercode.

Opmerking U mag enkel het gebruik wijzigen naar **Verplicht** of **Optioneel** nadat u een lijst voor het vervolgkeuzemenu hebt geconfigureerd. Er verschijnt een foutbericht indien u probeert een andere gebruiksinstelling te wijzigen dan **Niet gebruikt** indien u niet eerst de traceercodegroep en invoermodus hebt geconfigureerd.

Stap 6 Selecteer **Opslaan**.
De instellingen voor uw traceercode zijn opgeslagen.

Traceercodes bewerken

Traceercodes worden standaard weergegeven als tekstvakken. Als u opties voor traceercodes wilt weergeven in een vervolgkeuzemenu, moet u een lijst met opties configureren. Nadat u **Vervolgkeuzemenu** van het vervolgkeuzemenu **Invoermodus** hebt geselecteerd, wordt een koppeling **Lijst bewerken** weergegeven.

Voordat u begint

Als u uw traceercodes wilt bewerken, moet u **Gebruikers** > **Traceercodes** selecteren en **Vervolgkeuzemenu** selecteren voor uw **Invoermodus**.

Procedure

Stap 1 Selecteer de koppeling **Lijst bewerken**.
Het dialoogvenster **Traceercodelijst bewerken** wordt weergegeven.

Stap 2 Configureer de velden in het dialoogvenster **Traceercodelijst bewerken**.

a) Selecteer **Alleen actieve codes weergeven** om alleen actieve traceercodes weer te geven wanneer u dit dialoogvenster opent. Hef deze optie op om alle traceercodes weer te geven. Houd er rekening mee dat u deze optie niet kunt selecteren als u traceercodes voor de eerste keer configureert voor elke **Invoermodus**.
b) Selecteer **Ga naar eerste lege traceercode** om naar de eerste pagina met lege codevelden te gaan.
c) **Actief** is standaard geselecteerd. U kunt **Actief** uitschakelen om een traceercode inactief te maken. Inactieve traceercodes worden niet weergegeven in het vervolgkeuzemenu van deze traceercodegroep. Vink **Actief** aan om een inactieve traceercode te activeren.
d) Geef de naam van het menu-item op in het tekstvak **Code**. Limiet: 128 tekens.
e) Selecteer het keuzerondje **Standaard** om dit menu-item de standaardselectie voor het vervolgkeuzemenu te maken.
f) Selecteer **20 regels toevoegen** om 20 extra configureerbare traceercoderegels toe te voegen. Navigatiekoppelingen (**Volgende**, **Vorige** en paginanummers) worden toegevoegd als u meer dan 20 regels weergeeft. Limiet: 500 regels (25 pagina's).
g) Selecteer het keuzerondje **Sorteren** om de sorteermethode (**Niet sorteren**, **Sorteren van laag naar hoog**, **Sorteren van hoog naar laag**) voor de traceercodes in te stellen. Merk op dat **Sorteren** enkel werkt voor de huidige pagina.

Stap 3 Selecteer **Bijwerken** om uw instellingen op te slaan.
Uw instellingen zijn opgeslagen en de pagina **Traceercodelijst bewerken** wordt gesloten.

Directory-integratie configureren

Met Directory-integratie stelt u het systeem in staat om uw gebruikersdatabase van Cisco WebEx Meetings Server in te vullen met gegevens en te synchroniseren met de gebruikersdatabase van Cisco Unified Communications Manager (CUCM), die vervolgens wordt geïntegreerd met een LDAP-directory.

Directory-integratie vereenvoudigt het beheer van gebruikersprofielen op de volgende manieren:

- Importeert gebruikersprofielen uit CUCM naar Cisco WebEx Meetings Server.
- Werkt de Cisco WebEx Meetings Server-database regelmatig bij met nieuwe of gewijzigde gebruikerskenmerken in de CUCM-database, inclusief de voornaam, de achternaam en het e-mailadres van iedere gebruiker. Cisco WebEx Meetings Server onderscheidt gebruikers op basis van hun e-mailadres. Als gebruikers dezelfde voor- en achternaam maar verschillende e-mailadressen hebben, beschouwt Cisco WebEx Meetings Server ze dus als verschillende gebruikers.
- Controleert de CUCM-database regelmatig op vermeldingen van inactieve gebruikers en deactiveert hun gebruikersprofielen in de Cisco WebEx Meetings Server-database.
- Stelt het systeem in staat LDAP-verificatie te gebruiken om gebruikers van de Cisco WebEx Meetings Server-functie voor directory-integratie te verifiëren op basis van de externe directory.
- Ondersteunt volledig gecodeerde LDAP-integratie wanneer Beveiligde LDAP (SLDAP) is ingeschakeld in CUCM en op de LDAP-server.
- Alle gebruikers die in CUCM zijn geconfigureerd, worden gesynchroniseerd naar Cisco WebEx Meetings Server en hun accounts worden geactiveerd. Nadat de synchronisatie is voltooid, kunt u eventueel accounts deactiveren. Alle actieve gebruikers in CUCM worden gesynchroniseerd naar Cisco WebEx Meetings Server. Inactieve gebruikers worden niet geïmporteerd in Cisco WebEx Meetings Server.

Voordat u begint

Zorg ervoor dat aan de volgende vereisten wordt voldaan voordat u een directory-integratie uitvoert:

- We raden u aan om synchronisaties te plannen buiten de piekuren of in het weekend, om de impact ervan op uw gebruikers tot een minimum te beperken.
- Zorg ervoor dat u over een ondersteunde versie van Cisco Unified Communications Manager (CUCM) beschikt. Raadpleeg de Systeemvereisten voor Cisco WebEx Meetings Server voor meer informatie.
- Haal de referenties voor een CUCM-gebruiker met beheerdersrechten op (vereist om een CUCM-server voor directory-integratie toe te voegen).
- U moet een AXL- en LDAP-directoryservice in CUCM configureren voordat u de functie voor directory-integratie kunt gebruiken. CUCM is vereist om gebruikers te importeren in uw Cisco WebEx Meetings Server-systeem. Gebruik CUCM voor het volgende:
  - Cisco AXL Web Service inschakelen
  - Synchronisatie van de Cisco-directory inschakelen
  - LDAP-integratie configureren
  - LDAP-verificatie configureren

Zie CUCM gebruiken om AXL Web Service en directorysynchronisatie te configureren en CUCM gebruiken om de LDAP-integratie en -verificatie te configureren. Raadpleeg de CUCM-documentatie voor meer informatie.

- Zorg ervoor dat alle gebruikers die hostrechten nodig hebben, beschikbaar zijn in CUCM. Gebruikers die niet aan CUCM zijn toegevoegd, kunnen zich niet aanmelden en kunnen geen vergaderingen hosten (alle gebruikers kunnen deelnemen als gast). Maak indien nodig CUCM-groepen of -filters met daarin alleen de gebruikers die u vanuit CUCM wilt importeren.

Opmerking Als u geen CUCM-groepen gebruikt, worden tijdens de eerste directorysynchronisatie alle actieve CUCM-gebruikers in Cisco WebEx Meetings Server geïmporteerd. Inactieve CUCM-gebruikers worden niet geïmporteerd. Tijdens volgende synchronisaties worden alleen actieve nieuwe en gewijzigde gebruikers geïmporteerd. U moet de gebruikersaccounts in Cisco WebEx Meetings Server waaraan u geen hosttoegang wilt verlenen, deactiveren. Cisco WebEx Meetings Server gebruikt alleen een hostlicentie wanneer een gebruiker daadwerkelijk een vergadering host. Accounts die geen vergaderingen hosten, gebruiken ook geen licenties. Zie 'Licenties beheren' in Uw systeem configureren voor meer informatie over licentiegebruik.

- Gebruikers die geen e-mailadres hebben, worden niet geïmporteerd.
- Als gebruikers meerdere accounts in CUCM hebben met dezelfde voor- en achternaam, maar met een ander toegewezen e-mailadres, worden deze adressen bij het importeren in Cisco WebEx Meetings Server als verschillende gebruikers beschouwd. CUCM-gebruikers hebben een unieke gebruikersnaam, dus beheerders kunnen meerdere gebruikersaccounts maken met hetzelfde e-mailadres. Accounts in Cisco WebEx Meetings Server hebben echter een uniek e-mailadres. Als meerdere CUCM-gebruikeraccounts hetzelfde e-mailadres hebben, moet de CUCM-beheerder er vóór het importeren van deze accounts naar Cisco WebEx Meetings Server dus handmatig voor zorgen dat ze allemaal een uniek e-mailadres hebben.
- Wanneer LDAP-verificatie is ingeschakeld, gebruikt Cisco WebEx Meetings Server poort 8443 om verbinding met CUCM te maken als u **Nu synchroniseren** selecteert of als u het selectievakje **Volgende synchronisatie** inschakelt en een datum en tijd invoert.

Procedure

Stap 1 Meld u aan bij uw Cisco WebEx Meetings Server-beheersite.

Stap 2 (Optioneel) Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Opmerking Voor het uitvoeren van een directory-integratie is de onderhoudsmodus niet vereist, maar grote synchronisaties kunnen wel van invloed zijn op de prestaties van het systeem. U kunt de onderhoudsmodus voor uw systeem inschakelen om te voorkomen dat gebruikers het systeem tijdens een synchronisatie gebruiken.

Stap 3 Selecteer **Gebruikers** > **Directory-integratie**.

Stap 4 Voer uw CUCM-servergegevens in als u dit nog niet hebt gedaan:

- Het IP-adres of de volledige domeinnaam (FQDN)
- Gebruikersnaam
- Wachtwoord

De gebruikersnaam en het wachtwoord kunnen uw gebruikersnaam en wachtwoord als CUCM-beheerder of uw AXL-gebruikersnaam en -wachtwoord zijn. Nadat u uw CUCM-gegevens hebt geconfigureerd, wordt het IP-adres of de volledige domeinnaam van uw CUCM-server onder het CUCM-pictogram weergegeven.

Opmerking Als u uw CUCM-instellingen al hebt geconfigureerd, is deze stap niet nodig en kunt u doorgaan met de volgende stap. Zodra u uw CUCM-gegevens hebt geconfigureerd en u deze wilt wijzigen, moet u een complexe procedure volgen die kan leiden tot synchronisatieproblemen. We raden u daarom aan de gegevens achteraf niet te wijzigen.

Stap 5 Selecteer **CUCM-gebruikersgroepen om te filteren** om alleen de gebruikers uit de geselecteerde CUCM-gebruikersgroepen in Cisco WebEx Meetings Server te importeren.

Stap 6 Synchroniseer uw WebEx Meetings Server-systeem met uw LDAP-directoryservice. U kunt op de volgende manieren een synchronisatie uitvoeren:

- Selecteer **Nu synchroniseren** om meteen te synchroniseren.
  Opmerking Zodra de synchronisatie is gestart, kunt u deze niet meer annuleren.
- Schakel het selectievakje **Volgende synchronisatie** in en voer een datum, tijd, en herhaalmechanisme in om toekomstige synchronisaties te plannen.

Als u **Nu synchroniseren** selecteert, voert uw systeem onmiddellijk een synchronisatie uit. Hoe lang dit proces in beslag neemt, is afhankelijk van het aantal gebruikers dat wordt gesynchroniseerd. U ontvangt een e-mailbericht wanneer de synchronisatie is voltooid. De andere beheerders op uw systeem ontvangen geen melding nadat de functie **Nu synchroniseren** is uitgevoerd. Als u een synchronisatie plant, wordt deze uitgevoerd op de opgegeven datum en tijd. Alle beheerders ontvangen een e-mail nadat een geplande synchronisatie is voltooid. Schakel het selectievakje **Volgende synchronisatie** uit als u toekomstige synchronisaties wilt voorkomen.

De volgende kenmerken worden toegewezen tijdens het synchronisatieproces:

CUCM-kenmerk	Cisco WebEx Meetings Server-kenmerk
Voornaam	Voornaam
Achternaam	Achternaam
Mail-id	E-mailadres

Opmerking De voornaam en achternaam zijn in Cisco WebEx Meetings Server componenten van de volledige naam die voor gebruikers wordt weergegeven.

De kenmerken die in Cisco WebEx Meetings Server worden toegewezen, kunnen niet door eindgebruikers worden bijgewerkt.

Als uw synchronisatie mislukt, wordt er een foutbericht weergegeven op de pagina en wordt er een e-mail met gedetailleerde informatie over de fout naar de beheerder verzonden. Selecteer **Logbestand weergeven** voor een gedetailleerde uitleg van de fout. Er worden onder andere logboeken verstrekt met rapporten over gedeactiveerde gebruikers, mislukte gebruikers en een samenvatting.

Nadat u minimaal één synchronisatie hebt uitgevoerd, wordt er een overzicht van uw meest recente synchronisatie weergegeven. In dit overzicht kunt u zien of de synchronisatie wel of niet is voltooid, op welke datum en tijd de synchronisatie is voltooid (waarbij gebruik wordt gemaakt van de tijd en datum die zijn geconfigureerd in de instellingen voor Bedrijfsinfo) en welke wijzigingen door gebruikers zijn aangebracht, waaronder de volgende:

- Toegevoegd - Het aantal nieuwe gebruikers dat is toegevoegd.
- Gedeactiveerd - Het aantal gebruikers dat is gedeactiveerd.

Stap 7 Selecteer **Opslaan** als u uw synchronisatieplanning of uw instellingen voor beheerdersmeldingen hebt geconfigureerd of gewijzigd.

Stap 8 Selecteer het tabblad **Gebruikers** en controleer of de juiste gebruikers zijn gesynchroniseerd.

a) Selecteer **Externe gebruikers** in het vervolgkeuzemenu om de gebruikerslijst te filteren. Zorg ervoor dat de gebruikers die u wilde synchroniseren, zich in de lijst bevinden. Externe gebruikers worden in Cisco WebEx Meetings Server geïmporteerd via een directorysynchronisatie. Als een gebruiker eerst lokaal wordt gemaakt en vervolgens wordt overschreven door een directorysynchronisatie, wordt deze gebruiker een externe gebruiker en geen lokale gebruiker.

b) Selecteer **Lokale gebruikers** om te zien welke gebruikers niet zijn opgenomen in de synchronisatie. Lokale gebruikers worden lokaal gemaakt door een Cisco WebEx Meetings Server-beheerder. Lokale gebruikers kunnen handmatig worden toegevoegd of worden geïmporteerd met een CSV-bestand.

Stap 9 Zorg ervoor dat de synchronisatieplanning van uw CUCM en Cisco WebEx Meetings Server elkaar opvolgen. Eerst moet uw CUCM-synchronisatie worden uitgevoerd en meteen daarna de synchronisatie van Cisco WebEx Meetings Server.

Stap 10 (Optioneel) Schakel het selectievakje **Beheerders op de hoogte brengen wanneer de synchronisatie is voltooid** in of uit en selecteer vervolgens **Opslaan**. Deze optie is standaard geselecteerd en informeert beheerders alleen na een geplande synchronisatie.

Stap 11 Selecteer **LDAP-verificatie inschakelen**.

Opmerking Als uw systeem is geconfigureerd voor het gebruik van SSO, moet u SSO eerst uitschakelen. Zie SSO uitschakelen voor meer informatie. Als uw systeem niet is geconfigureerd voor het gebruik van SSO, wordt de standaardverificatie gebruikt totdat u de LDAP-verificatie inschakelt.

Nadat LDAP is ingeschakeld, raden we beheerders aan de Active Directory-server te gebruiken voor het beheer van gebruikers, inclusief het toevoegen, uitschakelen en wijzigen van gebruikers. Nadat LDAP-verificatie is ingeschakeld, moeten alle deelnemers hun LDAP-referenties gebruiken om zich aan te melden bij de WebEx-site. Beheerders kunnen echter gewoon hun Cisco WebEx Meetings Server-referenties blijven gebruiken om zich aan te melden bij de beheersite.

Stap 12 Zorg ervoor dat uw gebruikers zich met hun AD-domeinreferenties kunnen aanmelden bij het systeem.

Stap 13 Als u de onderhoudsmodus voor uw systeem hebt ingeschakeld, selecteert u **Onderhoudsmodus uitschakelen**.

Stap 14 (Optioneel) Als u een synchronisatie hebt uitgevoerd, kunt u **Nu op de hoogte brengen** selecteren om gebruikers via e-mail op de hoogte te brengen dat er accounts voor ze zijn gemaakt op uw Cisco WebEx Meetings Server-systeem of dat hun accounts zijn gewijzigd. U kunt eventueel ook **Automatisch meldingen verzenden** selecteren, zodat er na de synchronisatie automatisch een e-mail wordt verzonden naar de gebruikers die zijn toegevoegd. Nadat er wijzigingen zijn aangebracht in de verificatie-instellingen (bijvoorbeeld wanneer LDAP is ingeschakeld), wordt het e-mailbericht Gebruikers–Wachtwoord gewijzigd naar de desbetreffende gebruikers verzonden.
Wanneer u **Nu op de hoogte brengen** selecteert

- Alle gebruikers ontvangen slechts eenmalig een melding. Bij volgende synchronisaties worden er geen extra e-mails meer verzonden.
- Gebruikers die een melding moeten ontvangen' geeft aan welke gebruikers allemaal actief zijn en nog geen melding hebben ontvangen.
- Ontvangen inactieve gebruikers of lokale gebruikers geen melding.

- Ontvangt de desbetreffende gebruiker een e-mail wanneer er een lokale gebruiker aan Cisco WebEx Meetings Server wordt toegevoegd. Deze gebruiker moet echter worden toegevoegd op uw CUCM Active Directory-server voordat hij of zij zich kan aanmelden bij de WebEx-site.
- Kunt u alleen meldingen verzenden naar gebruikers die zijn toegevoegd met de synchronisatiefunctie.
- Kan het een aantal minuten duren voordat uw e-mailmeldingen naar uw gebruikers worden verzonden. Deze vertraging is het gevolg van verschillende factoren die buiten uw Cisco WebEx Meetings Server-systeem liggen, inclusief uw e-mailserver, problemen met de netwerkverbinding en anti-spamprogramma's die voor de afzonderlijke e-mailaccounts zijn geïnstalleerd.

Uw systeem verzendt de volgende e-mails:

- Iedere gebruiker die tijdens een synchronisatie voor de eerste keer in uw systeem wordt geïmporteerd, ontvangt een AD-activeringsmail. Gebruikers ontvangen deze e-mail niet bij volgende synchronisaties.
- Gebruikers die lokaal op uw systeem worden gemaakt, ontvangen de e-mail Gebruikerswachtwoord–Gewijzigd.

Zie Over e-mailsjablonen voor informatie over het aanpassen van deze e-mailsjablonen.

Opmerking Als u directory-integratie met LDAP-verificatie gebruikt, worden gebruikers die in CUCM zijn geconfigureerd als hosts met Cisco WebEx Meetings Server gesynchroniseerd en moeten ze zich met hun gebruikersgegevens aanmelden bij hun WebEx-site. Als u het accounttype van een geïmporteerde gebruiker wijzigt van host in beheerder, ontvangt de gebruiker echter een e-mail met een koppeling waarmee hij of zij een wachtwoord kan maken. De gebruiker kan op deze koppeling klikken en een nieuw wachtwoord voor Cisco WebEx Meetings Server invoeren. De gebruiker gebruikt dit nieuwe wachtwoord om zich bij de beheerwebsite aan te melden, maar blijft voor de WebEx-site zijn of haar LDAP-gebruikersgegevens gebruiken.

Gebruikersgroepen synchroniseren

Een beheerder kan groepen met gebruikers maken in CUCM. Een beheerder kan bijvoorbeeld een gebruikersgroep maken die bestaat uit gebruikers die Cisco WebEx Meetings Server mogen gebruiken. Vanuit CWMS kan de beheerder filters gebruiker en bepaalde gebruikers importeren door bepaalde gebruikersgroepen te selecteren.

Voordat u begint

Gebruik CUCM om groepen gebruikers te maken. Raadpleeg het gedeelte "Gebruikersbeheer configureren" in de *Beheerdershandleiding van Cisco Unified Communications Manager*http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html voor meer informatie.

Procedure

Stap 1 Meld u aan bij uw Cisco WebEx Meetings Server-beheersite.

Stap 2 Selecteer **Gebruikers** > **Directory-integratie**.

Stap 3 Selecteer de koppeling **CUCM-gebruikersgroepen om te filteren**.

Stap 4 Schakel het selectievakje in van de gebruikersgroepen die u wilt synchroniseren.

Opmerking Als er geen groepen worden geselecteerd, worden bij de directory-integratie alle gebruikersgroepen gesynchroniseerd.

Stap 5 Selecteer **Opslaan**.

Stap 6 Selecteer Nu synchroniseren om de synchronisatie uit te voeren. Hoe lang dit proces in beslag neemt, is afhankelijk van het aantal gebruikers dat wordt gesynchroniseerd.

Opmerking Het systeem onthoudt welke gebruikersgroepen al eerder zijn gesynchroniseerd. Als u geen gebruikersgroep selecteert die al eerder is gesynchroniseerd, worden de gebruikers in de niet-geselecteerde gebruikersgroep tijdens het synchronisatieproces gedeactiveerd.

Wanneer de synchronisatie is voltooid, geeft het systeem het aantal toegevoegde en gedeactiveerde gebruikers weer.

Stap 7 Selecteer **Logbestand weergeven** om samenvattingsinformatie te bekijken over de gebruikers die zijn geïmporteerd of gedeactiveerd tijdens het synchronisatieproces.

CUCM gebruiken om AXL Web Service en directorysynchronisatie te configureren

Gebruik CUCM om AXL Web Service en directorysynchronisatie te configureren.

Voordat u begint

Voer deze procedure uit voordat u de functie Directory-integratie gebruikt. Zie Directory-integratie configureren, op pagina 144 voor meer informatie.

Procedure

	Opdracht of actie	Doel
Stap 1	Meld u aan bij uw CUCM-account.	
Stap 2	Selecteer in het vervolgkeuzemenu in de rechterbovenhoek **Cisco Unified Serviceability** en selecteer vervolgens **Start**.	
Stap 3	Selecteer **Tools** > **Service-activering**.	
Stap 4	Selecteer **Cisco AXL Web Service** en **Cisco DirSync** en selecteer vervolgens **Opslaan**.	

Volgende stappen

Gebruik CUCM om de LDAP-integratie en -verificatie te configureren als u dit nog niet hebt gedaan. Zie CUCM gebruiken om de LDAP-integratie en -verificatie te configureren, op pagina 150 voor meer informatie.

CUCM gebruiken om de LDAP-integratie en -verificatie te configureren

Gebruik CUCM om de LDAP-integratie en -verificatie te configureren.

Opmerking Als CUCM is geconfigureerd voor directory-integratie, kunt u ervoor kiezen om SSO-, LDAP- of lokale verificatie te gebruiken.

Voordat u begint

Voer deze procedure uit voordat u de functie Directory-integratie gebruikt. Zie Directory-integratie configureren voor meer informatie.

Procedure

	Opdracht of actie	Doel
Stap 1	Meld u aan bij uw CUCM-account.	
Stap 2	Selecteer in het vervolgkeuzemenu in de rechterbovenhoek **Cisco Unified CM Administration** en selecteer vervolgens **Start**.	
Stap 3	Selecteer **Bestand** > **LDAP** > **LDAP-systeem**.	
Stap 4	Selecteer achtereenvolgens **Synchroniseren vanaf de LDAP-server inschakelen**, de **Microsoft Active Directory** voor het type LDAP-server, de **SAM-accountnaam** van het LDAP-kenmerk voor de gebruikers-id en **Opslaan**.	
Stap 5	Schakel het selectievakje voor uw LDAP-server in en selecteer vervolgens **Nieuwe toevoegen**.	
Stap 6	Vul de velden op de pagina LDAP-directory in en selecteer vervolgens **Opslaan**.	
Stap 7	Schakel op de pagina LDAP-verificatie het selectievakje **LDAP-verificatie voor eindgebruikers gebruiken** in, vul de velden op de pagina in en selecteer vervolgens **Opslaan**.	

Volgende stappen

Gebruik CUCM om Cisco AXL Web Service en Cisco Directory Sync te configureren als u dit nog niet hebt gedaan. Zie CUCM gebruiken om AXL Web Service en directorysynchronisatie te configureren voor meer informatie.

Gebruikers e-mailen

Gebruik dit hulpprogramma om een e-mail naar uw gebruikers te verzenden.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Gebruikers** > **Gebruikers e-mailen**.

Stap 3 Voer in het veld **Aan** het e-mailadres van een doelgebruiker in, of een e-mailalias.

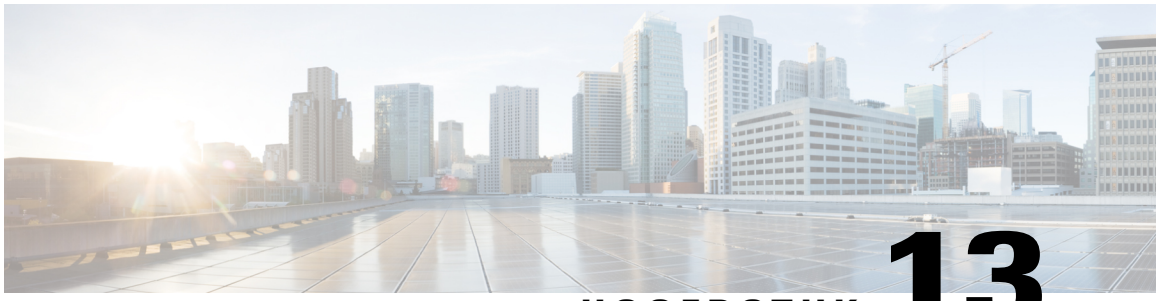
Stap 4 Voer indien gewenst in het veld **BCC** e-mailadressen in.

Stap 5 Voer in het veld **Onderwerp** uw onderwerp in.

Stap 6 Voer in het veld **Bericht** uw bericht in.

Stap 7 Selecteer **Verzenden**.
Uw e-mail wordt verzonden.

Opmerking Het kan een paar minuten duren voordat uw e-mails door de gebruikers worden ontvangen. Deze vertraging kan door verschillende factoren buiten het Cisco WebEx Meetings Server-systeem om worden veroorzaakt, zoals uw e-mailserver, de snelheid van de netwerkverbinding en spaminstellingen van individuele e-mailaccounts.



HOOFDSTUK 13

Uw systeem configureren

Deze module beschrijft hoe u de beheerpagina's moet gebruiken om uw systeem te configureren.

- Systeemeigenschappen configureren, pagina 153
- Algemene instellingen configureren, pagina 161
- Servers configureren, pagina 163
- Uw SNMP-instellingen configureren, pagina 169
- Licenties beheren, pagina 176

Systeemeigenschappen configureren

Configureer uw systeemeigenschappen door Systeem en Meer weergeven in de Systeemsectie te selecteren.

De instellingen van uw virtuele machine aanpassen

Gebruik deze functie om de instellingen van uw virtuele machine te wijzigen.

Opmerking Gebruik VMware vCenter niet om de instellingen van uw virtuele machine te bewerken.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer **Meer weergeven** in het systeemgedeelte.

Stap 3 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 4 Om de instellingen van een virtuele machine te wijzigen, selecteert u de koppeling van de naam van de virtuele machine in het gedeelte Primair systeem of systeem met hoge beschikbaarheid.

Stap 5 U kunt de volgende instellingen van de virtuele machine aanpassen:

- Volledige domeinnaam: De FQDN van uw systeem.

- Virtuele machine: Het IP-adres van uw virtuele machine.
- Primaire DNS-server
- Secundaire DNS-server
- Subnetmasker/prefix
- Gateway

Opmerking U kunt uw systeem configureren met IPv4 of IPv6-instellingen voor virtuele machines. Tijdens het implementeren kunt u alleen IPv4-instellingen configureren, maar op deze pagina kunt u uw machine bijwerken naar IPv6.

Stap 6 Selecteer **Opslaan**.
Uw wijzigingen worden opgeslagen en de virtuele machine wordt opnieuw opgestart.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Volgende stappen

Indien u wijzigingen uitvoert in één van uw virtuele machines, moet u nieuwe certificaten ophalen voor elke virtuele machine op uw systeem, tenzij u wildcardcertificaten gebruikt voor systemen in hetzelfde domein. Zie Certificaten beheren, op pagina 226 voor meer informatie.

Een systeem met hoge beschikbaarheid configureren

Een systeem met hoge beschikbaarheid is een redundant systeem dat voor een back-up zorgt wanneer er een fout optreedt in het primaire systeem.

Opmerking Schakel de onderhoudsmodus in voordat u een systeem met hoge beschikbaarheid toevoegt of verwijdert. Houd er, wanneer u een onderhoudsperiode voor deze taak plant, rekening mee dat het systeem opnieuw zal worden opgestart wanneer u de onderhoudsmodus uitschakelt. Het opnieuw opstarten duurt ongeveer een half uur, afhankelijk van de omvang van uw systeem.

Een systeem met hoge beschikbaarheid toevoegen

Opmerking De meeste functies op uw systeem met hoge beschikbaarheid zijn verboden. Zo hebt u bijvoorbeeld geen toegang tot upgrades, SNMP-configuratie, opslagtoegang en e-mailservers op uw systeem met hoge beschikbaarheid. U kunt de systeemeigenschappen bekijken, maar kunt geen wijzigingen aanbrengen.

Opmerking Voltooi de volgende procedure op het primaire systeem.

Voordat u begint

- Installeer Cisco WebEx op een tweede virtuele machine vanuit een OVA-bestand, die u wilt gebruiken als uw systeem met hoge beschikbaarheid.

Opmerking De grootte van uw systeem met hoge beschikbaarheid moet hetzelfde zijn als het primaire systeem.

- Uw systeem met hoge beschikbaarheid moet worden geconfigureerd met dezelfde OVA en patch als uw primaire systeem. Indien de versies van uw primaire systeem en uw systeem met hoge beschikbaarheid niet overeenstemmen, wordt u gevraagd bij te werken naar het hoogste versieniveau.
- Kopieer de volledige domeinnaam (FQDN) van de virtuele machine met hoge beschikbaarheid. U moet de FQDN hebben om uw systeem met hoge beschikbaarheid toe te voegen.
- Controleer of alle virtuele machines normaal werken. Bepaal de status van de virtuele machine door de systeemmonitor te bekijken zoals beschreven in Informatie over uw dashboard, op pagina 115.
- We raden u aan een momentopname te maken op de virtuele machines met hoge beschikbaarheid voordat u deze procedure uitvoert. Herhaal de procedure vanaf de momentopname indien er een fout optreedt.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen**.

Stap 3 Selecteer de koppeling **Meer weergeven** op het primaire systeem, in de Systeemsectie.

Stap 4 Selecteer **Systeem met hoge beschikbaarheid toevoegen**.

Stap 5 Volg de instructies op de pagina **Systeemeigenschappen** om dit HA-systeem toe te voegen.

Stap 6 Voer de FQDN van de virtuele machine van de beheersite in van de machine met hoge beschikbaarheid en selecteer **Doorgaan**.
We zullen de gereedheid van zowel het primaire systeem als het HA-systeem valideren voor deze HA-toevoeging.

- Als beide systemen klaar zijn, ziet u een groene knop **Toevoegen**. Selecteer niets totdat u uw systeem in de onderhoudsmodus hebt geplaatst.
- Als een systeem niet klaar is, ziet u een foutbericht. Herstel de fout en probeer de procedure voor hoge beschikbaarheid nogmaals toe te voegen.

Stap 7 Selecteer **Toevoegen**.

Opmerking Als de fout 'Foutcode: Database-64' wordt weergegeven, herhaalt u deze procedure met gebruik van de momentopname van de virtuele machines met hoge beschikbaarheid.

Uw systeem met hoge beschikbaarheid wordt toegevoegd en automatisch geconfigureerd om te werken als back-up indien het primaire systeem uitvalt.

Stap 8 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem wordt opnieuw opgestart nadat u de onderhoudsmodus hebt uitgeschakeld. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Systeem met hoge beschikbaarheid verwijderen

Voordat u begint

U moet momenteel een secundair systeem hebben geconfigureerd als uw systeem met hoge beschikbaarheid.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen**.

Stap 3 Selecteer de koppeling **Meer weergeven** in de Systeemsectie

Stap 4 Selecteer **Systeem met hoge beschikbaarheid verwijderen**.
De pagina **Systeem met hoge beschikbaarheid verwijderen** wordt weergegeven en toont de volledige domeinnaam (FQDN) van uw systeem met hoge beschikbaarheid.

Stap 5 Selecteer **Doorgaan**.

Opmerking Nadat u een systeem met hoge beschikbaarheid hebt verwijderd, kunt u hetzelfde systeem met hoge beschikbaarheid niet terug toevoegen aan uw site. Om hoge beschikbaarheid opnieuw te configureren, moet u opnieuw beginnen door een systeem met hoge beschikbaarheid opnieuw te implementeren vanaf het OVA-bestand. Zie Een systeem met hoge beschikbaarheid toevoegen, op pagina 73 voor meer informatie.

Uw systeem met hoge beschikbaarheid is verwijderd.

Stap 6 Open VMware vCenter en verwijder het systeem met hoge beschikbaarheid met de opdracht **Delete from Disk**.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem wordt opnieuw opgestart nadat u de onderhoudsmodus hebt uitgeschakeld. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Systeemgedrag na componentstoringen

Wanneer specifieke media- en platformcomponenten die worden uitgevoerd op een virtuele machine crashen, worden deze componenten automatisch opnieuw opgestart door het systeem. Getroffen vergaderingen worden overgenomen door andere beschikbare hulpmiddelen op dezelfde of een andere virtuele machine in het systeem (bij andere systemen dan een standalone-systeem met 50 gebruikers).

Systemen met hoge beschikbaarheid

Bij systemen met hoge beschikbaarheid (HA, High Availability) herstelt Cisco WebEx Meetings Server de volgende componenten wanneer er een storing van één component optreedt:

- Eén service op één virtuele machine.
- Een virtuele machine.

- Eén fysieke server of blade die maximaal twee virtuele machines host (mits de lay-out van de virtuele machine voldoet aan de specificaties die zijn vermeld in de *Systeemvereisten voor Cisco WebEx Meetings Server* en de *Planningsgids voor Cisco WebEx Meetings Server*).
- Eén netwerkkoppeling, indien het netwerk wordt voorzien op een volledig redundante wijze.
- Eén CUCM-knooppunt (CUCM, Cisco Unified Communications Manager), indien CUCM wordt voorzien op redundante wijze.

Na een storing van één component gedraagt het Cisco WebEx Meetings Server-systeem zich als volgt:

- Gedurende een periode van maximaal drie minuten kunnen het delen van toepassingen, audio/spraakverbindingen via de computer en video worden onderbroken. Cisco WebEx Meetings Server geeft drie minuten de tijd om de storing te detecteren en om alle getroffen vergaderingsclients automatisch opnieuw te verbinden. Het is niet nodig voor gebruikers om hun vergaderingsclients te sluiten en zich opnieuw aan te melden bij de vergadering.
- Sommige storingen kunnen ervoor zorgen dat audioverbindingen bij teleconferenties worden verbroken. Als dat gebeurt, moeten gebruikers zich handmatig opnieuw verbinden. Het moet mogelijk zijn om binnen twee minuten de verbinding te herstellen.
- Bij sommige storingen worden mogelijk niet alle clients en vergaderingen getroffen. Vergaderverbindingen worden meestal verdeeld over meerdere virtuele machines en hosts.

Aanvullende informatie voor een systeem met 2000 gebruikers

Een systeem met 2000 gebruikers biedt enkele functionaliteiten met hoge beschikbaarheid zonder het toevoegen van een HA-systeem. Bij een systeem met 2000 gebruikers zonder hoge beschikbaarheid:

- Uw systeem functioneert nog steeds na het verlies van virtuele machines voor media en web, maar de capaciteit van uw systeem is aangetast.
- Het verlies van de virtuele beheermachine zorgt ervoor dat het systeem onbruikbaar wordt.

Bij een systeem met 2000 gebruikers met hoge beschikbaarheid:

- Het verlies van één virtuele machine (beheer, media of web) is niet van invloed op het systeem. Uw systeem blijft actief op volledige capaciteit, zelfs na het verlies van één fysieke server die de primaire virtuele machines host (beheer en media of web en media) of de virtuele machines met hoge beschikbaarheid (beheer en media of web).
- Wanneer een virtuele machine met een storing opnieuw is opgestart, wordt deze weer opgenomen in het systeem en keert het systeem terug naar de normale bedrijfstoestand.
- Wanneer er een storing optreedt bij een virtuele mediamachine, worden de vergaderingen die op die machine worden gehost kort onderbroken, maar wordt de vergadering overgenomen door een alternatieve virtuele mediamachine. Gebruikers moeten zich handmatig opnieuw aanmelden bij de audio- en videosessies op het bureaublad.
- Wanneer er een storing optreedt bij een virtuele webmachine, treedt er ook een storing op bij de websessies die op die virtuele machine worden gehost. Gebruikers moeten zich opnieuw aanmelden bij de Cisco WebEx-site en een nieuwe browsersessie openen die op een andere virtuele webmachine wordt gehost.
- Wanneer er een storing optreedt bij een virtuele beheermachine, treedt er ook een storing op bij alle bestaande beheerderssessies. Beheerders moeten zich opnieuw aanmelden bij de beheerwebsite en een nieuwe browsersessie openen die op een andere virtuele beheermachine wordt gehost. Er kan ook een korte onderbreking optreden bij bestaande vergadersessies van beheerders of eindgebruikers.

Uw virtuele IP-adres wijzigen

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** en selecteer **Meer weergeven** in het systeemgedeelte.

Stap 4 Selecteer in het gedeelte Virtueel IP-adres een koppeling in de kolom Type.

Voorbeeld:
Selecteer **Privé** voor het privé virtuele IP-adres.

Stap 5 Voer uw nieuw virtueel IP-adres in het dialoogvenster VIP IPv4-adres in.

Stap 6 Selecteer **Opslaan**.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem wordt opnieuw opgestart nadat u de onderhoudsmodus hebt uitgeschakeld. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Opmerking Het opnieuw opstarten duurt ongeveer een half uur. Als u een onderhoudsperiode voor systeemonderhoud plant waarin deze taak wordt uitgevoerd, trek dan ook tijd uit om het systeem opnieuw te laten opstarten. Zie Een onderhoudsperiode plannen, op pagina 123 voor meer informatie.

Openbare toegang configureren

Met publieke toegang kunnen personen buiten uw netwerk vergaderingen hosten of bijwonen via het internet of mobiele apparaten. Door openbare toegang uit te schakelen, worden de instellingen van het openbare virtuele IP-adres van uw WebEx-site URL's verwijderd en externe toegang tot uw site beëindigd.

Openbare toegang aan uw systeem toevoegen

Voordat u begint

Om publieke toegang in te schakelen, moet u eerst een reverse proxy virtuele machine configureren die als uw systeem voor publieke toegang werkt.

Start VMware vCenter en voer het volgende uit:

- Maak een back-up van uw virtuele machines met behulp van VMware-gegevensherstel (vSphere 5.0) of VMware vSphere-gegevensbeveiliging (vSphere 5.1). Dit geeft u de gelegenheid om indien nodig uw wijzigingen ongedaan te maken. Zie Een back-up maken met VMware vCenter, op pagina 4 voor meer informatie.
- Implementeer een reverse proxy-virtuele machine met gebruik van hetzelfde OVA-bestand dat u hebt gebruikt om uw virtuele beheermachine te implementeren. Uw Reverse proxy virtuele machine moet op hetzelfde subnet zitten als het publieke virtuele IP-adres. Zie Openbare toegang toevoegen, op pagina 32 voor meer informatie.

Opmerking Als u een systeem met hoge beschikbaarheid hebt, moet u ook een Reverse Proxy-virtuele machine implementeren voor uw systeem met hoge beschikbaarheid.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de Systeemsectie.

Stap 4 Selecteer **Openbare toegang toevoegen**.

Stap 5 Voer uw Internet Reverse Proxy virtuele machine in, in het veld **FQDN**.

Opmerking Er zijn twee velden voor volledige domeinnaam (FQDN) indien uw systeem is geconfigureerd voor hoge beschikbaarheid. Voer uw FQDN met hoge beschikbaarheid in het tweede veld in.

Stap 6 Selecteer **Virtuele machines detecteren**.

- Als uw systeem niet geconfigureerd is voor hoge beschikbaarheid, verschijnt een tabel die de Internet Reverse Proxy virtuele machine weergeeft.
- Als uw systeem geconfigureerd is voor hoge beschikbaarheid, verschijnt een tabel die de Internet Reverse Proxy virtuele machine van het primaire systeem en de Internet Reverse Proxy virtuele machine met hoge beschikbaarheid weergeven.

Als uw systeem updates heeft die niet compatibel zijn met de OVA-versie die u hebt gebruikt om de Reverse Proxy-virtuele machine te creëren, ontvangt u een foutmelding en kunt u niet verdergaan totdat u de Reverse Proxy-virtuele machine opnieuw hebt geïmplementeerd aan de hand van een OVA-bestand dat compatibel is met de updates op uw primaire systeem.

Stap 7 Selecteer **Doorgaan**.

Stap 8 Voer het IP-adres van hetzelfde subnet in dat u gebruikte om uw Internet Reverse Proxy virtuele machine te configureren in het veld **Openbaar virtueel IPv4 (VIP)-adres** en selecteer **Opslaan**.
Uw systeem is bijgewerkt en publieke toegang is geconfigureerd. Zorg dat u uw browservenster openhoudt gedurende het gehele proces.

Als uw primair systeem kleine updates vereist die compatibel zijn met de OVA-versie die u gebruikte om de Internet Reverse Proxy virtuele machine te creëren, worden ze automatisch toegepast op uw Internet Reverse Proxy virtuele machine.

Stap 9 Als uw systeem kleine updates vereist, wordt u gevraagd om **Opnieuw starten** te selecteren nadat de updates voltooid zijn. Als er geen updates nodig zijn, gaat u verder met de volgende stap.
Nadat uw systeem opnieuw opstart, ontvangt u een bevestigingsbericht dat aangeeft dat u publieke toegang hebt toegevoegd.

Stap 10 Controleer uw configuratie. Indien u tevreden bent, kunt u de back-up van de virtuele machine verwijderen die u vóór het uitvoeren van deze procedure hebt geconfigureerd.

Stap 11 Selecteer **Klaar**.

Stap 12 Controleer of uw beveiligingscertificaten nog steeds geldig zijn. Deze procedure wijzigt uw virtuele machine en kan dus uw certificaten beïnvloeden. Uw systeem biedt indien nodig een zelfondertekend certificaat om

uw systeem te laten werken tot u uw certificaten opnieuw kunt configureren. Zie Certificaten beheren, op pagina 226 voor meer informatie.

Stap 13 Voer indien nodig wijzigingen uit aan uw DNS-servers.

Stap 14 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Openbare toegang uitschakelen

Voordat u begint

Maak een back-up van uw virtuele machines met behulp van VMware-gegevensherstel (vSphere 5.0) of VMware vSphere-gegevensbeveiliging (vSphere 5.1). Dit geeft u de gelegenheid om uw wijzigingen ongedaan te maken indien nodig. Zie Een back-up maken met VMware vCenter, op pagina 4 voor meer informatie. Zorg dat u uw virtuele machines inschakelt nadat uw back-up voltooid is.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de Systeemsectie.

Stap 4 Selecteer de gewenste site, selecteer **Publieke toegang uitschakelen** en selecteer **Doorgaan**.
Openbare toegang is verwijderd van de site.

Opmerking Nadat u publieke toegang verwijdert van uw site, kunt u dezelfde proxy virtuele machine niet toevoegen aan die site. Om publieke toegang opnieuw te configureren, moet u opnieuw beginnen door een reverse proxy-virtuele machine opnieuw te implementeren vanaf het OVA-bestand. Zie Openbare toegang aan uw systeem toevoegen, op pagina 158 voor meer informatie.

Stap 5 Selecteer **Klaar**.

Stap 6 Open VMware vCenter, schakel uit en verwijder de Internet Reverse Proxy machine (en Internet reverse proxy machine met hoge beschikbaarheid indien geïmplementeerd) van uw systeem.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Het systeem vergroten

Voordat u begint

Raadpleeg, voordat u een systeemuitbreiding uitvoert, Uw systeem uitbreiden naar een groter systeemformaat. Hierin worden de stappen beschreven die u moet uitvoeren voordat u deze functie gebruikt en leest u hoe u uw systeem kunt uitbreiden door middel van automatische of handmatige implementatie.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de systeemsectie.

Stap 4 Selecteer **Systeemgrootte uitbreiden**.

Stap 5 Selecteer **Doorgaan**.
Uw systeem controleert de verbinding met de virtuele machines. Als er verbindingsproblemen zijn met een of meer virtuele machines, moet u de problemen oplossen voordat u kunt verdergaan. Als er geen verbindingsproblemen zijn, voert uw systeem automatisch een back-up uit. Nadat de back-up is voltooid, krijgt u een melding dat u kunt verdergaan met uw uitbreiding.

Stap 6 Implementeer het OVA-bestand aan de hand van één van de volgende methodes:

- Het systeem uitbreiden met automatische implementatie
- Het systeem uitbreiden met handmatige implementatie

U krijgt een melding van het systeem zodra de uitbreiding voltooid is.

Stap 7 Selecteer **Opnieuw opstarten**.

Stap 8 Meld u aan bij de Beheersite.

Stap 9 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Algemene instellingen configureren

Om uw algemene instellingen te openen, selecteert u **Systeem** en de koppeling **Meer weergeven** onder Configuratie > Algemene instellingen. Algemene instellingen omvatten de volgende functies:

- Site-instellingen—Gebruik deze functie om uw site-URL te configureren of te wijzigen. Deze functie toont ook het privé virtuele IP-adres van uw site en het openbare virtuele IP-adres van uw site.
- Beheerinstellingen-Gebruik deze functie om de URL van uw beheersite te configureren of te wijzigen. Deze functie toont ook het privé virtuele IP-adres van uw beheersite.

Uw site-instellingen wijzigen

Gebruik deze functie om de URL van uw site te wijzigen. U kunt de instelling van de URL van uw oorspronkelijke site instellen tijdens het implementeren. Raadpleeg URL's van WebEx-site en WebEx-beheer, op pagina 34 voor meer informatie over de configuratie van de URL van een site en naamconventies.

Voordat u begint

Zorg dat u de URL van uw oorspronkelijke site op de DNS-server behoudt. Leid de URL van de oorspronkelijke site om naar de URL van de bijgewerkte site. Indien gebruikers proberen de oorspronkelijke URL te gebruiken,

en u hebt deze niet omgeleid naar de nieuwe URL, zullen zij geen vergaderingen kunnen hosten of bijwonen of inloggen vanaf webpagina's, productiviteitstools en mobiele apps.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** > **Configuratie** > **Algemene instellingen** > **Meer weergeven**.

Stap 4 Selecteer in het gedeelte Site-instellingen **Bewerken**.

Stap 5 Voer de URL van uw nieuwe site in het dialoogvenster in en selecteer **Opslaan**.

Stap 6 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Volgende stappen

Werk uw sitecertificaat bij om veilige toegang te garanderen. Zie Certificaten beheren, op pagina 226 voor meer informatie.

Uw beheerinstellingen wijzigen

U kunt de instelling van de URL van uw oorspronkelijke beheersite instellen tijdens het implementeren. Raadpleeg URL's van WebEx-site en WebEx-beheer, op pagina 34 voor meer informatie over de configuratie van een beheersite en naamconventies.

Voordat u begint

Zorg dat u de URL van uw oorspronkelijke beheersite op de DNS-server behoudt. Leid de URL van de oorspronkelijke beheersite om naar de URL van de bijgewerkte beheersite. Indien gebruikers proberen de oorspronkelijke URL te gebruiken, en u hebt deze niet omgeleid naar de nieuwe URL, zullen zij geen vergaderingen kunnen hosten of bijwonen of inloggen vanaf webpagina's, productiviteitstools en mobiele apps.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** > **Configuratie** > **Algemene instellingen** > **Meer weergeven**.
De pagina **Algemene instellingen** wordt weergegeven.

Stap 4 Selecteer in het deel Beheersite-instellingen **Bewerken**.

Stap 5 Voer de URL van uw nieuwe beheersite in het dialoogvenster in en selecteer **Opslaan**.

Stap 6 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Volgende stappen

Werk uw sitecertificaat bij om veilige toegang te garanderen. Zie Certificaten beheren, op pagina 226 voor meer informatie.

Servers configureren

Gebruik deze functies om uw servers te configureren:

- SMTP-server: de SMTP-server verwerkt de verzending van e-mails van Cisco WebEx Meetings Server naar de bestemming.
- Opslagserver: de NFS-server is de opslagserver waar alle opnames van vergaderingen worden opgeslagen.

Een mailserver configureren

Configureer een e-mailserver om toe te staan dat uw systeem vergaderinguitnodigingen en andere communicatie aan gebruikers verzendt.

Opmerking Het is erg belangrijk dat uw e-mailserver altijd operationeel is. E-mail is de belangrijkste communicatiemethode met uw gebruikers, waaronder het registreren van meldingen, wijzigingen in vergaderingsinformatie, accountstatus en vele andere belangrijke meldingen.

Opmerking Het inschakelen van de onderhoudsmodus is niet vereist voor het wijzen van deze eigenschappen.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer **Meer weergeven** in het Servergedeelte.

Stap 3 Selecteer **Bewerken** in het Mailservergedeelte

Stap 4 Voer de hostnaam van uw mailserver in en selecteer optioneel het selectievakje **TLS ingeschakeld**.

Stap 5 Voer het poortnummer van uw mailserver in en selecteer optioneel het selectievakje **Verificatie server ingeschakeld**.

Stap 6 Selecteer **Doorgaan**.

Een SMTP-server configureren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem**.

Stap 3 Selecteer in het gedeelte Servers de optie **Meer weergeven**.

Stap 4 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 5 Selecteer bij SMTP Server de koppeling **Bewerken**.

Stap 6 Vul de SMTP-servervelden in:

- Hostnaam: De hostnaam van uw SMTP-server.
- Poort: Het poortnummer voor uw SMTP-server.
- Gebruikersnaam: Gebruikersnaam voor de e-mailclient.
- Wachtwoord: Wachtwoord voor de gebruiker.

Stap 7 Schakel optioneel de selectievakjes **TLS ingeschakeld** en **Verificatie server ingeschakeld** in.

Stap 8 Selecteer **Opslaan**.

Stap 9 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Een opslagserver configureren

Gebruik uw opslagserver om een back-up te maken van uw systeem en vergaderingsopnames op te slaan. Tijdens een noodherstel (zie De noodherstelfunctie gebruiken) kan het systeem met deze back-ups worden hersteld. (Momenteel wordt de opslagmethode Network File System (NFS) ondersteund.) Zorg ervoor dat uw opslagserver toegankelijk is vanaf alle interne virtuele machines. (Ook met VMware Data Recovery kunnen back-ups worden gemaakt van de virtuele machines. Zie http://www.vmware.com/pdf/vdr_11_admin.pdf voor meer informatie.)

Opmerking Het is niet nodig om uw opslagserver te verbinden met externe virtuele machines zoals externe Internet Reverse Proxy (IRP)-servers.

Uw opslagserver maakt dagelijks back-ups van de volgende gegevens:

- Bepaalde systeeminstellingen
- Gebruikersgegevens
- Vergaderinformatie
- SSL-certificaat dat naar het systeem is geüpload

- De site-URL

Back-ups worden dagelijks uitgevoerd en staan standaard ingesteld op 4:20 lokale tijd. Tijdens het back-upproces functioneert Cisco WebEx Meetings Server zonder onderbreking van vergaderingen, opnames, of andere functies. De vorige back-up wordt pas verwijderd nadat de back-up van de daaropvolgende dag is voltooid om aanwezigheid van een back-up te garanderen.

Uw systeem heeft ongeveer vijf minuten nodig om een back-up te maken van 500 MB. De benodigde tijd voor een back-up van uw systeem is afhankelijk van de opslagsnelheid, NFS-snelheid, en andere factoren. Het duurt ongeveer een uur om een back-up te maken van een database van 70 GB, en het verplaatsen ervan naar het NFS duurt 10 minuten. De overdrachtstijd is 12 MB/sec om netwerkcommunicatie mogelijk te maken en een niet-onderbroken werking van het product te garanderen.

Voordat u begint

Zorg dat u uw Unix-toegangsrechten configureert, zodat uw systeem door de gebruiker gegenereerde inhoud en systeemback-ups kan opslaan.

Op Linux-gebaseerde opslagsystemen is dit afhankelijk van de lees-/schrijfmachtigingen die u hebt geconfigureerd voor anonieme gebruikers van een specifieke directory die moet worden gebruikt voor uw NFS (Network File System).

Op Windows-gebaseerde opslagsystemen is dit afhankelijk van de instelling **Netwerktoegang: machtigingen voor Iedereen toepassen op anonieme gebruikers**. Daarnaast moet u iedereen in de gebruikersgroep lees- en schrijfmachtigingen geven voor de NFS.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem**.

Stap 4 Selecteer in het gedeelte Servers de optie **Meer weergeven**.
Als er een opslagserver aanwezig is op uw systeem, wordt het weergegeven op deze pagina. Als er geen opslagserver op uw systeem aanwezig is, krijgt u de optie om er een te configureren.

Stap 5 Selecteer nu in het gedeelte Opslagserver de optie **Voeg nu een opslagserver toe**

Stap 6 Geef het NFS-koppelingspunt op en selecteer **Opslaan**.
Het systeem bevestigt uw NFS-koppelpunt.

Stap 7 Selecteer **Doorgaan**.
U ziet een bevestigingsbericht dat de opslagserver is toegevoegd.

Stap 8 Selecteer **Klaar**.

Stap 9 Optioneel kunt u de standaardtijd voor de dagelijkse back-up wijzigen. In het gedeelte Opslagserver klikt u op Schema systeemback-up **tijd** en selecteert u een andere tijd in het vervolgkeuzemenu. Selecteer vervolgens **Opslaan**.
Er wordt dagelijks een back-up gemaakt op de tijd die u hebt geselecteerd in plaats van de standaard ingestelde tijd van 4:20 uur lokale tijd.

Stap 10 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Volgende stappen

Configureer uw systeem om de opslagserver voor het volgende te gebruiken:

- Vergaderingsopnamen.
- Noodherstel. Zie De noodherstelfunctie gebruiken, op pagina 166 voor meer informatie.

Voor een goede werking van uw opslagserver moet u zorgen voor het volgende:

- Uw opslagserver is toegankelijk van buiten Cisco WebEx Meetings Server.
- Uw opslagserver is ingeschakeld.
- Er is een netwerkverbinding met uw opslagserver.
- Koppelen/toegang is mogelijk vanaf een niet-Cisco WebEx Meetings Server-machine.
- Uw opslagserver is niet vol.

Opmerking Als een gebruiker per ongeluk een opname van de pagina **Cisco WebEx-vergaderingopnamen** verwijdert en de opname ook op de NFS-opslagserver (Network File System) is opgeslagen, neemt u contact op met het Cisco Technical Assistance Center (TAC) voor ondersteuning bij het herstellen van de opname.

De noodherstelfunctie gebruiken

Gebruik de noodherstelfuncties om uw implementatie te herstellen na een systeemfout of andere calamiteit. Een noodgeval is bijvoorbeeld een netwerkcrash, serverstoring, uitvallen van het gegevenscenter of een andere gebeurtenis waardoor u uw systeem niet langer kunt gebruiken. Er zijn twee typen noodherstel:

- Noodherstel voor een datacenter—Als u één datacenter hebt en uw systeem wegvalt, kunt u uw systeem opnieuw installeren in hetzelfde datacenter en het in dezelfde staat herstellen.
- Noodherstel met twee datacenters — Als u twee datacenters hebt en uw systeem op het eerste datacenter onbeschikbaar wordt, kunt u het systeem openen vanuit uw tweede datacenter en vervolgens het eerste datacenter herstellen naar de staat daarvan.

Nadat u een opslagserver hebt geconfigureerd, wordt er dagelijks een back-up van uw systeem gemaakt. Op uw dashboard wordt een melding weergegeven met informatie over de laatste back-up van het systeem. Er wordt slechts één back-upsysteem tegelijkertijd bewaard in de opslag. Nadat u een upgrade of update hebt uitgevoerd, wordt er een back-up bewaard van uw vorige versie van Cisco WebEx Meetings Server. We raden u aan om niet dezelfde opslaglocatie te gebruiken voor verschillende installaties van Cisco WebEx Meetings Server.

Denk eraan dat noodherstel:

- Meer dan 30 minuten duurt.
- Uw instellingen overschrijft met de instellingen op de laatste back-up.
- Vereist dat u aanvullende stappen uitvoert om de service aan uw gebruikers te herstellen (uitgelegd in *Wat u nog meer moet doen* in dit hoofdstuk).

Deze procedure maakt back-ups van bepaalde systeeminstellingen, gebruikersinformatie, vergaderingsinformatie, SSL-certificaten die naar het systeem zijn geüpload en de site-URL. Het back-upproces slaat geen VMware-gegevens of IP-adresinformatie voor individuele virtual machines op. (Ook met VMware Data Recovery kunnen back-ups worden gemaakt van de virtuele machines. Zie http://www.vmware.com/pdf/vdr_11_admin.pdf voor meer informatie.) Wanneer u een noodherstel uitvoert, moet u handmatig bepaalde instellingen opnieuw toepassen, waaronder:

- Verbindingen met bepaalde externe componenten, bijvoorbeeld Cisco Unified Communications Manager (CUCM)
- SSL-certificaten (in het geval dat de hostnamen van het noodherstelsysteem anders zijn dan de namen in het originele systeem)
- Bij implementaties met één datacenter kunt u eventueel hetzelfde IP-adres of dezelfde hostnaam gebruiken. Bij implementaties met twee datacenters kunt u eventueel hetzelfde IP-adres of dezelfde hostnaam voor uw primaire systeem gebruiken.

Voer deze procedure uit nadat er een calamiteit is opgetreden en u uw systeem niet meer kunt gebruiken.

Voordat u begint

Voor het uitvoeren van noodherstelprocedures is het volgende van belang:

- Er moet een opslagserver zijn geconfigureerd. Als u geen opslagserver geconfigureerd hebt, is de optie **Noodherstel** niet beschikbaar en worden er geen back-ups gemaakt. Zie Een opslagserver configureren voor meer informatie.
- U moet toegang hebben tot een systeem waarin u uw implementatie kunt herstellen. Zie de informatie over noodherstel op een datacenter en twee datacenters hieronder.
- Uw herstelsysteem moet dezelfde implementatiegrootte en softwareversie hebben als uw oorspronkelijke systeem.

  Op een systeem met hoge beschikbaarheid moet u eerst noodherstel configureren. Vervolgens configureert u hoge beschikbaarheid op dat systeem. Indien u een systeem met hoge beschikbaarheid hebt waarvoor noodherstel is vereist na een calamiteit, moet u eerst uw systeem terugzetten en vervolgens hoge beschikbaarheid configureren op uw herstelde systeem. Zie Een systeem met hoge beschikbaarheid toevoegen voor meer informatie over hoge beschikbaarheid.

Procedure

Stap 1 Meld u aan bij de beheersite op een systeem waarin u uw implementatie kunt herstellen.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** > **Servers** > **Opslagserver toevoegen**.

Stap 4 Voer de naam in van uw opslagserver in het veld **NFS-koppelpunt** en selecteer **Opslaan**.

Voorbeeld:
192.168.10.10:/CWMS/backup.

Stap 5 Selecteer **Doorgaan** om het noodherstel verder te zetten.
Als de implementatiegrootte en de softwareversie van het herstelsysteem overeenkomen met uw oorspronkelijke systeem, kunt u verdergaan met het noodherstel. Als het systeem een andere implementatiegrootte of softwareversie heeft, kunt u pas verdergaan nadat u de toepassing opnieuw hebt geïmplementeerd op uw

herstelsysteem, zodat de implementatiegrootte en de softwareversie overeenkomen met de oorspronkelijke implementatie. Het IP-adres of de hostnaam hoeft niet overeen te komen met de oorspronkelijke implementatie.

Stap 6 Selecteer een van de volgende handelingen om door te gaan:

- **Annuleren**—een back-up maken van uw vooraf bestaand systeem alvorens een opslagserver toe te voegen. Nadat u een back-up hebt gemaakt van uw systeem, keert u terug naar deze pagina en selecteert u **Doorgaan** om verder te gaan.
- **Doorgaan**-uw vooraf bestaand systeem overschrijven en verdergaan met noodherstel.

Het noodherstelproces begint. Als u uw browser sluit, kunt u zich niet opnieuw aanmelden in het systeem totdat het proces voltooid is.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Volgende stappen

U moet de volgende procedures uitvoeren om de service voor uw gebruikers te herstellen:

- Configureer uw teleconferentie-instellingen opnieuw. Raadpleeg CUCM configureren in de Planningshandleiding voor meer informatie.
- Configureer uw SSO-instellingen opnieuw. Zie Gefedereerd eenmalig aanmelden (SSO) configureren voor meer informatie.
- Configureer uw SNMP-instellingen opnieuw. Zie Uw SNMP-instellingen configureren voor meer informatie.
- Configureer uw certificaten opnieuw. Het kan gebeuren dat u uw SSL-certificaten opnieuw moet laden als ze niet overeenkomen met de SSL-certificaten die geconfigureerd zijn op het herstelsysteem. Zie Een SSL-certificaat herstellen voor meer informatie.
- Het herstelde systeem wordt in eerste instantie geconfigureerd voor een licentievrije modus die na 180 dagen vervalt. Configureer de licenties van uw vorige systeem opnieuw op het herstelde systeem. Zie Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding en Over licenties voor meer informatie.
- Configureer uw DNS-instellingen zodat uw website-URL naar de huidige VIP verwijst. Uw VIP op het herstelde systeem kan verschillen van wat u op uw oorspronkelijk systeem had. U moet uw DNS-configuratie voor eindgebruikers voltooien om hun oorspronkelijke koppelingen te gebruiken en aan te melden bij vergaderingen op het herstelde systeem. Zie Uw virtuele IP-adres wijzigen voor meer informatie.
- Als u uw systeem hebt geconfigureerd voor directory-integratie en LDAP-verificatie hebt ingeschakeld, controleert u of uw CUCM-referenties werken. Nadat u uw systeem uit de onderhoudsmodus hebt gehaald en het systeem helemaal opnieuw is opgestart, meldt u zich aan bij de beheersite en selecteert u achtereenvolgens **Gebruikers** > **Directory-integratie** en **Opslaan**. Als uw CUCM-gebruikersgegevens niet kloppen, wordt het foutbericht **Ongeldige gebruikersgegevens** weergegeven. Als dit foutbericht wordt weergegeven, voert u de juiste referenties in en selecteert opnieuw **Opslaan**. Zie Directory-integratie configureren voor meer informatie.

Uw SNMP-instellingen configureren

U kunt de volgende SNMP-instellingen configureren:

- Communityreeksen: SNMP communityreeksen verifiëren toegang tot MIB-objecten en werken als een geïntegreerd wachtwoord.
- USM-gebruikers—Configureer gebruikersgebaseerde beveiliging (USM) om aanvullende beveiliging op berichtniveau te bieden. Selecteer een bestaande USM-configuratie om deze te bewerken of aanvullende USM-configuraties toe te voegen. Anders dan de standaard USM-gebruiker, serveradmin, die lees- en schrijfrechten voor MIB-gegevens heeft, hebben alle nieuwe USM-gebruikers die u configureert alleen-lezenrechten voor MIB-gegevens.
- Meldingsdoelen—Gebruik deze functie om de trap/inform-ontvanger te configureren.

Communityreeksen configureren

U kunt communityreeksen en toegangsrechten voor communityreeksen toevoegen en bewerken.

Communityreeksen toevoegen

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de SNMP-sectie.

Stap 4 Selecteer **Toevoegen** in het gedeelte communityreeksen.

Stap 5 Vul de gewenste velden in op de pagina **Communityreeks toevoegen**.

Optie	Beschrijving
Naam communityreeks	Voer de naam in van uw communityreeks. Maximumlengte: 256 tekens.
Rechten bekijken	Toegangsrechten voor de communityreeks instellen. Opties omvatten: • Alleen lezen • Lezen, schrijven • Lezen, schrijven, melden • Alleen melden • Geen **Standaard:** Alleen lezen

Optie	Beschrijving
Informatie IP-adres host	Selecteer uw informatietype voor IP-adres host. (Standaard: **SNMP-pakketten van elke host accepteren**) Als u **SNMP-pakketten van deze hosts accepteren** selecteert, wordt een dialoogvenster onder de selectie weergegeven. Voer namen of IP-adressen in, gescheiden door komma 's.

Selecteer **Toevoegen**.

De communityreeks is aan uw systeem toegevoegd.

Stap 6 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Communityreeksen bewerken

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de SNMP-sectie.

Stap 4 Selecteer een link voor de naam van de communityreeks in de sectie Communityreeksen.

Stap 5 Wijzig de gewenste velden op de pagina **Communityreeks bewerken**.

Optie	Beschrijving
Naam communityreeks	Wijzig uw naam van de communityreeks. Maximumlengte: 256 tekens.
Rechten bekijken	Toegangsrechten voor de communityreeks instellen. Opties omvatten: • Alleen lezen • Lezen, schrijven • Lezen, schrijven, melden • Alleen melden • Geen **Standaard:** Alleen lezen

Optie	Beschrijving
Informatie IP-adres host	Selecteer uw informatietype voor IP-adres host. **Standaard:** SNMP-pakketten accepteren van elke host Als u **SNMP-pakketten van deze hosts accepteren** selecteert, wordt een dialoogvenster onder de selectie weergegeven. Voer namen of IP-adressen in, gescheiden door komma 's.

Selecteer **Bewerken**.

Uw communityreeksinformatie is gewijzigd.

Stap 6 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

USM-gebruikers configureren

U kunt uw USM-gebruikers toevoegen en bewerken.

USM-gebruikers toevoegen

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer **Meer weergeven** in het SNMP-gedeelte.

Stap 3 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 4 Selecteer **toevoegen** in het gedeelte USM-gebruikers.

Stap 5 Vul de velden in op de pagina **USM-gebruiker toevoegen**.

Optie	Beschrijving
USM-gebruikersnaam	Voer de naam in van de USM-gebruiker die u wilt configureren. Maximaal 256 tekens.

Optie	Beschrijving
Beveiligingsniveau	Selecteer het beveiligingsniveau. Het beveiligingsniveau dat u selecteert, bepaalt welke algoritmen en wachtwoorden u kunt instellen voor de gebruiker. Opties omvatten: • noAuthNoPriv?Geen verificatiealgoritme en wachtwoord en geen privacyalgoritme en wachtwoord voor de gebruiker. • authPriv?Hiermee kunt u een verificatiealgoritme en wachtwoord en een privacyalgoritme en wachtwoord voor de gebruiker configureren. • authNoPriv: Hiermee kunt u een verificatiealgoritme en wachtwoord configureren voor de gebruiker. **Standaard:** noAuthNoPriv
Verificatiealgoritme	Selecteer het verificatiealgoritme voor de gebruiker. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv** of **authNoPriv**. **Standaard:** SHA
Verificatiewachtwoord	Het verificatiewachtwoord voor de gebruiker invoeren. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv** of **authNoPriv**.
Privacyalgoritme	Selecteer het privacyalgoritme voor de gebruiker. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv**. **Standaard:** AES128
Privacywachtwoord	Het privacywachtwoord voor de gebruiker invoeren. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv**.

Stap 6 Selecteer **Toevoegen**.
De USM-gebruiker is aan uw systeem toegevoegd.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

USM-gebruiker bewerken

Opmerking De standaard USM-gebruiker, serveradmin, wordt intern gebruikt en de gebruiker kan enkel het wachtwoord wijzigen, maar niet het beveiligingsniveau, de authenticatie en het privacyalgoritme.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer **Meer weergeven** in het SNMP-gedeelte.

Stap 3 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 4 Selecteer een USM-gebruiker in het gedeelte USM-gebruikers.

Stap 5 Wijzig de gewenste velden op de pagina **USM-gebruiker bewerken**.

Optie	Beschrijving
USM-gebruikersnaam	Wijzig de naam van de USM-gebruiker. Maximaal 256 tekens.
Beveiligingsniveau	Selecteer het beveiligingsniveau. Het beveiligingsniveau dat u selecteert, bepaalt welke algoritmen en wachtwoorden u kunt instellen voor de gebruiker. Opties omvatten: • noAuthNoPriv?Geen verificatiealgoritme en wachtwoord en geen privacyalgoritme en wachtwoord voor de gebruiker. • authPriv?Hiermee kunt u een verificatiealgoritme en wachtwoord en een privacyalgoritme en wachtwoord voor de gebruiker configureren. • authNoPriv: Hiermee kunt u een verificatiealgoritme en wachtwoord configureren voor de gebruiker. **Standaard:** noAuthNoPriv
Verificatiealgoritme	Selecteer het verificatiealgoritme voor de gebruiker. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv** of **authNoPriv**. **Standaard:** SHA
Verificatiewachtwoord	Het verificatiewachtwoord voor de gebruiker wijzigen. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv** of **authNoPriv**.
Privacyalgoritme	Selecteer het privacyalgoritme voor de gebruiker. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv**. **Standaard:** AES128

Optie	Beschrijving
Privacywachtwoord	Het privacywachtwoord voor de gebruiker wijzigen. **Opmerking** Deze optie wordt alleen weergegeven als het beveiligingsniveau is ingesteld op **authPriv**.

Stap 6 Selecteer **Bewerken**.
De USM-gebruikersinformatie is gewijzigd.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Meldingsdoelen configureren

U kunt virtuele machines op uw systeem configureren om SNMP-meldingen of traps voor het volgende te genereren:

- Virtuele machine opstarten (trap koude start)
- Alle alarmvoorwaarden

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de SNMP-sectie.

Stap 3 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 4 Selecteer **Nieuw doel voor meldingen toevoegen** bij **Meldingsdoelen**.

Stap 5 Configureer de volgende velden voor uw meldingsdoel:

Optie	Beschrijving
Hostnaam/IP-adres doel	De hostnaam of IP-adres van de virtuele machine die u wilt instellen als een meldingsdoel.
Poortnummer	Het poortnummer van uw virtuele machine. **Standaard:** 162
SNMP-versie	Uw SNMP-versie. **Standaard:** V3
Type melding	Selecteer **Informeren** of **Traps**. **Standaard:** Traps

Optie	Beschrijving
USM-gebruikers **Opmerking** Deze optie verschijnt enkel wanneer SNMP-versie is ingesteld op V3.	Selecteer USM-gebruikers. Zie USM-gebruikers configureren, op pagina 171 voor meer informatie.
communityreeks **Opmerking** Deze optie verschijnt enkel wanneer SNMP-versie niet is ingesteld op V3.	Selecteer communityreeksen. Zie Communityreeksen configureren, op pagina 169 voor meer informatie.

Stap 6 Selecteer **Toevoegen**.
Uw meldingsdoel is toegevoegd.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Doel voor meldingen bewerken

Meldingsdoelen configureren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de SNMP-sectie.

Stap 3 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 4 Selecteer een koppeling meldingsdoel uit de lijst **Meldingdoelen**.

Stap 5 U kunt de volgende velden configureren voor uw meldingsdoel:

Optie	Beschrijving
Hostnaam/IP-adres doel	De hostnaam of IP-adres van de virtuele machine die u wilt instellen als een meldingsdoel.
Poortnummer	Het poortnummer van uw virtuele machine. **Standaard:** 162
SNMP-versie	Uw SNMP-versie. **Standaard:** V3
Type melding	Selecteer **Informeren** of **Traps**. **Standaard:** Informeren

Optie	Beschrijving
USM-gebruikers **Opmerking** Deze optie verschijnt enkel wanneer SNMP-versie is ingesteld op V3.	Selecteer USM-gebruikers. Zie USM-gebruikers configureren, op pagina 171 voor meer informatie.
communityreeks **Opmerking** Deze optie verschijnt enkel wanneer SNMP-versie niet is ingesteld op V3.	Selecteer communityreeksen. Zie Communityreeksen configureren, op pagina 169 voor meer informatie.

Stap 6 Selecteer **Opslaan**.
De wijzigingen aan uw meldingsdoel zijn opgeslagen.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Licenties beheren

Als u dit product aanschaft, krijgt u een gratis proefperiode van zes maanden. Nadat uw gratis proefperiode is verlopen, moet u licenties voor uw gebruikers aanschaffen.

Licenties kunnen worden verkregen via de geïntegreerde Cisco Enterprise License Manager (zie Licenties uitvoeren met License Manager), eFulfilment (zie Licenties bestellen met eFulfilment) of de technische ondersteuning (zie Licenties uitvoeren door contact op te nemen met de technische ondersteuning).

Over licenties

Informatie over gebruikergebaseerde licenties

Dit product gebruikt hostgebaseerde licenties. U moet een licentie kopen voor iedere gebruiker die vergaderingen wil hosten. Zorg ervoor dat u weet wat de volgende belangrijke begrippen inhouden:

- Deelnemer: iemand die aan vergaderingen deelneemt, maar die geen vergaderingen plant of host en die geen hostfuncties kan instellen. Een deelnemer kan bijvoorbeeld geen inhoud presenteren, tenzij hij of zij door een host is aangewezen als presentator.
- Host van een vergadering: iemand die vergaderingen plant, die als host aan vergaderingen deelneemt en die bepaalde functies kan instellen, zoals het aanwijzen van een presentator of het dempen van het geluid van een andere deelnemer.
- Alternatieve host: iemand die tijdens het plannen van de vergadering is aangewezen als persoon die de rol van host op zich kan nemen als de host van de vergadering niet aanwezig is. Als de host die de vergadering heeft gepland niet aan de vergadering deelneemt, kan de alternatieve host vrijwel dezelfde functies instellen als de host van de vergadering. Als de host en de persoon die als alternatieve host is aangewezen allebei aan de vergadering deelnemen, verandert wat betreft het licentiegebruik de status van de alternatieve host in de status *deelnemer*.

- Deelnemen vóór host (Join Before Host, JBH): een functie waardoor deelnemers zich bij een vergadering kunnen aanmelden voordat de host of een alternatieve host zich heeft aangemeld.
- Overlappende vergaderingen: twee of meer vergaderingen die door dezelfde host voor hetzelfde tijdstip zijn gepland. Wanneer een host van een vergadering of een alternatieve host overlappende vergaderingen start, worden mogelijk extra licenties gebruikt. Iemand kan overlappende vergaderingen plannen, maar die persoon kan maximaal één vergadering tegelijkertijd hosten. Er is sprake van een overlappende vergadering wanneer de host van één vergadering die vergadering verlaat om een andere te starten en de eerste vergadering wordt voortgezet onder leiding van een andere persoon, die als host optreedt.
- Proefperiode: een overlappingsperiode van een kwartier. De proefperiode is alleen van toepassing wanneer JBH is ingeschakeld en er een vergadering wordt gestart door een andere deelnemer dan de host.

Het licentiegebruik wordt één keer per maand berekend, bijvoorbeeld één keer van 1 tot en met 31 januari, één keer van 1 tot en met 28 februari enzovoort. Licenties worden als volgt geteld:

- Voor het *plannen* van vergaderingen worden nooit licenties gebruikt. Tijdens het plannen van een vergadering kan de host alternatieve hosts aanwijzen. Voor het aanwijzen van alternatieve hosts of het plannen van vergaderingen namens anderen worden geen licenties gebruikt. Standaard wordt bij het deelnemen aan een vergadering de persoon die de vergadering heeft gepland automatisch als host aangewezen.
- Deelnemers gebruiken nooit licenties. Als iemand in een maand alleen als deelnemer (en niet als host) aan vergaderingen heeft deelgenomen, heeft die persoon geen licenties gebruikt.
- Er wordt één licentie gebruikt en aan een persoon gekoppeld wanneer diegene in een maand voor het eerst een vergadering start en als host van die vergadering wordt aangewezen. Als iemand in een maand meerdere niet-overlappende vergaderingen plant, worden geen extra licenties gebruikt. Als dezelfde persoon gedurende de maand daarna niet als host aan vergaderingen deelneemt, gebruikt die persoon tijdens die maand geen licenties. De persoon kan als deelnemer aan vergaderingen deelnemen zonder licenties te gebruiken.
- Er wordt een extra licentie gebruikt en aan een persoon gekoppeld voor elke overlappende vergadering waaraan die persoon als host deelneemt. Het totale aantal licenties dat door één persoon wordt gebruikt, wordt bepaald aan de hand van het hoogste aantal overlappende vergaderingen dat door die persoon wordt gehost. Als een persoon in één maand als host aan twee vergaderingen deelneemt, worden er voor die maand twee licenties gebruikt en aan die persoon gekoppeld. Als die persoon in diezelfde periode drie overlappende vergaderingen start, gebruikt hij of zij drie licenties enzovoort. Als een persoon als host aan een vergadering deelneemt, de vergadering verlaat voordat deze is afgelopen en als host aan een andere vergadering deelneemt, heeft deze persoon twee licenties nodig.
- Er worden geen extra licenties gebruikt wanneer iemand die als alternatieve host is aangewezen en die in die maand nog geen licentie heeft gebruikt, een vergadering start en de host van de vergadering aan die vergadering deelneemt.
- Er wordt één licentie gebruikt en aan een alternatieve host gekoppeld wanneer een alternatieve host die in die maand nog geen licentie heeft gebruikt, als host aan een vergadering deelneemt en de host die de vergadering heeft gepland, niet aan de vergadering deelneemt.

Als u op uw systeem een belangrijke upgrade of een noodherstelprocedure uitvoert, moet u nieuwe virtuele machines configureren en de licenties opnieuw configureren. (Zie Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding.)

Het systeem telt het licentiegebruik voor elke gebruiker per maand, zoals in de voorbeeldscenario's in de tabel. In de scenario's in de tabel is aangenomen dat het in elk voorbeeld de eerste keer in die maand is dat een gebruiker een vergadering host.

Scenario	Vergaderdatum	Tijdstip vergadering	Gebruikte licenties
Gebruiker A plant een vergadering, maar die wordt niet gestart.	1 januari	9:00 tot 10:00 uur	0
Gebruiker B start een vergadering.	2 januari	9:00 tot 10:00 uur	1
Gebruiker C host twee of meer niet-overlappende vergaderingen.	3 januari 3 januari 4 januari	9:00 tot 10:00 uur 14:00 tot 14:30 uur 10:00 tot 11:00 uur	1
Gebruiker D neemt aan twee vergaderingen deel die op dezelfde dag en tijd plaatsvinden.	6 januari 6 januari	9:00 tot 10:00 uur 9:30 tot 10:00 uur	2
Gebruiker E neemt aan twee vergaderingen deel die op dezelfde dag en tijd plaatsvinden. De tweede vergadering wordt gehost door de host die beide vergaderingen heeft gestart en een alternatieve host.	6 januari 6 januari	9:00 tot 10:00 uur 9:30 tot 10:00 uur	3 Er wordt één licentie gebruikt door de host die de vergaderingen heeft gestart en één door de alternatieve host.
Gebruiker F start twee vergaderingen op dezelfde dag en verlaat beide vergaderingen. Beide vergaderingen worden door een alternatieve host gehost.	7 januari 7 januari	9:00 tot 10:00 uur 9:00 tot 10:00 uur	2 Eén voor elke oorspronkelijke host en één voor de alternatieve hosts die een vergadering hebben voortgezet.
Gebruiker G start een vergadering en geeft de hostrechten tijdens de vergadering door aan een andere deelnemer. Vervolgens start de host een tweede vergadering die tegelijk met de eerste plaatsvindt.	8 januari 8 januari	9:00 tot 10:00 uur 9:30 tot 10:00 uur	2 Eén voor elke oorspronkelijke host en één voor de alternatieve hosts die een vergadering hebben voortgezet.

Scenario	Vergaderdatum	Tijdstip vergadering	Gebruikte licenties
Gebruiker H start een vergadering waarvoor **JBH** is ingeschakeld. Een host neemt deel aan de vergadering. Vervolgens plant de eerste gebruiker een tweede vergadering die gelijktijdig met de eerste vergadering plaatsvindt, maar alle deelnemers van de tweede vergadering nemen alleen deel aan de teleconferentie (en niet aan het webgedeelte).	11 januari 11 januari	9:00 tot 10:00 uur 9:00 tot 10:00 uur	2
Gebruiker J plant een vergadering. **JBH** is ingeschakeld. Deelnemers melden zich aan, maar de vergadering wordt niet bijgewoond door de host van de vergadering of een alternatieve host, en alle deelnemers verlaten de vergadering.	11 januari	9:00 tot 10:00 uur	1
Gebruiker K start een vergadering waarvoor **JBH** is ingeschakeld. De JBH-deelnemer start namens de host een tweede vergadering. De host verlaat en beëindigt de eerste vergadering voordat de proefperiode is afgelopen.	12 januari 12 januari	9:00 tot 10:00 uur 9:10 tot 10:00 uur	1
Gebruiker L start drie persoonlijke conferenties (niet het webgedeelte) met account 1, account 2 en account 3 op dezelfde datum maar op verschillende tijden.	12 januari 12 januari 12 januari	9:00 tot 10:00 uur 10:00 tot 11:00 uur 11:00 tot 12:00 uur	1
Gebruiker M start drie persoonlijke conferenties (niet het webgedeelte) met account 1, account 2 en account 3 op dezelfde datum en tijd.	14 januari	9:00 tot 10:00 uur	3

Scenario	Vergaderdatum	Tijdstip vergadering	Gebruikte licenties
Gebruiker N start op dezelfde dag, maar op verschillende tijden, een vergadering waarvoor **JBH** is ingeschakeld en een persoonlijke conferentie (niet het webgedeelte).	14 januari 14 januari	9:00 tot 10:00 uur 11:00 tot 12:00 uur	1
Gebruiker P start op dezelfde dag en tijd een vergadering waarvoor **JBH** is ingeschakeld en een persoonlijke conferentie (niet het webgedeelte).	15 januari 15 januari	9:00 tot 10:00 uur 9:00 tot 10:00 uur	2
Gebruiker Q start een persoonlijke conferentie (niet het webgedeelte) en kort daarna het overlappende webgedeelte.	16 januari 16 januari	9:00 tot 10:00 uur (persoonlijke conferentie) 9:15 tot 10:00 uur (WebEx-vergadering gestart in combinatie met een persoonlijke conferentie)	1

Op de pagina **Rapporten** kunt u een rapport aanvragen dat het totaal aantal gebruikte licenties gedurende de maand weergeeft. Bovendien raden wij u aan het samenvattende PDF-rapport te bekijken dat de maandelijkse trends van het licentiegebruik weergeeft. Door de algemene licentietrend te bekijken, kunt u toekomstige aankopen van licenties efficiënter plannen om te voldoen aan het groeiend gebruik van dit systeem in uw bedrijf.

Voorzichtig In uw systeem kan het licentiegebruik het aantal op uw systeem geïnstalleerde licenties overschrijden. Systeembeheerders ontvangen e-mails met het bericht **Aantal licenties overschreden** en dashboardmeldingen die aangeven dat zij het licentiegebruik moeten verminderen of binnen zes maanden meer licenties moeten aanschaffen. Tijdens deze zesmaandelijkse periode zal het systeem normaal blijven werken voor eindgebruikers. Als u het licentiegebruik niet hebt verminderd of niet binnen zes maanden meer licenties hebt aangeschaft, wordt het systeem afgesloten voor alle gebruikers zolang een beheerder niet meer licenties installeert.

Zolang het systeem is afgesloten, kunnen gebruikers geen vergaderingen plannen, hosten of bijwonen, of toegang krijgen tot opnamen van de vergadering. Op de WebEx-site wordt voor gebruikers het bericht **Website niet bereikbaar in verband met onderhoud** weergegeven. De beheerwebsite blijft normaal functioneren, zodat de beheerder zich kan aanmelden en genoeg licenties kan toevoegen om het probleem ten aanzien van het overschreden aantal licenties aan te pakken. Nadat de extra licenties zijn geïnstalleerd, hebben gebruikers weer toegang tot de WebEx-site, kunnen ze weer vergaderingen hosten en beëindigen en hebben ze weer toegang tot opnamen.

Gratis proefperiode van zes maanden

Nadat u zich voor het eerst bij dit product hebt aangemeld en de introductiewizard hebt doorlopen, gaat uw gratis proefperiode van zes maanden van start. Gedurende de gratis proefperiode kunnen beheerders het systeem configureren en kunnen uw gebruikers vergaderingen plannen, hosten en bijwonen. Boven aan de Beheerwebsite verschijnt een banner die aangeeft hoeveel maanden er nog van uw gratis proefperiode over zijn. Een maand vóór afloop van uw gratis proefperiode ontvangt u een e-mail met de mededeling dat u licenties moet aanschaffen en op uw systeem moet installeren omdat het systeem anders wordt gedeactiveerd.

Aan het einde van de gratis proefperiode wordt uw systeem gedeactiveerd. U kunt zich nog wel aanmelden bij uw systeem, maar u kunt de overige functies pas weer gebruiken nadat u licenties hebt toegevoegd. Raadpleeg het gedeelte Licenties beheren van de *Beheerhandleiding voor Cisco WebEx Meetings Server* voor meer informatie over het beheren van uw licenties.

Licenties opnieuw configureren

Nadat CWMS-software is geüpgraded of nadat een bestaand systeem is uitgebreid, kan er door de licenties opnieuw te configureren voor worden gezorgd dat oudere, geldige licenties op het geüpgradede of uitgebreide systeem kunnen worden gebruikt. Zie Licenties opnieuw configureren na een software-upgrade of systeemuitbreiding in de *Beheerhandleiding voor Cisco WebEx Meetings Server*.

Het verkrijgen van licenties

Neem contact op met uw verkoopvertegenwoordiger van Cisco om licenties voor uw systeem te bestellen. Wanneer u contact opneemt met uw verkoopvertegenwoordiger, moet u aangeven hoeveel licenties u wilt. U hebt een licentie nodig voor elke werknemer in uw organisatie die vergaderingen zal hosten.

Er zijn verschillende manieren om te bepalen hoeveel licenties u nodig hebt. U kunt uw dashboard gebruiken om het gebruik, de geschiedenis van de gebruikte bronnen en uw vergadertrends in te zien en te bepalen hoeveel gebruikers vergaderingen op uw systeem hosten en bijwonen. Nadat u het product een aantal maanden hebt gebruikt, kunt u uw maandelijkse overzichtsrapporten en aangepaste gegevensrapporten gebruiken om u te helpen bepalen hoeveel licenties u nodig hebt. Uw maandelijkse overzichtsrapporten bieden statistieken over de serviceacceptatie en het gebruik van gebruikerslicenties. De statistieken over de serviceacceptatie tonen de snelheid waarmee nieuwe gebruikers uw systeem in gebruik nemen. U ziet de acceptatiesnelheid de vorige drie maanden en een voorspelling van de groei voor de komende drie maanden. De statistieken met betrekking tot de gebruikerslicenties tonen het licentiegebruik over de afgelopen drie maanden en de verwachte groei voor de komende drie maanden.

U kunt licenties verkrijgen via de geïntegreerde Cisco Enterprise License Manager, eFulfilment of door contact op te nemen met de technische ondersteuning. Raadpleeg het gedeelte Licenties beheren in de *Beheerhandleiding voor Cisco WebEx Meetings Server* voor meer informatie over het beheren van uw licenties.

Overschrijding van het aantal licenties

Nadat u de licenties voor uw systeem hebt aangeschaft en geconfigureerd, moet u nagaan of u over voldoende licenties beschikt voor alle actieve hosts op uw systeem. Uw systeem controleert elke maand om vast te stellen of er voldoende licenties voor elke actieve host beschikbaar zijn. De licentietelling wordt elke kalendermaand op nul gezet. Als het aantal actieve hosts in uw systeem het aantal licenties overschrijdt, wordt er een e-mail naar de beheerder verzonden met de melding dat het aantal licenties is overschreden. U hebt zes maanden de tijd om uw licentiegebruik te verminderen of om het aantal licenties op uw systeem te vergroten zodat deze overeenkomt met het aantal actieve hosts of dit aantal overschrijdt. Als u vóór afloop van deze periode van zes maanden niet uw licentiegebruik vermindert of voldoende licenties aanschaft om aan het gebruik te voldoen, wordt uw systeem gedeactiveerd. Het e-mailbericht informeert de beheerder over de datum waarop dit zal gebeuren.

Het systeem controleert en past de licentie-aantallen aan die op de Beheerwebsite worden vermeld. De controle wordt eens per dag uitgevoerd (om 02.00 uur) om het overschot aan licenties zo nodig aan te passen. Aan het einde van elke maand controleert het systeem het licentiegebruik. Als het aantal hosts tot beneden het aantal licenties is gedaald, eindigt de overschotsituatie. Als het aantal actieve hosts nog steeds het aantal licenties overschrijdt, wordt er elke maand een nieuwe e-mail naar de beheerder verzonden met de mededeling dat de overschotsituatie nog steeds aanhoudt, met de datum waarop het systeem wordt gedeactiveerd.

Als de overschotsituatie na zes opeenvolgende maanden nog steeds aanwezig is, wordt uw systeem gedeactiveerd en ontvangt de beheerder een e-mail met informatie over wat er is gebeurd. Nadat uw systeem is gedeactiveerd, kunnen uw gebruikers geen vergaderingen plannen, hosten en bijwonen of opnames raadplegen binnen uw systeem. De Beheerwebsite blijft normaal functioneren, zodat de beheerder zich kan aanmelden en licenties kan toevoegen. Gebruikers kunnen weer vergaderingen plannen, hosten en bijwonen en opnames raadplegen zodra de beheerder licenties aan het systeem heeft toegevoegd.

Tijdelijke licenties

Als u tijdelijke licenties op uw systeem hebt geconfigureerd, wordt uw tijdelijke licentiestatus weergegeven op een banner op elke pagina van de Beheerwebsite. De banner informeert u over hoeveel tijdelijke licenties u hebt geconfigureerd en wanneer de tijdelijke licenties komen te vervallen. Wanneer de tijdelijke licenties vervallen, keert uw systeem terug naar de vorige licentiestatus.

Verlopen licenties

Als u een upgrade van uw systeem uitvoert, moet u ook uw licenties bijwerken. Nadat u een upgrade van uw systeem hebt uitgevoerd, wordt er een e-mail naar de beheerder verzonden met de mededeling dat u zes maanden de tijd krijgt om de licenties bij te werken. Als u uw licenties niet bijwerkt vóór afloop van deze periode van zes maanden, wordt uw systeem gedeactiveerd. Het e-mailbericht informeert de beheerder over de datum waarop dit zal gebeuren.

Het systeem controleert en past de licentie-aantallen aan die op de Beheerwebsite worden vermeld. De controle wordt eens per dag uitgevoerd (om 02.00 uur) om zo nodig de verlopen licenties aan te passen. Aan het einde van elke maand controleert het systeem of de licenties van de vorige periode zijn bijgewerkt. Als de licenties zijn bijgewerkt, eindigt de situatie van vervallen licenties. Als de licenties nog niet zijn bijgewerkt, wordt er elke maand een nieuwe e-mail naar de beheerder verzonden met de mededeling dat de situatie met vervallen licenties nog steeds aanhoudt, met de datum waarop het systeem wordt gedeactiveerd.

Als de situatie met vervallen licenties na zes maanden nog steeds aanwezig is, wordt uw systeem gedeactiveerd en ontvangt de beheerder een e-mail met informatie over wat er is gebeurd. Nadat uw systeem is gedeactiveerd, kunnen uw gebruikers geen vergaderingen plannen, hosten en bijwonen of opnames raadplegen binnen uw systeem. De Beheerwebsite blijft normaal functioneren, zodat de beheerder zich kan aanmelden en licenties kan bijwerken. Gebruikers kunnen weer vergaderingen plannen, hosten en bijwonen en opnames raadplegen zodra de beheerder de licenties heeft bijgewerkt.

Verbinding met Prime License Manager (PLM) verbroken

Wanneer u licenties aanschaft, gebruikt u een geïntegreerde PLM-tool om uw PAK in te voeren en uw licenties te registreren. PLM voert elke 12 uur een synchronisatie uit om de licentiestatus en het tijdstip waarop voor het laatst aan de voorwaarden werd voldaan, bij te werken. Als er twee dagen verstrijken zonder verbinding met PLM, wordt er een e-mail naar uw beheerder verzonden om hem of haar te laten weten dat PLM niet kan synchroniseren met uw systeem. U hebt zes maanden de tijd om opnieuw verbinding met PLM te maken. Als uw systeem niet opnieuw verbinding maakt met PLM voordat deze periode van zes maanden is afgelopen, wordt het systeem uitgeschakeld. Het e-mailbericht informeert de beheerder over de datum waarop dit zal gebeuren.

Aan het eind van elke maand waarin het systeem geen verbinding met PLM kan maken, wordt er een nieuwe e-mail naar uw beheerder verzonden om hem of haar te laten weten op welke datum het systeem zal worden uitgeschakeld. Deze situatie eindigt als uw systeem opnieuw verbinding met PLM maakt voordat de periode van zes maanden is afgelopen.

Als uw systeem na zes maanden nog steeds geen verbinding met PLM kan maken, wordt uw systeem uitgeschakeld en ontvangt de beheerder een e-mail over wat er is gebeurd. Wanneer uw systeem is uitgeschakeld, kunnen gebruikers geen vergaderingen plannen of hosten, niet aan vergaderingen deelnemen en geen opnames openen op het systeem. De beheerwebsite blijft normaal werken. Beheerders kunnen zich dus bij het systeem aanmelden, maar pas als het systeem weer verbinding heeft gemaakt met PLM komt er een einde aan deze situatie en kunnen gebruikers weer vergaderingen plannen of hosten, aan vergaderingen deelnemen en opnames openen.

Handelingen waarvoor nieuwe licenties noodzakelijk zijn

Bij de volgende handelingen die het systeem wijzigen is het noodzakelijk om nieuwe licenties te installeren:

- Uitbreiden: zie Uw systeem uitbreiden naar een groter systeemformaat voor meer informatie.
- Upgraden: zie Het systeem bijwerken voor meer informatie.
- Noodherstel: zie De noodherstelfunctie gebruiken voor meer informatie.

Licenties uitvoeren met License Manager

Ga als volgt te werk om licenties te verkrijgen via de geïntegreerde Cisco Enterprise License Manager:

Voordat u begint

Neem contact op met uw verkoopvertegenwoordiger van Cisco om licenties voor uw systeem te bestellen. Uw verkoopvertegenwoordiger zal u een e-mailbericht sturen dat uw productautorisatiesleutel (PAK) bevat.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de Licentiesectie.

Stap 3 Selecteer **Licenties beheren**
In uw browser wordt een nieuw tabblad of venster geopend met Cisco Prime License Manager (PLM).

Opmerking Deze versie van PLM is geïntegreerd in Cisco WebEx Meetings Server. De PLM-site is geen externe website.

Stap 4 Selecteer **Licentiebeheer** > **Licenties**.

Stap 5 Selecteer **Een licentieaanvraag maken**.
Het dialoogvenster **Licentieaanvraag en vervolgstappen** wordt weergegeven.

Stap 6 Kopieer de geselecteerde tekst in het veld en selecteer **Registratie van Cisco-licentie**.

Stap 7 Meld u aan bij uw Cisco-account.

Stap 8 Voer de PAK in die u van uw verkoopvertegenwoordiger van Cisco hebt gekregen in het veld **Productautorisatiesleutel** en selecteer **Volgende**.

De pagina **PAK invullen** verschijnt.

Stap 9 Plak de inhoud van het licentieverzoek dat u hierboven kopieerde in het veld, voer het aantal licenties in dat u aankoopt en selecteer **Volgende**.

Stap 10 Bekijk de pagina en selecteer **Ik ga akkoord met de voorwaarden van de licentie**.

Stap 11 Zorg ervoor dat het contacte-mailadres juist is. Wijzig het contacte-mailadres eventueel in het veld **Verzenden aan**.

Stap 12 Selecteer **Licentie verkrijgen**
Het dialoogvenster **Status licentieaanvraag** wordt weergegeven.

Stap 13 Verkrijg uw licentiebestand op één van de volgende manieren:

- Selecteer **Downloaden** om uw licentiebestand (.bin) te downloaden.
- Pak uw licentiebestand (.bin) uit van het ZIP-bestand dat u wordt toegestuurd via e-mail.

Stap 14 Keer terug naar de Beheersite en selecteer **Systeem** en vervolgens de koppeling **Meer weergeven** in de rubriek Licenties.

Stap 15 Selecteer **Licenties beheren**.
In uw browser wordt een nieuw tabblad of venster geopend met Cisco Prime License Manager (PLM).

Stap 16 Selecteer **Licentiebestand installeren**.

Stap 17 Selecteer **Bladeren** en selecteer het licentiebestand (.bin) dat u hebt gedownload of uitgepakt uit het ZIP-bestand in uw e-mail.

Stap 18 Selecteer **Installeren**.
Uw licentiebestand is geïnstalleerd. Controleer de licentie-informatie die wordt weergegeven om ervoor te zorgen dat deze correct is.

Stap 19 Selecteer in de kolom Uitvoerdatum de optie **Vandaag**.
De pagina **Licentie uitvoeren** wordt weergegeven. Verifieer of de informatie in het gedeelte **Uitgevoerde licenties** klopt.

Licenties uitvoeren met eFulfilment

Voltooi de licentiebestelling door, zonder de website te gebruiken, de PAK (Product Authorization Key) in te voeren in License Manager.

Voordat u begint

Neem contact op met uw verkoopvertegenwoordiger van Cisco om licenties voor uw systeem te bestellen. Uw verkoopvertegenwoordiger zal u een e-mailbericht sturen dat uw productautorisatiesleutel (PAK) bevat.

Voor eFulfilment is een netwerkverbinding tussen het systeem en Cisco Systems, Inc. nodig. Verifieer of uw systeem zich niet achter een firewall bevindt die de toegang blokkeert. Als de toegang wordt geblokkeerd, gebruik dan op bestanden gebaseerde uitvoering (zie Licenties uitvoeren met License Manager) of neem contact op met de technische ondersteuning om licenties te bestellen (zie Licenties uitvoeren door contact op te nemen met de technische ondersteuning).

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Systeem** en selecteer de koppeling **Meer weergeven** in de Licentiesectie.

Stap 3 Selecteer **Licenties beheren**
In uw browser wordt een nieuw tabblad of venster geopend met Cisco Prime License Manager (PLM), die in Cisco WebEx Meetings Server is geïntegreerd. (De PLM-site is geen externe website.)

Stap 4 Selecteer **Licenties uitvoeren vanuit PAK**.
De wizard **Licenties uitvoeren vanuit PAK** wordt weergegeven.

Stap 5 Voer de PAK in die u van uw verkoopvertegenwoordiger van Cisco hebt gekregen in het veld **Productautorisatiesleutel** en selecteer **Volgende**.
De pagina **PAK invullen** verschijnt.

Stap 6 Selecteer **Licenties toevoegen vanuit een nieuwe PAK**.

Stap 7 Voer in het vak *** PAK-code** de PAK-code in en selecteer **Volgende**.

Stap 8 Meld u aan met uw gebruikers-id en wachtwoord van Cisco.com.
Het venster **Licenties uitvoeren** wordt weergegeven, met daarin het aantal beschikbare licenties.

Stap 9 Selecteer in de kolom **Acties** de optie **Uitvoeren**.

Stap 10 Klik op de kolom **Installeren** om de waarden te bewerken.

Stap 11 Voer het aantal licenties in dat u voor dit systeem wilt uitvoeren. Als de PAK gedeeltelijke uitvoering ondersteunt, loopt het bereik van 1 tot het aantal resterende licenties in de PAK.

Stap 12 Selecteer **Opslaan**.

Stap 13 Selecteer **OK**.
Het venster **Licenties uitvoeren** wordt weergegeven. De waarde in de kolom **Installeren** geeft aan hoeveel licenties u hebt geselecteerd om uit te voeren.

Stap 14 Selecteer **Volgende**.
Het venster **Inhoud bekijken** wordt weergegeven. In de kolom **Huidige waarden** wordt het aantal actieve licenties weergegeven. In de kolom **Na uitvoering** wordt weergegeven hoeveel licenties u hebt wanneer eFulfilment is voltooid.

Stap 15 Selecteer **Volgende**.

Stap 16 Selecteer **Door dit selectievakje in te schakelen, bevestig ik dat ik de voorwaarden van de licentieovereenkomst voor eindgebruikers heb gelezen en begrepen en dat ik ermee akkoord ga gebonden te zijn aan deze voorwaarden**.

Stap 17 Selecteer **Voltooien**.
De voortgangsbalk **Verbinden met licentieserver** wordt weergegeven terwijl de licentiemanager verbinding met Cisco maakt om uw licenties uit te voeren. Wanneer eFulfilment is voltooid, wordt er een nieuwe regel toegevoegd in het venster **Licenties**. In de kolom **Uitvoerdatum** wordt de huidige datum weergegeven, gevolgd door **- vandaag**. U kunt deze koppeling selecteren om meer informatie over uw licenties weer te geven, zoals het type en het aantal licenties dat op dit systeem is geïnstalleerd.

Licenties uitvoeren door contact op te nemen met de technische ondersteuning

Voordat u begint

Haal uw registratie-id-nummer op. U vindt uw registratie-id-nummer door uw Enterprise License Management tool te openen en **Over** te selecteren.

Procedure

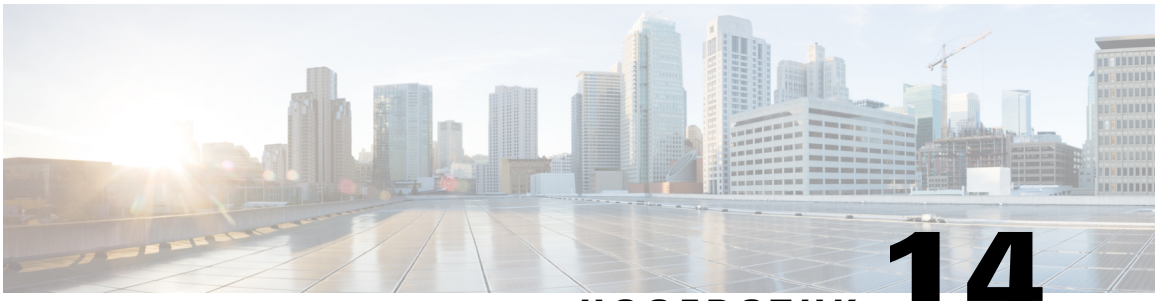
Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Ondersteuning** en bel de TAC op het vermelde nummer.

Stap 3 Open een dossier en vraag hierbij het aantal aanvullende licenties aan dat u nodig hebt.
Cisco verwerkt uw aanvraag en activeert de aanvullende licenties op uw systeem.

Stap 4 Selecteer **Systeem**.

Stap 5 Controleer het gedeelte Licenties om te bevestigen dat de licenties zijn toegevoegd.



HOOFDSTUK 14

Instellingen configureren

Deze module beschrijft hoe u uw instellingen moet configureren.

- Uw bedrijfsgegevens configureren, pagina 188
- Uw brandinginstellingen configureren, pagina 189
- Uw vergaderinstellingen configureren, pagina 190
- Over het configureren van uw audio-instellingen, pagina 192
- Uw video-instellingen configureren, pagina 197
- Uw mobiele instellingen configureren, pagina 197
- Servicekwaliteit (Quality of Service – QoS) configureren, pagina 198
- Wachtwoorden configureren, pagina 200
- Uw e-mailinstellingen configureren, pagina 204
- Uw downloadinstellingen configureren, pagina 224
- Certificaten beheren, pagina 226
- SSL-certificaten genereren, pagina 227
- SSO IdP-certificaten importeren, pagina 234
- Certificaten voor beveiligde teleconferenties importeren, pagina 234
- Veiligheid gebruikerssessie configureren, pagina 235
- Gefedereerd eenmalig aanmelden (SSO) configureren, pagina 236
- Uw Cloud-functies configureren, pagina 240
- Beveiliging van de virtuele machine configureren, pagina 240

Uw bedrijfsgegevens configureren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Als u de instelling Taal wilt wijzigen, selecteert u **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Opmerking U hoeft de onderhoudsmodus niet in te schakelen wanneer u de andere instellingen op de pagina **Bedrijfsinfo** wijzigt.

Stap 3 Selecteer **Instellingen**. Indien u een van de andere instellingenpagina's bekijkt, kunt u ook **Bedrijfsinformatie** selecteren in het gedeelte Instellingen.

Stap 4 Vul de velden in op de pagina en selecteer **Opslaan**.

Optie	Beschrijving
Bedrijfsnaam	De naam van uw bedrijf of organisatie.
Adres 1	Adresregel 1.
Adres 2	Adresregel 2.
Plaats	Uw stad.
Staat/provincie	De naam van uw staat of provincie.
ZIP-/postcode	ZIP- of postcode.
Land/regio	De naam van uw land of regio.
Telefoonnr werk	Vervolgkeuzemenu met landcode en veld voor bedrijfstelefoon met netnummer.
Tijdzone	Uw tijdzone.
Taal	Uw taal. Taalinstelling beïnvloedt het volgende: • De aanmeldingspagina die gezien wordt door beheerders wanneer ze hun beheerdersaccount voor de eerste keer activeren. • De standaard audiomeldingen die afgespeeld worden voor gebruikers van een inbelteleconferentie.
Landinstelling	Uw landinstelling. De landinstelling is van invloed op de weergave van de tijd, datums, valuta en getallen.

Stap 5 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Uw brandinginstellingen configureren

Voordat u begint

Bereid het volgende voor voordat u uw brandinginstellingen configureert:

- Een PNG-, GIF- of JPEG-afbeelding van 120x32 van uw bedrijfslogo
- De URL van de privacyverklaring van uw bedrijf
- De URL van de servicevoorwaarden van uw bedrijf
- De URL voor ondersteuning van uw bedrijf

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Branding**.

Stap 3 Vul de velden in op de pagina en selecteer **Opslaan**.

Optie	Beschrijving
Bedrijfslogo	Ga naar uw logobestand. Uw logo moet in PNG-, JPEG- of GIF-indeling zijn. De maximale afmetingen zijn 120x32 pixels en de maximale bestandsgrootte is 5MB.
Privacymelding	Voer een URL in voor de privacyverklaring van uw bedrijf.
Servicevoorwaarden	Voer een URL in voor de servicevoorwaarden van uw bedrijf.
Aangepaste voettekst	De tekst die u invoert, staat in de voettekst van alle e-mails van eindgebruikers en beheerders die via uw systeem worden verzonden.
Achtergrondkleur koptekst	Selecteer deze optie om de standaard achtergrondkleur uit te schakelen. Dit heeft invloed op alle browserwerkbalken en e-mails.
Contact-URL voor ondersteuning	Voer een URL in voor de ondersteuningspagina van uw bedrijf.

Een bedrijfslogo verwijderen

Voordat u begint

Een transparant 120x32 PNG- of GIF-bestand maken.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Branding**.

Stap 3 Selecteer **Bladeren** en kies uw transparante 120x32 PNG- of GIF-bestand voor het veld Bedrijfslogo.

Stap 4 Selecteer **Opslaan**.
Uw vorige bedrijfslogo is vervangen door uw lege PNG- of GIF-bestand. Bevestig dat het originele logo is verwijderd.

Uw vergaderinstellingen configureren

Configureer uw vergaderinstellingen om te beheren welke functies deelnemers kunnen gebruiken. Configureer de volgende functies:

- Instellingen voor deelnemen aan vergadering
- Max. aantal deeln. per vergadering (vergaderingsgrootte)

Opmerking Deze instellingen is beperkt door de systeemgrootte die tijdens de implementatie is ingesteld. Zie De grootte van uw systeem bevestigen, op pagina 29 voor meer informatie.

- Deelnemersrechten

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Vergaderingen**.

Stap 3 Selecteer uw opties in het gedeelte Vergadering bijwonen.
Standaardinstellingen zijn **Aanmelden van deelnemers bij vergaderingen vóór host toestaan**, **Aanmelden van deelnemers bij teleconferentie vóór host toestaan** en **Eerste deelnemer die deelneemt, zal de presentator zijn**. Als de selectievakjes **Aanmelden van deelnemers bij vergaderingen vóór host toestaan** en **Aanmelden van deelnemers bij teleconferentie vóór host toestaan** zijn ingeschakeld, kunnen deelnemers zich maximaal 15 minuten voor de aanvangstijd aanmelden bij een vergadering. Optioneel kunt u **Iedereen kan de vergadering presenteren** selecteren.

Opmerking Als u de selectie van **Aanmelden van deelnemers bij vergaderingen vóór host toestaan** ongedaan maakt, wordt de functie **Eerste deelnemer die deelneemt, zal de presentator zijn** automatisch gedeselecteerd.

Stap 4 Selecteer het maximum aantal deelnemers per vergadering met behulp van de schuifknop. Het maximum aantal deelnemers voor uw systeem is geconfigureerd tijdens implementatie. Hierna volgen de instellingen met de systeemgrootte en overeenkomstige maximale vergaderingsgrootte.

Systeemgrootte	Maximale vergaderingsgrootte
50	50
250	100 (geen HA), 250 (met HA)
800	100 (geen HA), 250 (met HA)
2,000	100 (geen HA), 250 (met HA)

Stap 5 Selecteer uw opties in het gedeelte deelnemersrechten. **Chatten**, **Polling**, **Documentrevisie en presentatie** en **Delen en extern beheer** zijn standaard geselecteerd. De geselecteerde deelnemersrechten verschijnen in de besturingselementen van gebruikers.
Opname is standaard uitgeschakeld. Selecteer **Opnemen** om vergaderingen op te nemen en op te slaan op uw opslagserver.

Opmerking U kunt een opslagserver configureren om opnemen in te schakelen. Zie Een opslagserver configureren, op pagina 164 voor meer informatie.

Stap 6 Selecteer **Opslaan**.

Over vergaderingsbeveiliging

Cisco WebEx Meetings Server biedt verschillende beveiligingsfuncties voor vergaderingen afhankelijk van de volgende factoren:

- Gebruikerstype: host, alternatieve host, gebruiker (aangemeld) en gast.
- Vergadering heeft een wachtwoord of geen wachtwoord.
- Wachtwoord is verborgen of zichtbaar in de vergaderingsuitnodiging.
- Wachtwoord is verborgen of zichtbaar in de vergaderingsuitnodigingse-mail.
- Gedrag weergegeven op de pagina voor het deelnemen aan vergaderingen (zie de volgende tabellen).

Tabel 1: Wachtwoord wordt uitgesloten tijdens het plannen van uw vergadering

Gebruikerstype	Wachtwoord dat wordt weergegeven in uitnodigingse-mail en herinnering	Pagina met vergaderingsgegevens
Host	Ja	Ja
Alternatieve host	Ja	Ja

Gebruikerstype	Wachtwoord dat wordt weergegeven in uitnodigingse-mail en herinnering	Pagina met vergaderingsgegevens
Uitgenodigde deelnemer	Nee	Nee
Doorgestuurde deelnemer	Nee	Nee

Tabel 2: Wachtwoord is inbegrepen tijdens het plannen van uw vergadering

Gebruikerstype	Wachtwoord dat wordt weergegeven in uitnodigingse-mail en herinnering	Pagina met vergaderingsgegevens
Host	Ja	Ja
Alternatieve host	Ja	Ja
Uitgenodigde deelnemer	Ja	Ja
Doorgestuurde deelnemer	Ja	Ja

- Deelnemen vóór host is ingeschakeld/uitgeschakeld.
  - Ingeschakeld: Deelnemer/gast/uitgenodigde deelnemer kan deelnemen aan een vergadering vóór de host, 15 minuten voor de geplande starttijd.
  - Uitgeschakeld: Deelnemer/gast/uitgenodigde deelnemer kan niet deelnemen aan een vergadering vóór de host. De host of alternatieve host kan de vergadering starten, en vervolgens kunnen de deelnemers deelnemen.
- Deelnemen teleconferentie vóór host is ingeschakeld/uitgeschakeld.
  - Ingeschakeld: Als de host de teleconferentie niet in de vergaderingsclient start, kunnen deelnemers deelnemen aan de teleconferentie vóór de host.
  - Uitgeschakeld: Als de host de teleconferentie niet in de vergaderingsclient start, kunnen deelnemers niet deelnemen aan de teleconferentie vóór de host.
- Eerste deelnemer kan presenteren is ingeschakeld/uitgeschakeld.
  - Ingeschakeld: Wanneer deelnemen vóór host is ingesteld, is de eerste deelnemer de presentator.
  - Uitgeschakeld: De host heeft altijd de bal.

Over het configureren van uw audio-instellingen

De eerste keer dat u uw audio-instellingen configureert, wordt u door het proces geleid door een wizard die u helpt bij het instellen van uw CUCM SIP-configuratie en inbeltoegangsnummers. Nadat u de wizard hebt

voltooid en u uw audio-instellingen voor de eerste keer hebt geconfigureerd, kunt u alle andere audio-instellingen configureren.

Uw audio-instellingen voor de eerste keer configureren

Wanneer u de audio-instellingen voor het eerst configureert, moet u opgeven welke functies u wilt en moet u uw CUCM-instellingen configureren. Een wizard leidt u doorheen het eerste installatieproces.

Voordat u begint

U moet teleconferenties inschakelen en CUCM configureren voordat u verdergaat met uw audioconfiguratie. U moet CUCM op twee systemen configureren indien u teleconferentie voor hoge beschikbaarheid wilt aanbieden. Raadpleeg de Planningshandleiding voor meer informatie. Om verder te gaan, moet u over de volgende informatie beschikken:

- Maak een lijst van toegangsnummers voor inbellen waarmee uw gebruikers kunnen inbellen in vergaderingen.
- Het IP-adres van uw CUCM.
- (Optioneel) Verkrijg een geldig veilig conferentiecertificaat als u van plan bent de TLS/SRTP-teleconferentie-encryptie te gebruiken. Zie Certificaten voor beveiligde teleconferenties importeren voor meer informatie.

Opmerking Deze functie is niet beschikbaar in Rusland of Turkije.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Audio**.
De pagina **Audio** verschijnt en uw Huidige audio-instellingen worden weergegeven.

Stap 4 Selecteer **Volgende**.
De pagina **SIP-configuratie** wordt weergegeven. Deze pagina geeft de informatie over de SIP-configuratie weer die u nodig hebt om CUCM te configureren, zoals het IP-adres en het poortnummer voor elk servertype.

Stap 5 Selecteer **Volgende**.
De pagina **Teleconferentie inschakelen: De pagina CUCM-instelling** verschijnt met uw huidige instellingen.

Stap 6 Selecteer **Bewerken** om uw instellingen te wijzigen.
Het dialoogvenster **CUCM (Cisco Unified Communications Manager)** verschijnt.

Stap 7 Vul de velden in het dialoogvenster **CUCM (Cisco Unified Communications Manager)** als volgt in:

a) Vul de IP-adressen voor CUCM 1-IP-adres en optioneel CUCM 2-IP-adres in.
Deze IP-adressen moeten overeenkomen met het primaire en het optionele secundaire CUCM-knooppunt die deel uitmaken van de Cisco Unified Communications Manager Group, zoals ingesteld in de apparaatpool die in CUCM in de SIP-trunks voor het toegangspunt is geconfigureerd. Zie 'Een SIP-trunk configureren voor een toepassingspunt' in de *Planningshandleiding* voor meer informatie.

Opmerking CUCM 2 is niet vereist, maar is aanbevolen voor teleconferenties met hoge beschikbaarheid.

b) Voer het poortnummer voor uw systeem in. Het poortnummer moet overeenkomen met het poortnummer toegewezen in CUCM. (**Standaard:** 5062)

c) Gebruik het vervolgkeuzemenu **Transport** om het transporttype voor uw systeem te selecteren. (**Standaard:** TCP)

Opmerking Indien u TLS selecteert als uw transporttype, moet u een geldig certificaat voor beveiligde conferentie importeren voor elke CUCM-server, het SSL-certificaat exporteren en uploaden naar CUCM en de volledige domeinnaam (FQDN) van uw systeem configureren als de SIP-domeinnaam op elke CUCM-server. Zie Certificaten voor beveiligde teleconferenties importeren voor meer informatie over het importeren van uw certificaten. Zie 'CUCM configureren' in de Planningshandleiding voor meer informatie over CUCM.

d) Selecteer **Doorgaan**.

Uw nieuwe of bijgewerkte CUCM-instellingen verschijnen op de pagina **Teleconferentie inschakelen: CUCM-instelling**.

Stap 8 Selecteer **Volgende**.
De pagina **Teleconferentie inschakelen: Instelling toegangsnummer** verschijnt.

Stap 9 Selecteer **Bewerken**.
Het dialoogvenster **Inbelfunctie voor toegangsnummers** verschijnt.

Stap 10 Selecteer **Toevoegen** om een toegangsnummer voor inbellen toe te voegen.
Er wordt een lijn toegevoegd in het dialoogvenster voor het telefoonlabel en -nummer. Telkens u **Toevoegen** selecteert, verschijnt een bijkomende regel in het dialoogvenster.

Stap 11 Voer het **Telefoonlabel** en **Telefoonnummer** in voor elk toegangsnummer dat u toevoegt en selecteer **Doorgaan** nadat u klaar bent met het toevoegen van nummers.

Opmerking Zorg dat u enkel nummers toevoegt die u hebt geconfigureerd in CUCM. De cijfers die u toevoegt, verschijnen in e-mailuitnodigingen en in uw Cisco WebEx-vergaderclient.

Voorbeeld:
Voer "Hoofdkantoor" in als **Telefoonlabel** en "888-555-1212" als **Telefoonnummer**.
De toegangsnummers die u invoerde, worden aan uw systeem toegevoegd en u wordt teruggebracht naar de pagina **Teleconferentie inschakelen: Instelling toegangsnummer.** De pagina geeft nu aan hoeveel toegangsnummers zijn geconfigureerd.

Stap 12 Selecteer **Opslaan**.
De wizard geeft aan dat u uw teleconferentiefuncties met succes hebt ingesteld.

Stap 13 (Optioneel) Voer een weergavenaam in het dialoogvenster **Weergavenaam** in.

Stap 14 (Optioneel) Voer een geldig beller-id in het dialoogvenster **Nummerweergave** in.

Opmerking Het beller-id is beperkt tot numerieke tekens en een streep (-) en heeft een maximale lengte van 32 tekens.

Stap 15 (Optioneel) Configureer uw instelling voor WebEx Bel me op (**Standaard**: Druk op 1 om verbinding te maken met de vergadering). U kunt deze optie inschakelen om niet te vragen om op **1** te drukken om verbinding te maken met een vergadering.

Opmerking Wij raden u niet aan om deze optie in te schakelen, tenzij uw telefoonsysteem het cijfer **1** niet kan verzenden.

Stap 16 (Optioneel) Selecteer uw **Ingangs- en uitgangstoon van de telefoon**.

- Piep (standaard)

- Geen signaal
- Naam aankondigen

Stap 17 (Optioneel) Als IPv6 geconfigureerd is op uw systeem, dient u uw **IPv6-teleconferentie** in te stellen op **Aan** of **Uit**. (**Standaard:** Uit. De instelling **Uit** geeft aan dat IPv4 de instelling is.)

Opmerking De optie **IPv6 Teleconferentie** is niet beschikbaar op systemen die niet zijn geconfigureerd voor IPv6.

Stap 18 Selecteer bij **Audiotaal systeem** welke taal gebruikers horen wanneer ze inbellen op het audiogedeelte van een Cisco WebEx-vergadering of wanneer ze de service Bel me gebruiken.

Stap 19 Selecteer **Opslaan**.

Stap 20 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Uw audio-instellingen configureren

Voordat u begint

Zie het gedeelte Uw audio-instellingen voor de eerste keer configureren, op pagina 193 indien u uw audio-instellingen nog niet hebt geconfigureerd.

Opmerking Het inschakelen van de onderhoudsmodus is niet vereist voor het configureren of wijzigen van de inbelnummers, de weergavenaam of de audio-instellingen voor beller-id.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Audio**.

Stap 4 Configureer uw instellingen voor **Audiofuncties bewerken**.

Optie	Beschrijving
WebEx Audio	• Service Inbellen voor gebruikers en Bel me op: Hiermee kunnen gebruikers deelnemen aan een teleconferentie door bepaalde telefoonnummers te bellen of door een Bel me-oproep te krijgen van het systeem. • Inbellen: Hiermee kunnen gebruikers een teleconferentie bijwonen door bepaalde telefoonnummers te bellen. • UIT: Schakelt alle belfuncties uit.

Optie	Beschrijving
Spraakverbinding via computer	• AAN • UIT

Stap 5 Selecteer in het gedeelte Instellingen teleconferentie bewerken, de koppeling **Bewerken** bij CUCM (Cisco Unified Communication Manager) om uw instellingen te wijzigen.

Optie	Beschrijving
CUCM 1 IP-adres	Voer de hostnaam of een IP-adres in voor uw CUCM 1-systeem.
CUCM 2 IP-adres	(Optioneel) Voer de hostnaam of een IP-adres in voor uw CUCM 2-systeem (load balancing service). **Opmerking** CUCM 2 is niet vereist, maar is aanbevolen voor teleconferenties met hoge beschikbaarheid.
Poortnummer	Voer een geldig poortnummer in. Zorg ervoor dat het poortnummer overeenkomt met de instelling in CUCM. **Standaard:** 5062
Transport	Selecteer het transporttype. **Opmerking** Indien u TLS selecteert als uw transporttype, moet u een geldig certificaat voor beveiligde conferentie importeren voor elke CUCM-server, het SSL-certificaat exporteren en uploaden naar CUCM en de volledige domeinnaam (FQDN) van uw systeem configureren als de SIP-domeinnaam op elke CUCM-server. Zie Certificaten voor beveiligde teleconferenties importeren, op pagina 234 voor meer informatie over het importeren van uw certificaten. Zie 'CUCM configureren' in de *Planningshandleiding van Cisco WebEx Meetings Server* voor meer informatie over CUCM. **Standaard:** TCP

Het dialoogvenster **CUCM (Cisco Unified Communications Manager)** verschijnt. Vul de velden in en selecteer **Doorgaan**.

Stap 6 Selecteer in het gedeelte Instellingen teleconferentie bewerken de koppeling **Bewerken** bij Toegangsnummers voor inbellen om uw toegangsnummers toe te voegen, te wijzigen of te verwijderen.

a) Selecteer **Toevoegen** en voer een telefoonlabel en telefoonnummer in voor elk nieuw toegangsnummer dat u wilt toevoegen.
b) Om een nummer te verwijderen, selecteert u de koppeling **Verwijderen** achter de lijn.
c) Voer bijgewerkte informatie in de velden telefoonlabel en telefoonnummer in voor elk toegangsnummer dat u wilt wijzigen.
d) Selecteer **Doorgaan** als u klaar bent.

Opmerking Zorg dat u enkel nummers toevoegt die u hebt geconfigureerd in CUCM. De cijfers die u toevoegt, verschijnen in e-mailuitnodigingen en in uw Cisco WebEx-vergaderclient.

Stap 7 Voer een weergavenaam in het dialoogvenster **Weergavenaam** in.

Stap 8 Voer een geldige beller-id in het dialoogvenster **Nummerweergave** in.

Opmerking Het beller-id is beperkt tot numerieke tekens en een streep (-) en heeft een maximale lengte van 32 tekens.

Stap 9 Configureer uw instelling voor WebEx Bel me op (**Standaard**: Druk op 1 om verbinding te maken met de vergadering). U kunt deze optie inschakelen om niet te vragen om op **1** te drukken om verbinding te maken met een vergadering.

Opmerking Cisco raadt u niet aan om deze optie in te schakelen, tenzij uw telefoonsysteem het cijfer **1** niet kan verzenden.

Stap 10 Selecteer uw **Ingangs- en uitgangstoon van de telefoon**.

- Piep (standaard)
- Geen signaal
- Naam aankondigen

Stap 11 Als IPv6 geconfigureerd is op uw systeem, dient u uw **IPv6-teleconferentie** in te stellen op **Aan** of **Uit**. (**Standaard:** Uit. De instelling **Uit** geeft aan dat IPv4 de instelling is.)

Opmerking De optie **IPv6 Teleconferentie** is niet beschikbaar op systemen die niet zijn geconfigureerd voor IPv6.

Stap 12 Selecteer **Opslaan**.

Stap 13 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Uw video-instellingen configureren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Video**.

Stap 3 Selecteer **Aan** of **Uit** en selecteer **Opslaan**. (**Standaard:** Aan).

Uw mobiele instellingen configureren

Opmerking Android wordt ondersteund in Cisco WebEx Meetings Server 2.0 en hoger. De WebEx-toepassingen voor iOS en Android zijn beide standaard ingeschakeld.

Voordat u begint

Om mobiele instellingen te configureren, moet u openbare toegang toevoegen aan uw systeem tijdens implementatie. Zie Openbare toegang aan uw systeem toevoegen voor meer informatie.

Houd er rekening mee dat als uw systeem is ingesteld op het toestaan van meer dan één inbelnummer, automatisch wordt aangenomen dat het eerste nummer een gratis inbelnummer is en dat dit nummer in de mobiele app standaard als eerste wordt geprobeerd. Er kan geen verbinding worden gemaakt vanuit de app als dit nummer niet bereikbaar is vanuit het mobiele netwerk. Zorg ervoor dat dit nummer toegankelijk is vanuit het mobiele netwerk.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Mobiel**.

Stap 3 Configureer uw mobiele instellingen door te selecteren welke mobiele platforms uw systeem ondersteunt, en selecteer **Opslaan**. (**Standaard:**WebEx voor iOS en WebEx voor Android zijn geselecteerd)

Opmerking
- Mobiele apparaten met iOS of Android hebben alleen toegang tot vergaderingen als u over een DMZ-netwerk beschikt. Als u niet over een DMZ-netwerk beschikt, zijn de opties voor de WebEx-toepassingen voor iOS en Android niet beschikbaar.
- De WebEx-toepassingen voor iOS en Android werken, net als de Cisco WebEx-toepassing voor desktops, via een intern intranet of extern internet.

Servicekwaliteit (Quality of Service – QoS) configureren

De DSCP-instellingen (Differentiated Services (DiffServ) code point) bepalen de QoS voor de audio- en videosignalen, zoals gedefinieerd in RFC 2475. Cisco raadt aan de standaardwaarde te behouden. De andere waarden zijn beschikbaar voor de uitzonderlijke gevallen waarbij een andere DSCP-instelling is vereist voor het netwerk. Raadpleeg voor meer informatie het hoofdstuk "Netwerkinfrastructuur" van het Cisco Unified Communications Solution Reference Network Design (SRND) dat van toepassing is op uw Cisco Unified Communications Manager op http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.

Dit zijn de standaardwaarden:

- WebEx-audio (Media)
  - IPv4 QoS-markering: **EF DSCP 101110**
  - IPv6 QoS-markering: **EF DSCP 101110**
- WebEx-audio (Signalering)
  - IPv4 QoS-markering: **CS3 (prioriteit 3) DSCP 011000**

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Servicekwaliteit**.

Stap 3 Selecteer QoS-markeerinstellingen vanuit de geschikte vervolgkeuzemenu's en selecteer **Opslaan**.

Over QoS-markering

In de onderstaande tabellen vindt u informatie over QoS-markeringen voor implementaties met verkeer dat via een Internet Reverse Proxy-server plaatsvindt, versus een implementatie zonder verkeer dat via een Internet Reverse Proxy-server plaatsvindt.

QoS-markering op Cisco WebEx Meetings Server-systemen met verkeer dat via een Internet Reverse Proxy-server plaatsvindt

Verkeer	QoS-markering
SIP Audio—media—CWMS naar endpoint	Ja
SIP Audio—signalering—CWMS naar endpoint	Ja
PC Audio—media—CWMS naar Client	Nee
PC Audio—signalering—CWMS naar client	Nee
PC Audio—media—Client naar CWMS	Nee
PC Audio—signalering—Client naar CWMS	Nee
PC Video—media—CWMS naar client	Nee
PC Video—signalering—CWMS naar client	Nee
PC Video—media—Client naar CWMS	Nee
PC Video—signalering—Client naar CWMS	Nee

QoS-markering op Cisco WebEx Meetings Server-systemen zonder verkeer dat via een Internet Reverse Proxy-server plaatsvindt

Verkeer	QoS-markering
SIP Audio—media—CWMS naar endpoint	Ja
SIP Audio—signalering—CWMS naar endpoint	Ja
PC Audio—media—CWMS naar Client	Ja
PC Audio—signalering—CWMS naar client	Ja
PC Audio—media—Client naar CWMS	Nee

Verkeer	QoS-markering
PC Audio—signalering—Client naar CWMS	Nee
PC Video—media—CWMS naar client	Ja
PC Video—signalering—CWMS naar client	Ja
PC Video—media—Client naar CWMS	Nee
PC Video—signalering—Client naar CWMS	Nee

Wachtwoorden configureren

U kunt wachtwoordinstellingen configureren voor het volgende:

- Algemene wachtwoorden—Beheert de verloopperioden van wachtwoorden en u kunt ervoor zorgen dat gebruikers direct of na een bepaald interval hun wachtwoord moeten wijzigen.
- Gebruikerswachtwoorden—Hiermee kunt u wachtwoordsterkte voor gebruikersaccounts configureren, inclusief een combinatie van hoofdletters en kleine letters, lengte, tekensoorten en -gebruik, beheer van dynamische webpaginatekst en het opstellen van een lijst met onacceptabele wachtwoorden.
- Vergaderingswachtwoorden—Hiermee kunt u wachtwoordgebruik voor vergaderingen invoeren en wachtwoordsterkte voor vergaderingen configureren, inclusief een combinatie van hoofdletters en kleine letters, lengte, tekensoorten en -gebruik, beheer van dynamische webpaginatekst en het opstellen van een lijst met onacceptabele wachtwoorden.

Opmerking Als SSO is ingeschakeld op uw systeem, zijn de instellingen op de pagina's **Algemeen wachtwoord** en **Gebruikerswachtwoord** en de besturingselementen voor het wijzigen van een wachtwoord op de pagina **Gebruiker bewerken** niet langer van toepassing op hostaccounts.

Uw algemene wachtwoordinstellingen configureren

Met uw algemene wachtwoordinstellingen kunt u beperkingen opleggen betreffende het deactiveren van accounts en de geldigheidsduur van een wachtwoord. Alle wachtwoordinstellingen op deze pagina zijn optioneel en kunnen aangezet (geselecteerd) of uitgezet (niet geselecteerd) worden.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Wachtwoordbeheer** > **Algemeen wachtwoord**.

Stap 3 (Optioneel) Schakel het selectievakje **Hostaccount deactiveren na aantal dag(en) inactiviteit** in en voer het aantal dagen in het tekstveld in. (**Standaard:** Aangevinkt en ingesteld op 90 dagen)
Als u de standaardinstelling gebruikt, wordt een gebruiker gedeactiveerd als hij of zij gedurende negentig opeenvolgende dagen geen vergadering heeft gehost of gepland.

Opmerking Deze functie geldt enkel voor hostaccounts. U kunt met deze functie geen beheerderaccount deactiveren. Raadpleeg Gebruikers deactiveren, op pagina 139 om een beheerderaccount te deactiveren.

Stap 4 (Optioneel) Schakel het selectievakje **Alle gebruikers verplichten hun wachtwoord te wijzigen om de aantal dag(en)** in en voer het aantal dagen in het tekstveld in. (**Standaard:** Niet aangevinkt)

Stap 5 (Optioneel) Selecteer **Alle gebruikers dwingen het wachtwoord te wijzigen bij de volgende aanmelding**. (**Standaard:** Niet aangevinkt)

Stap 6 Selecteer **Opslaan**.

Uw gebruikerswachtwoordinstellingen configureren

De vereisten en beperkingen van uw gebruikerswachtwoord configureren.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Wachtwoordbeheer** > **Gebruikerswachtwoord**.

Stap 3 Wijzig de instellingen voor gebruikerswachtwoorden door de velden op de pagina te configureren.

Optie	Beschrijving
Sterke wachtwoorden voor gebruikersaccounts verplichten	Selecteer deze optie om de resterende opties in te schakelen. **Standaard:** Geselecteerd
Minimum aantal tekens	Minimale tekenvereisten. **Standaard:** Geselecteerde en **6** tekens
Minimum aantal letters	Minimale alfabetische tekens (niet-numeriek, niet-speciale tekens). **Standaard:** Geselecteerde en **1** teken
Minimum aantal numerieke tekens	Minimale numerieke tekens (niet-alfabetisch, niet-speciale tekens). **Standaard:** Geselecteerde en **1** cijfer
Minimum aantal speciale tekens	Minimale speciale tekens (niet-alfabetische, niet-numerieke tekens). **Standaard:** Niet-geselecteerde en **1** teken
Moet hoofdletters en kleine letters bevatten	Wachtwoord moet hoofdletters en kleine letters bevatten. **Standaard:** Geselecteerd

Optie	Beschrijving
Niet toestaan dat een teken vaker dan 3 keer wordt herhaald	Een teken (alfabetisch, numeriek of speciaal) mag niet meer dan drie keer worden herhaald. **Standaard:** Geselecteerd
Lijst met onacceptabele wachtwoorden	Door beheerder opgestelde lijst van verboden wachtwoorden. **Standaard:** Niet geselecteerd
Bedrijfsnaam, sitenaam, e-mailadres gebruiker en hostnaam zijn nooit acceptabel	Gebruik deze specifieke namen niet. **Standaard:** Geselecteerd
Moet verschillen van de vorige *n* wachtwoorden.	Gebruik geen eerder gebruikte wachtwoorden. Selecteer een nummer in de vervolgkeuzelijst om het aantal vorige wachtwoorden dat u niet kunt gebruiken aan te geven. **Standaard:** Geselecteerd **Standaardnummer**: 5

Stap 4 Selecteer **Opslaan**.

Uw vergaderwachtwoorden configureren

Gebruik deze functie om parameters voor het vergaderingswachtwoord te configureren. De volgende tabel beschrijft welke gebruikers een wachtwoord moeten opgeven wanneer een vergadering is geconfigureerd met een wachtwoord.

Wachtwoord geconfigureerd	Wachtwoord uitgesloten van e-mail uitnodiging	Maker van vergadering aangemeld	Host aangemeld	Uitgenodigde aangemeld	Gast aangemeld	Gast niet aangemeld
Nee	N.v.t.	Wachtwoord niet vereist.	Wachtwoord niet vereist.	Wachtwoord niet vereist.	Wachtwoord niet vereist.	Wachtwoord niet vereist.
Ja	Ja	Wachtwoord niet vereist.	Wachtwoord niet vereist.	Wachtwoord niet vereist.	Wachtwoord vereist.	Wachtwoord vereist.
Ja	Nee	Wachtwoord niet vereist.	Wachtwoord niet vereist.	Wachtwoord niet vereist.	Wachtwoord vereist. Wachtwoord kan vooraf worden ingevuld.	Wachtwoord vereist. Wachtwoord kan vooraf worden ingevuld.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Wachtwoordbeheer** > **Wachtwoord voor vergadering**.

Stap 3 Wijzig de instellingen voor vergaderwachtwoorden door de velden op de pagina te configureren.

Opmerking Niet alle opties zijn standaard geselecteerd.

Optie	Beschrijving
Alle vergaderingen moeten een wachtwoord hebben	Vereist dat alle vergaderingen een wachtwoord hebben.
Sterke wachtwoorden voor vergaderingen verplichten	Selecteer deze optie om de resterende opties in te schakelen.
Minimum aantal tekens	Minimale tekenvereisten. **Standaard:** 6
Minimum aantal letters	Minimale alfabetische tekens (niet-numeriek, niet-speciale tekens). **Standaard:** 1
Minimum aantal numerieke tekens	Minimale numerieke tekens (niet-alfabetisch, niet-speciale tekens). **Standaard:** 1
Minimum aantal speciale tekens	Minimale speciale tekens (niet-alfabetische, niet-numerieke tekens). **Standaard:** 1
Mag niet een van de volgende speciale tekens bevatten (spatie, \, ', ", /, &, <, >, =, [,])	Selecteer deze optie om het gebruik van deze tekens te verbieden.
Moet hoofdletters en kleine letters bevatten	Wachtwoord moet hoofdletters en kleine letters bevatten.
Lijst met onacceptabele wachtwoorden	Door beheerder opgestelde lijst van verboden wachtwoorden.
Bedrijfsnaam, sitenaam, e-mailadres gebruiker, hostnaam en vergaderthema zijn nooit acceptabel	Selecteer deze optie om het gebruik van deze woorden of tekenreeksen te verbieden.

Stap 4 Selecteer **Opslaan**.

Uw e-mailinstellingen configureren

U kunt uw e-mailinstellingen en -sjablonen configureren. Uw e-mailsjablonen hebben standaardinstellingen die u optioneel kunt wijzigen.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **E-mail**.
De pagina **Variabelen** verschijnt.

Stap 3 Voer bij **Naam afzender**, **E-mail afzender** en **Antwoorden aan** de gewenste gegevens in en selecteer vervolgens **Opslaan**.

Opmerking U kunt op de pagina Variabelen bij Naam afzender de naam van een persoon invoeren, maar in uitnodigingen voor vergaderingen zal het e-mailadres van de host worden weergegeven.

Stap 4 Selecteer **Sjablonen**. Raadpleeg Over e-mailsjablonen, op pagina 204 voor een beschrijving van elk sjabloontype.
De pagina **Sjablonen** wordt weergegeven. Selecteer het tabblad **Algemeen** of **Vergaderingen**. **Algemeen** is standaard.

Stap 5 Selecteer de gewenste sjabloonkoppeling op het tabblad **Algemeen** en **Vergaderingen** om e-mailsjablonen te configureren.

Stap 6 Maak indien nodig wijzingen aan het geselecteerde e-mailsjabloon en selecteer **Opslaan**.

Voorbeeld:
Selecteer de sjabloonkoppeling **Account opnieuw geactiveerd** op het tabblad **Algemeen**. Wijzig de velden in het dialoogvenster **Account opnieuw geactiveerd** en selecteer **Opslaan**.
De standaardwaarden voor **Naam van** en **E-mailadres afzender** en **Antwoorden aan** zijn afkomstig van de instellingen op de pagina **Variabelen**.

Opmerking Als u bij **Naam afzender** op de pagina **Variabelen** de naam van een persoon invoert, vervangt het systeem deze voor alle uitnodigingen voor vergaderingen automatisch door de URL van de WebEx-site.

Over e-mailsjablonen

Gebruik de e-mailsjablonen om belangrijke gebeurtenissen naar gebruikers te communiceren. Elk e-mailsjabloon heeft variabelen die u moet instellen. Zie de tabel hieronder voor beschrijvingen van de variabelen in elk sjabloon.

Er zijn twee typen e-mailsjablonen:

- Algemeen–Bevat vergeten wachtwoord, meldingen voor hosts en genodigden, opnamemogelijkheid en andere algemene mededelingen.
- Vergaderingen–Bevat uitnodigingen voor vergaderingen, annuleringen, updates, herinneringen en informatiemededelingen.

Tabel 3: Algemene e-mailsjablonen

Titel	Beschrijving	Variabelen
AD-activering	Verstuurd naar een gebruiker nadat een AD-account is geactiveerd.	• %SiteURL% • %DisplayName% • %SSOSignINLink% • %OrgLogo% • %Participants% • %Support% • %CustomFooterText% • %Jaar%
AD-synchronisatie is mislukt	Wordt naar de beheerder verzonden nadat een synchronisatie is mislukt.	• %FullName% • %Failure_Reason% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
AD-synchronisatie voltooid	Wordt naar de beheerder verzonden nadat een synchronisatie is voltooid.	• %FullName% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Account opnieuw geactiveerd	Verzonden naar een gebruiker nadat een beheerder het account van de gebruiker opnieuw activeert.	• %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Wachtwoord vergeten–Wachtwoord gewijzigd	Verzonden naar een gebruiker nadat hij zijn wachtwoord heeft hersteld vanaf de eindgebruikersite.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Wachtwoord vergeten–Wachtwoord herstellen	Verzonden naar een gebruiker nadat hij zijn wachtwoord heeft hersteld vanaf de eindgebruikersite. Deze e-mail vraagt de gebruiker een nieuw wachtwoord te maken.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
PT PCN-vergaderingsuitnodiging - Genodigde	Verzonden naar genodigden van een vergadering nadat een vergadering is gepland met Productiviteitstools van een PCN-account.	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
PT PCN-vergaderingsmelding - Host	Verzonden naar de host van een vergadering nadat een vergadering is gepland met Productiviteitstools van een PCN-account.	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
PT-Hostmelding	Verzonden naar een vergaderingshost nadat een vergadering is gepland met Productiviteitstools.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
PT-Genodigdenmelding	Verzonden naar genodigden van een vergadering nadat een vergadering is gepland met Productiviteitstools.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
Opnemen beschikbaar voor host	Stuurt een koppeling met een vergaderingsopname naar de host.	• %SiteURL% • %OrgLogo% • %DisplayName% • %Topic Name% • %Duur% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
SSO activeringse-mail	Verzonden nadat Single Sign-On (SSO) is ingeschakeld.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Stuur e-mail naar alle gebruikers	Stuurt een e-mail naar alle gebruikers in het systeem.	• %SiteURL% • %Subject% • %OrgLogo% • %AttendeeName% • %Body% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Cisco WebEx-Android instellen	Informeert gebruikers over de Cisco WebEx-app voor Android en levert een downloadkoppeling voor de app.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Cisco WebEx instellen - iPhone/iPad	Informeert gebruikers over de Cisco WebEx-app voor iPhone/iPad en levert een downloadkoppeling voor de app.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Opname delen	Stuurt een koppeling met een vergaderingsopname naar geselecteerde vergaderingsdeelnemers.	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %HostName% • %Topic Name% • %Duur% • %Recording Time% • %Personalized Message% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Opname van MC delen	Stuurt een koppeling met een vergaderingsopname naar geselecteerde vergaderingsdeelnemers. Deelnemers geselecteerd door de host in Meeting Center na het selecteren van **Vergadering verlaten**.	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %Topic Name% • %Duur% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Gebruikers - wachtwoord gewijzigd	Stuurt gebruikers een e-mail wanneer hun wachtwoord is gewijzigd.	• %SiteURL% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Welkomstbericht	Verzonden naar een nieuwe beheerder nadat zijn of haar account is gemaakt.	• %SiteURL% • %DisplayName% • %SiteURL% • %Support% • %participants% • %CustomFooterText% • %Jaar%

Tabel 4: E-mailsjablonen voor vergaderingen

Titel	Beschrijving	Variabelen
Lopende vergaderingsuitnodiging voor deelnemer	Verzonden naar gebruikers wanneer een host ze uitnodigt voor een vergadering terwijl de vergadering actief is.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Directe vergaderingsuitnodiging voor host	Verzonden naar de host en deelnemers wanneer de host **Nu vergaderen** selecteert.	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Vergadering geannuleerd voor deelnemer	Informeert een gebruiker dat een geplande vergadering is geannuleerd.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Jaar%
Vergadering geannuleerd voor host	Verzonden naar de host van de vergadering om annulering van een vergadering te bevestigen.	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Vergaderingsinformatie bijgewerkt voor alternatieve host	Biedt vergaderingsinformatie voor de alternatieve host wanneer de vergaderingsinstellingen zijn gewijzigd.	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duur% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Vergaderingsinformatie bijgewerkt voor deelnemer	Biedt vergaderingsinformatie voor een genodigde van een vergadering wanneer de vergaderingsinstellingen zijn gewijzigd.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Vergaderingsgegevens bijgewerkt voor host	Biedt vergaderingsinformatie voor de host wanneer de vergaderingsinstellingen zijn gewijzigd.	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Vergaderingsherinnering voor alternatieve host	Stuurt een vergaderingsherinnering naar de alternatieve host van de vergadering.	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duur% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Vergaderingsherinnering voor host	Stuurt een vergaderingsherinnering naar de host van de vergadering.	• %SiteURL% • %Topic% • %OrgLogo% • %HostName% • %MeetingTime% • %HostName% • %Duur% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Vergadering opnieuw gepland voor alternatieve host	Stuurt bijgewerkte vergaderingsinformatie naar de alternatieve host.	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Vergadering opnieuw gepland voor deelnemer	Stuurt bijgewerkte vergaderingsinformatie naar deelnemers.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Vergaderingsinformatie voor alternatieve host	Stuurt een vergaderingsbevestiging naar de alternatieve host.	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Vergaderingsinformatie voor deelnemer	Stuurt een uitnodiging voor vergadering naar deelnemers.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%
Vergaderingsinformatie voor host	Stuurt een vergaderingsbevestiging naar de host.	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Jaar%

Titel	Beschrijving	Variabelen
Automatische herinnering PCN-vergadering - Host	Stuurt een automatische vergaderingsherinnering naar de host van de vergadering (alleen PCN-accounts).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Uitnodiging PCN-vergadering - Genodigde	Stuurt een vergaderingsuitnodiging naar genodigden (alleen PCN-accounts).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Titel	Beschrijving	Variabelen
Handmatige herinnering PCN-vergadering - Host	Stuurt een handmatige vergaderingsherinnering naar de host van de vergadering (alleen PCN-accounts).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Handmatige herinnering PCN-vergadering - Genodigde	Stuurt een handmatige vergaderingsherinnering naar genodigden (alleen PCN-accounts).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Titel	Beschrijving	Variabelen
Melding PCN-vergadering - Host	Stuurt een vergaderingsmelding naar de host (alleen PCN-accounts).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Directe uitnodiging PCN-vergadering - Host	Er wordt een melding voor een directe vergadering naar de host verzonden (alleen PCN-accounts).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %SiteURL% • %Support%

Titel	Beschrijving	Variabelen
Uitnodiging PCN-vergadering die bezig is - Genodigde	Er wordt een melding voor een directe vergadering naar een genodigde verzonden (alleen PCN-accounts).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
Planningswijziging voor PCN-vergadering - Host	Er wordt een melding naar de host verzonden dat de planning is gewijzigd (alleen PCN-accounts).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%

Titel	Beschrijving	Variabelen
Planningswijziging voor PCN-vergadering - Genodigde	Er wordt een melding naar een genodigde verzonden dat de planning is gewijzigd (alleen PCN-accounts).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
PCN-vergadering opnieuw gepland - Genodigde	Er wordt een melding naar een genodigde verzonden dat de vergadering opnieuw is gepland (alleen PCN-accounts).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Titel	Beschrijving	Variabelen
PCN-vergadering geannuleerd - Host	Er wordt een melding naar de host verzonden dat de vergadering is geannuleerd (alleen PCN-accounts).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%
PCN-vergadering geannuleerd - Genodigde	Er wordt een melding naar een genodigde verzonden dat de vergadering is geannuleerd (alleen PCN-accounts).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%

Uw downloadinstellingen configureren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Downloads**.

Stap 3 Schakel het selectievakje **WebEx productiviteitstools automatisch bijwerken** in om regelmatige automatische updates te configureren. (**Standaard:** ingeschakeld.)

Opmerking Als u van plan bent handmatig WebEx-productiviteitstools naar uw gebruikers te pushen, raden we u aan om dit selectievakje uit te schakelen.

Stap 4 Selecteer uw downloadmethode:

- Gebruikers toestaan om WebEx-bureaubladtoepassingen te downloaden
- WebEx Meetings en Productiviteitstools handmatig naar het bureaublad van de gebruiker pushen

Als u **Gebruikers toestaan om WebEx-bureaubladtoepassing te downloaden** selecteert, kunt u **Opslaan** selecteren om uw downloadconfiguratie te voltooien. U hoeft verder niets te doen. Als u **WebEx Meetings**

en Productivity Tools handmatig naar bureaublad van gebruikers pushen selecteert, ga dan naar de volgende stap.

Als u **Cisco WebEx Meetings en Productiviteitstools handmatig naar het bureaublad van de gebruiker pushen** selecteert, verschijnen de WebEx Meetings-toepassing, Productivitytools en de onderdelen voor de WebEx-speler voor netwerkopnamen op de pagina.

Stap 5 Selecteer voor elke toepassing die u wilt downloaden en installeren **Download** en **Opslaan** om een ZIP-bestand met installatieprogramma's voor de betreffende toepassing op uw systeem op te slaan.
Elk ZIP-bestand bevat installatieprogramma's voor de toepassing ten aanzien van alle ondersteunde talen en platforms.

Stap 6 Selecteer **Opslaan** om uw downloadinstellingen op te slaan.

Over downloads

Dit product kan gebruikt worden op Windows-pc's waar gebruikers beheerdersrechten hebben en op deze die dat niet hebben. Deze rubriek biedt basisinformatie over downloads. Raadpleeg de rubriek Over downloads van de Planningshandleiding voor gedetailleerde informatie over de configuratie van downloads.

Op pc's zonder beheerdersrechten:

- Wij adviseren u om de Cisco WebEx Meetings-toepassing en Productivity Tools offline te pushen naar het bureaublad van eindgebruikers voordat u eindgebruikers informeert dat er een gebruikersaccount voor hen is aangemaakt. Dit zorgt ervoor dat uw gebruikers vergaderingen kunnen starten en eraan deelnemen vanaf hun webbrowser en Windows-bureaublad als ze zich de eerste keer aanmelden.
- U kunt de .MSI-installatieprogramma's voor elk verkrijgen op de beheerwebsite op de pagina **Instellingen** > **Downloads** Zie Uw downloadinstellingen configureren, op pagina 224 voor meer informatie.
- Als u beslist de toepassingen niet naar uw gebruikers te pushen, kunnen ze nog steeds toegang krijgen tot deze toepassingen van op de pagina's met downloads voor de eindgebruiker. Als hun computer echter installatie van gedownloade toepassingen verbiedt, zullen zij niet in staat zijn om het installatieproces te voltooien.
- Wanneer gebruikers deelnemen aan vergaderingen via hun webbrowser (de WebEx Meetings-toepassing kan nog steeds op aanvraag gedownload worden), kunnen ze zonder problemen deelnemen aan vergaderingen. Bovendien probeert de WebEx Meetings-toepassing om een installatie uit te voeren om het proces van starten of deelnemen aan toekomstige vergaderingen te versnellen. Dit mislukt omdat de computer geen beheerdersrechten heeft.

Op pc's met beheerdersrechten:

- Gebruikers kunnen de WebEx Meetings-toepassing en Productivity Tools downloaden en installeren vanaf de pagina's met downloads voor de eindgebruiker. Er is geen extra beheerdersactie vereist.
- Gebruikers worden geadviseerd de productiviteitstools te installeren wanneer zij zich voor het eerst aanmelden.
- De WebEx Meetings-toepassing wordt op aanvraag gedownload de eerste keer dat een gebruiker deelneemt aan een vergadering en wordt op de achtergrond geïnstalleerd op de pc van de gebruiker.

Certificaten beheren

Certificaten worden gebruikt om een veilige communicatie tussen de componenten van uw systeem te garanderen. Wanneer uw systeem voor het eerst wordt geïmplementeerd, wordt het geconfigureerd met een zelfondertekend certificaat. Hoewel een zelfondertekend certificaat tot vijf jaar kan meegaan, dringen wij erop aan dat u certificaten configureert die gevalideerd zijn door een certificerende instantie. Een certificerende instantie verzekert dat communicatie tussen uw virtuele machines is geverifieerd. Houd er rekening mee dat u een certificaat moet hebben voor elke virtuele machine op uw systeem.

De volgende certificaattypen worden ondersteund:

- SSL—Vereist op alle systemen.
- SSO IdP—Voor SSO-certificaten met identiteitsprovider (IdP).
- Beveiligde teleconferentie—Vereist voor TLS-teleconferenties. U kunt tot twee veilige teleconferentiecertificaten configureren, één voor elk CUCM-systeem dat u kiest om te configureren.

Alle systemen moeten een SSL-certificaat hebben. Dit product ondersteunt de volgende SSL-certificaten:

- Zelfondertekend
- Ondertekend door een certificerende instantie
- Ondertekend door een externe certificerende instantie

U kunt uw certificaten niet bijwerken. Als u virtuele machines aan uw systeem toevoegt of uw bestaande virtuele machines wijzigt, moet u nieuwe certificaten genereren voor elke virtuele machine op uw systeem.

SSL-certificaten kunnen ongeldig worden voor de volgende redenen:

- Uw systeemgrootte is uitgebreid, wat heeft geleid tot de implementatie van nieuwe virtuele machines. De fully qualified domain names (FQDN's) van deze nieuwe virtuele machines zijn niet aanwezig in uw oorspronkelijke SSL-certificaat.
- Er is een systeem met hoge beschikbaarheid toegevoegd, wat heeft geleid tot de implementatie van nieuwe virtual machines. De FQDN's van deze nieuwe virtuele machines bestaan niet in uw oorspronkelijke SSL-certificaat.
- De URL van de Cisco WebEx-site is veranderd. Deze URL bestaat niet in uw oorspronkelijke SSL-certificaat.
- De URL van de Beheersite is veranderd. Deze URL bestaat niet in uw oorspronkelijke SSL-certificaat.
- De FQDN van de virtuele machine voor beheer is veranderd. Deze FQDN bestaat niet in uw oorspronkelijke SSL-certificaat.
- Uw huidige SSL-certificaat is verlopen.

Als uw SSL-certificaat om eender welke reden ongeldig wordt, zal uw systeem automatisch nieuwe zelfondertekende certificaten genereren en u wordt op de hoogte gebracht van deze wijziging door een algemeen waarschuwingsbericht bovenaan de pagina van de Beheersite, wat erop wijst dat SSL ongeldig geworden is.

SSL-certificaten genereren

Uw systeem moet een SSL-certificaat hebben geconfigureerd. Dit product ondersteunt de volgende typen SSL-certificaten:

- Zelfondertekend
- Ondertekend door een certificerende instantie
- Ondertekend door een externe certificerende instantie

Een CSR maken (Ondertekeningsaanvraag certificaat)

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Certificaten** > **CSR maken**.

Stap 4 Vul de velden in op de pagina **CSR maken (Ondertekeningsaanvraag certificaat)**.

Optie	Beschrijving
Algemene naam	Selecteer certificaat **Onderwerp alternatieve namen** of certificaat **Wildcard**.
Onderwerp alternatieve namen **Opmerking** Deze optie wordt alleen weergegeven als u **Onderwerp alternatieve namen** selecteert voor uw type algemene naam.	De namen van uw beheersite en uw virtuele machines. Alternatieve namen zijn niet vereist als u een algemene naam met joker hebt geselecteerd.
Organisatie	Geef uw organisatienaam op.
Afdeling	Geef uw afdelingsnaam op.
Plaats	Voer de plaatsnaam in.
Staat/provincie	Voer uw staat/provincie in.
Land	Selecteer uw land.
Sleutelgrootte	Selecteer uw sleutelgrootte uit de volgende opties: • 2048 **Standaard:** 2048 (Aanbevolen)

Stap 5 Selecteer **CSR maken**.

Het dialoogvenster **CSR downloaden** wordt weergegeven.

Stap 6 Selecteer **Downloads**.
U ontvangt een ZIP-bestand die CSR en de bijhorende privésleutel bevat. Het CSR-bestand heet csr.pem en het bestand met de privésleutel heet csr_private_key.pem.

Stap 7 Maak een back-up van uw systeem met behulp van VMware-gegevensherstel (vSphere 5.0) of VMware vSphere-gegevensbeveiliging (vSphere 5.1). Zie Een back-up maken met VMware vCenter, op pagina 4 voor meer informatie.
Opmerking Een back-up van uw systeem bewaart de privésleutel in het geval dat u deze moet herstellen.

Stap 8 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Een SSL-certificaat importeren

U kunt een SSL-certificaat importeren met behulp van deze functie. De Cisco WebEx-vergaderingsserver ondersteunt X.509-certificaten met PEM- en DER-codering en PKCS12-archieven.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Certificaten** > **Meer opties** > **SSL-certificaat/privécode importeren**.
Als u al een certificaat hebt geïnstalleerd, waarschuwt het systeem u dat een nieuw certificaat het zal overschrijven.

Stap 4 Selecteer **Doorgaan**.

Stap 5 Selecteer **Bladeren** en kies uw certificaatbestand.
U moet een met X.509 compatibel certificaat of certificaatketen selecteren. Geldige types zijn onder andere:

- Certificaat met PEM-/DER-codering: CER / .CRT / .PEM / .KEY
- Certificaat met PKCS12-codering: .P12 / .PFX

U kunt een certificaatketen importeren via een PKCS#12-bestand of via één enkel bestand bestaande uit PEM-blokken. Als u een PEM-bestand gebruikt, moet u dit als volgt opmaken:

- (Optioneel) Als u een private code wilt uploaden, moet de privécode het eerste blok in het bestand zijn. De code kan wel of niet gecodeerd zijn. Het bestand moet de PKCS#8-indeling hebben, PEM-gecodeerd. Als de code is gecodeerd, moet u het wachtwoord invoeren om het te decoderen in het veld voor de wachtwoordzin.
- Het volgende element moet het certificaat zijn van de instantie voor aanvullende certificaten die uw certificaat in PEM-gecodeerde X.509-indeling uitgaf.

- U kunt alle aanvullende certificaten bijvoegen die u gebruikt in uw infrastructuur. Het certificaat van de instantie voor hoofdcertificaten moet niet worden bijgevoegd. Als u een instantie voor private certificaten gebruikt, moet u ervoor zorgen dat het hoofdcertificaat naar alle clients wordt gedistribueerd.

Alle certificaten moeten samen worden geüpload in één bestand. U kunt niet één certificaat uploaden en de aanvullende certificaten pas later toevoegen. Misschien wilt u de aanvullende certificaten uploaden als u een certificerende instantie gebruikt die aanvullende certificaten gebruikt en als de aanvullende certificaten niet in hun clients zijn gedistribueerd. Door de certificaten te uploaden voorkomt u waarschuwingen.

PKCS#12-bestanden moeten een .p12-extensie hebben. Ze mogen alleen de certificaten en privécode (optioneel) bevatten.

Stap 6 Selecteer **Uploaden**.
Nadat u **Uploaden** selecteert, controleert het systeem of uw certificaat geldig is. Een certificaat kan ongeldig zijn voor de volgende redenen:

- Het certificaatbestand is geen geldig certificaatbestand.
- Het door u geselecteerde certificaatbestand is verlopen.
- Uw publieke code moet minstens 2048 bits zijn.
- De serverdomeinen in het certificaat komen niet overeen met de URL van de site.
- De privécode die automatisch is gegenereerd door het systeem is niet compatibel met het certificaat.

Als het certificaat geldig is, gaat u naar de volgende stap. Als het certificaat niet geldig is, kunt u het niet uploaden. U moet een geldig certificaat selecteren voordat u kunt doorgaan.

Stap 7 (Optioneel) Geef een wachtwoordzin op in het veld **Wachtwoordzin**.
Opmerking Een wachtwoordzin is vereist om PKCS12-archieven of een gecodeerde privésleutel te decoderen (indien geüploade .pem-bestanden de privésleutel bevatten).

Stap 8 Selecteer **Doorgaan**.
Uw systeem importeert uw SSL-certificaat en geeft het weer in een dialoogvenster waar u kunt scrollen.

Stap 9 Selecteer **Klaar**.

Stap 10 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Een SSL-certificaat exporteren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **Certificaten** > **Meer opties** > **SSL-certificaat exporteren**.

Stap 3 Sla het certificaatbestand op.

Volgende stappen

Zorg ervoor dat zowel beheerders als eindgebruikers zich kunnen aanmelden op de beheer- of webpagina's zonder browserwaarschuwingen voor onbetrouwbare site te zien.

Een SSL-certificaat voor mobiele apparaten exporteren

Op Apple iPhones en iPads waarop Apple iOS 5.0 of hoger wordt uitgevoerd, is een vertrouwd basiscertificaat geïntegreerd. Als uw bedrijf een zelfondertekend certificaat gebruikt of als het hoofdcertificaat op uw Cisco WebEx Meetings Server zich niet op de lijst met door Apple vertrouwde certificeringsinstanties bevindt, moet u een SSL-certificaat exporteren en dit naar uw gebruikers mailen. Uw gebruikers moeten het certificaat op hun mobiele apparaat installeren voordat ze een WebEx-vergadering kunnen bijwonen.

Opmerking Het exporteren van een SSL-certificaat is alleen vereist als u een zelfondertekend certificaat gebruikt. Als u gebruikmaakt van een vertrouwd certificaat dat door een certificeringsinstantie is ondertekend, is het exporteren van een SSL-certificaat niet vereist.

Voordat u begint

Verifieer of het vertrouwde basiscertificaat dat vooraf op de Apple iPhone of iPad van de gebruiker is geïnstalleerd, op de lijst met vertrouwde Apple-certificeringsinstanties staat. Zie http://support.apple.com/kb/ht5012 voor meer informatie.

Opmerking Gebruikers moeten over een actieve, snelle internetverbinding voor hun mobiele apparaat beschikken.

Procedure

Stap 1 Meld u aan bij de beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **Certificaten**.

Stap 3 Kopieer de certificaatnaam van het gedeelte SSL-certificaten.

Stap 4 Selecteer **Meer opties** > **SSL-certificaat exporteren**.

Stap 5 Sla het certificaatbestand op uw lokale harde schijf op.

Stap 6 Voeg het opgeslagen certificaatbestand als bijlage aan een e-mail toe en verzend deze naar de iOS-e-mailaccounts van de gebruikers.

Stap 7 Gebruikers openen de e-mail op hun mobiele apparaat en slaan het bestand op.

Stap 8 Gebruikers installeren het certificaatbestand op hun mobiele apparaat:

a) Tik op **Installeren** op de pagina **Profiel installeren**.
b) Tik op **Nu installeren** in het dialoogvenster voor het niet-ondertekende profiel.
c) Voer het iOS-wachtwoord van een gebruiker in.
d) Tik op **Volgende**.
e) Tik op **Gereed**.

Uw CSR en private code downloaden

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **Meer opties** > **CSR downloaden**.
Er verschijnt een dialoogvenster waarin u wordt gevraagd het bestand, CSR.zip, op te slaan, dat de CSR en private code bevat.

Stap 3 Selecteer op welke locatie binnen uw systeem u het bestand wilt opslaan, en selecteer vervolgens **OK**.

Stap 4 Maak een back-up van het bestand dat uw private code bevat, csr-private-key.pem, voor het geval u de code later nog nodig hebt.

Een zelfondertekend certificaat genereren

Er wordt automatisch een zelfondertekend certificaat gegenereerd nadat u uw systeem hebt geïmplementeerd. We raden u aan een certificaat te installeren die is ondertekend door een certificerende instantie. U kunt altijd een nieuw zelfondertekend certificaat genereren door deze functie te gebruiken.

Opmerking Gebruikers kunnen problemen ondervinden met het bijwonen van vergaderingen als hun systeem gebruik maakt van een zelfondertekend certificaat, tenzij de beheerder aan de client-zijde het systeem voor het gebruik van zelfondertekende certificaten heeft geconfigureerd.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Certificaten** > **Meer opties** > **Zelfondertekend certificaat genereren**.

Stap 4 Vul de velden in op de pagina **Zelfondertekend certificaat genereren**.

Optie	Beschrijving
Certificaatnaam	Voer een naam in voor uw zelfondertekende certificaat. (Vereist)
X.509-onderwerpnaam	De hostnaam van uw systeem. (niet configureerbaar)
Organisatie	Geef uw organisatienaam op.
Afdeling	Geef uw afdelingsnaam op.
Plaats	Voer de naam van uw stad in.
Staat/provincie	Voer de naam van uw provincie in.

Optie	Beschrijving
Land	Selecteer uw land.

Stap 5 Selecteer **Certificaat en privésleutel maken**.

Opmerking Als u na een belangrijke upgrade hetzelfde SSL-certificaat moet gebruiken, moet u de privécode uploaden die samen met de CSR is gegenereerd waarmee het certificaat is verkregen. De privécode moet het eerste blok zijn in het certificaatbestand.

Uw certificaatbestand wordt gegenereerd en weergegeven.

Stap 6 Selecteer **Klaar**.

Stap 7 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Een SSL-certificaat herstellen

In het geval dat uw certificaat ongeldig wordt of u een noodherstel op uw systeem hebt uitgevoerd, kunt u een SSL-certificaat herstellen met behulp van deze functie. De Cisco WebEx-vergaderingsserver ondersteunt X.509-certificaten met PEM- en DER-codering en PKCS12-archieven.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Certificaten** > **Meer opties** > **SSL-certificaat importeren**.
Als u al een certificaat hebt geïnstalleerd, waarschuwt het systeem u dat een nieuw certificaat het zal overschrijven.

Stap 4 Selecteer **Doorgaan**.

Stap 5 Selecteer **Bladeren** en kies uw certificaatbestand.
U moet een met X.509 compatibel certificaat of certificaatketen selecteren. Geldige types zijn onder andere:

- Certificaat met PEM-/DER-codering: CER / .CRT / .PEM / .KEY
- Certificaat met PKCS12-codering: .P12 / .PFX

U kunt een certificaatketen importeren via een PKCS#12-bestand of via één enkel bestand bestaande uit PEM-blokken. Als u een PEM-bestand gebruikt, moet u dit als volgt opmaken:

- (Optioneel) Als u een vorige combinatie van publieke code of privécode opnieuw wilt gebruiken voor een noodherstel, dient u het bestand voor de publieke code (csr_private_key.pem) en het certificaat dat u hebt ontvangen van uw certificerende instantie (CA, Certificate Authority) in één bestand samen te voegen. De privécode moet het eerste blok zijn in het certificaatbestand, waarna de publieke code volgt. De code kan wel of niet gecodeerd zijn. Het bestand moet de PKCS#8-indeling hebben en PEM-gecodeerd zijn. Als de code is gecodeerd, moet u het wachtwoord invoeren om het te decoderen in het veld voor de wachtwoordzin.

- Het volgende element moet het certificaat zijn van de instantie voor aanvullende certificaten die uw certificaat in PEM-gecodeerde X.509-indeling uitgaf.
- U kunt alle aanvullende certificaten bijvoegen die u gebruikt in uw infrastructuur. Het certificaat van de instantie voor hoofdcertificaten moet niet worden bijgevoegd. Als u een instantie voor private certificaten gebruikt, moet u ervoor zorgen dat het hoofdcertificaat naar alle clients wordt gedistribueerd.

Alle certificaten moeten samen worden geüpload in één bestand. U kunt niet één certificaat uploaden en de aanvullende certificaten pas later toevoegen. Misschien wilt u de aanvullende certificaten uploaden als u een certificerende instantie gebruikt die aanvullende certificaten gebruikt en als de aanvullende certificaten niet in hun clients zijn gedistribueerd. Door de certificaten te uploaden voorkomt u waarschuwingen.

PKCS#12-bestanden moeten een .p12-extensie hebben. Ze mogen alleen de certificaten en privécode (optioneel) bevatten.

Stap 6 Selecteer **Uploaden**.
Nadat u **Uploaden** selecteert, controleert het systeem of uw certificaat geldig is. Een certificaat kan ongeldig zijn voor de volgende redenen:

- Het certificaatbestand is geen geldig certificaatbestand.
- Het door u geselecteerde certificaatbestand is verlopen.
- Uw publieke code moet minstens 2048 bits zijn.
- De serverdomeinen in het certificaat komen niet overeen met de URL van de site.
- De privécode die automatisch is gegenereerd door het systeem is niet compatibel met het certificaat.

Als het certificaat geldig is, gaat u naar de volgende stap. Als het certificaat niet geldig is, kunt u het niet uploaden. U moet een geldig certificaat selecteren voordat u kunt doorgaan.

Stap 7 (Optioneel) Geef een wachtwoordzin op in het veld **Wachtwoordzin**.
Opmerking Een wachtwoordzin is vereist om PKCS12-archieven of een gecodeerde privésleutel te decoderen (indien geüploade .pem-bestanden de privésleutel bevatten).

Stap 8 Selecteer **Doorgaan**.
Uw systeem importeert uw SSL-certificaat en geeft het weer in een dialoogvenster waar u kunt scrollen.

Stap 9 Selecteer **Verdergaan** op de pagina **SSL-certificaat** om de importbewerking te voltooien.

Stap 10 Selecteer **Klaar**.

Stap 11 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

SSO IdP-certificaten importeren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **SSO IdP-certificaat**.

Stap 3 Selecteer **Bladeren** en kies uw SSO IdP-certificaat.

Stap 4 Selecteer **Uploaden**.
Uw certificaatbestand wordt weergegeven.

Stap 5 Selecteer **Klaar** om uw certificaat te verzenden.

Certificaten voor beveiligde teleconferenties importeren

Er zijn enkel veilige teleconferentiecertificaten vereist als TLS-conferentie ingeschakeld is. Als TLS-conferentie niet ingeschakeld is, is deze optie niet beschikbaar.

Voordat u begint

Er zijn veilige teleconferentiecertificaten vereist voor uw CUCM-servers wanneer TLS geselecteerd is als het transporttype in uw audio-instellingen. Zie Over het configureren van uw audio-instellingen, op pagina 192 voor meer informatie.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Certificaten**.
De rubriek Veilig teleconferentiecertificaat geeft één van de volgende twee berichten weer:

- Voor dit systeem zijn geen certificaten voor beveiligde teleconferentie vereist omdat TLS-teleconferentie niet is ingeschakeld.
- CUCM-certificaten voor beveiligde conferentie zijn nodig voor TLS teleconferenties, die zijn ingeschakeld op dit systeem.

Als er veilige teleconferentiecertificaten vereist zijn, wordt de knop **Certificaat importeren** getoond voor elke CUCM-server dat geconfigureerd moet worden.

Stap 4 Selecteer **Certificaat importeren** voor CUCM 1.
De pagina **Certificaat voor beveiligde teleconferentie** verschijnt.

Stap 5 Voer een certificaatnaam in.

Stap 6 Selecteer **Bladeren** en kies uw certificaatbestand.

Opmerking Gebruik het bestand CallManager.pem als CUCM gebruikmaakt van zelfondertekende certificaten. Gebruik het certificaat van een instantie voor basiscertificaten als CUCM gebruikmaakt van certificaten van derden. Zie 'CUCM-certificaten downloaden' in de *Planningshandleiding* voor meer informatie over het downloaden van een CUCM-certificaat op uw lokale harde schijf.

Stap 7 Selecteer **Uploaden**.
Nadat u **Uploaden** selecteert, controleert het systeem of uw certificaat geldig is.

Als het certificaat geldig is, gaat u naar de volgende stap. Als het certificaat niet geldig is, kunt u het niet uploaden. U moet een geldig certificaat selecteren voordat u kunt doorgaan.

Stap 8 Selecteer **Doorgaan**.
Uw systeem importeert uw SSL-certificaat en geeft het weer in een dialoogvenster waar u kunt scrollen. U krijgt een melding dat u een SSL-certificaat hebt geïmporteerd.

Stap 9 Selecteer **Klaar**.

Stap 10 Keer terug naar stap 4 en herhaal het proces voor uw CUCM 2-server.

Stap 11 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Veiligheid gebruikerssessie configureren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **Gebruikerssessies**.

Stap 3 Vul de velden in op de pagina **Gebruikerssessies** om de vervaltijd van de webpagina in te stellen.

Optie	Beschrijving
Vervaldag webpagina	Configureer dagen, uren en minuten voordat gebruikers automatisch worden afgemeld. **Standaard:** Een uur en 30 minuten.
Vervaldatum mobiele tools of productiviteitstools (SSO)	Configureer dagen, uren en minuten voordat gebruikers automatisch worden afgemeld. **Standaard:** 14 dagen **Opmerking** Dit veld verschijnt enkel indien SSO is geconfigureerd.

Stap 4 Selecteer **Opslaan**.

Gefedereerd eenmalig aanmelden (SSO) configureren

Dankzij de configuratie van SSO kunnen uw eindgebruikers zich aanmelden bij het systeem met behulp van hun bedrijfsgegevens, wat u een manier geeft om het product op te nemen in uw bedrijfsdirectory. U kunt ook SSO configureren om snel gebruikersaccounts aan te maken of beheren wanneer gebruikers een poging doen zich aan te melden.

Opmerking SSO configureren kan een ingewikkelde materie zijn en we raden u dan ook sterk aan contact op te nemen met uw Cisco Channel Partner of Cisco Advances Services voordat u verdergaat.

Voordat u begint

- Voordat u de gefedereerde SSO-service inschakelt, moet u een reeks publieke en privécodes instellen en een X.509-certificaat dat de publieke code bevat. Zodra u een openbare code of certificaat hebt, moet u deze uploaden naar het gedeelte Certificaten beheren, op pagina 226.

  Opmerking Nadat u SSO hebt ingeschakeld, worden de gebruikersgegevens beheerd door het verificatiesysteem van uw bedrijf. Bepaalde functies voor wachtwoordbeheer zijn niet meer van toepassing op uw gebruikers. Zie Wachtwoorden configureren, op pagina 200 en Gebruikers bewerken, op pagina 138 voor meer informatie. Denk eraan dat hoewel beheerders ook eindgebruikers zijn, ze niet aanmelden aan de hand van SSO. Zij melden zich aan aan de hand van hun beheerdersgegevens voor dit product.

- Configureer een SSO IdP-certificaat om deze functie te gebruiken. Zie SSO IdP-certificaten importeren, op pagina 234 voor meer informatie.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **Gefedereerde SSO**.

Stap 3 Nadat u publieke- en privécodes en een X.509-certificaat hebt gegenereerd, zoals beschreven in de randvoorwaarden, selecteert u **Doorgaan**.

Stap 4 Selecteer uw initiëringsmethode:

- Geïnitieerd door SP (Service Provider)?Gebruikers selecteren een koppeling naar de service provider en worden tijdelijk omgeleid naar de identiteitsprovider voor verificatie. Gebruikers worden vervolgens teruggestuurd naar de koppeling die ze initieel aanvroegen.
- Door IdP (Identiteitsprovider) geïnitieerd?Dit houdt in dat een gebruiker onmiddellijk begint bij de identiteitsprovider, aanmeldt en daarna wordt doorgestuurd naar een landingspagina bij de serviceprovider.

Stap 5 Vul de velden in en selecteer uw opties op de pagina **SSO-configuratie**:

Opmerking Raadpleeg uw IdP-configuratiebestand om de IdP-velden te voltooien. Selecteer de koppeling **IdP-certificaat**.

Veld	Beschrijving
SP (Service Provider) gestart	Selecteer deze optie voor aanmelden via de serviceprovider.
AuthnRequest ondertekend	Selecteer deze optie om te vereisen dat het AuthnRequest-bericht moet zijn getekend met de privésleutel van de serviceprovider. **Opmerking** U moet deze optie selecteren indien u wilt dat uw geëxporteerd bestand met SAML-metagegevens het SSL-certificaat van uw site bevatten.
Destination	De URL van de SAML 2.0-implementatie van IdP dat te verwerken verificatieaanvragen ontvangt. **Opmerking** Dit veld verschijnt enkel als **AuthnRequest ondertekend** is geselecteerd.
IdP (Identity Provider) gestart	Selecteer deze optie voor aanmelden via de identiteitsprovider.
Parameternaam URL doelpagina	Uw systeem wordt omgeleid naar deze URL wanneer SSO geslaagd is. **Standaard:** Doel **Opmerking** Bij een IdP-geïnitieerd systeem, moet de URL een gecombineerde URL in het volgende formaat zijn: de aanmeldings-URL van uw service, "?" of "&", de URL-parameter van de doelpagina, "=" (indien dit niet aanwezig is) en de doel-URL.
Uitgever SAML (SP ID)	Voer dezelfde SP ID in die geconfigureerd is voor IdP. Bekijk het SAML2-protocol.
Uitgever voor SAML (IdP ID)	Voer dezelfde ID in die geconfigureerd is voor IdP. Bekijk het SAML2-protocol.
Aanmeldings-URL SSO-service klant	De URL van het assertieverbruik voor SAML2 in IdP.

Veld	Beschrijving
Indeling naam-ID	Selecteer hetzelfde NameID-indeling dat u instelt in IdP. De NameID is de indeling waarin u de gebruikers-id verzendt in de assertie en het verzoek voor enkele afmelding van Cisco WebEx. Raadpleeg het SAML-protocol voor hulp. Wij bevelen aan dat u het e-mailadres instelt als uw NameId. Hierdoor is het gebruik van SSO gemakkelijk voor eindgebruikers die hun account al hebben ingesteld op basis van hun e-mailadres op het systeem. Het gebruik van andere indelingen van naam-ID wordt ondersteund, maar niet aanbevolen. Als u een andere indeling dan een e-mailadres gebruikt, kunnen gebruikers zich niet meer bij een WebEx-site aanmelden als SSO is uitgeschakeld. **Standaard:** Niet gespecificeerd
AuthnContextClassRef	Voer de waarde in die is geconfigureerd in IdP. AuthnContextClassRef is de waarde die verschijnt in het bericht AuthnRequest. **Standaard:** urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
Standaard-URL WebEx-doelpagina	Uw systeem wordt omgeleid naar deze URL wanneer SSO geslaagd is. De standaardpagina is de Cisco WebEx-vergaderingspagina die dezelfde is als een normale aanmeldpagina.
Fout-URL SSO van klant	Uw systeem wordt omgeleid naar deze URL wanneer SSO niet geslaagd is. De foutpagina is standaard een algemene Cisco WebEx-foutpagina.
Enkele afmelding	Met deze optie is enkele afmelding mogelijk zoals bepaald door het SAML2—protocol. Als u de SSO-optie hebt gekozen, maar niet de enkele afmeldingsoptie, wordt de optie afmelden niet weergegeven op de pagina's voor eindgebruikers. Schakel deze optie uit voor ADFS 2.0. **Opmerking** IdP-geïnitieerd SLO wordt niet ondersteund in deze versie.
Afmeldings-URL SSO-service klant **Opmerking** Deze optie wordt alleen weergegeven als Eenmalige afmelding is geselecteerd.	Voer de URL in van het assertieverbruik voor SAML2 in IdP.

Veld	Beschrijving
Automatisch account maken	Gebruikers zonder een Cisco WebEx-account kunnen niet aanmelden. Indien u deze optie selecteert, wordt automatisch een account gemaakt voor nieuwe gebruikers wanneer zij proberen aan te melden.
Automatisch account bijwerken	Als u deze optie selecteert, wordt gebruikersinformatie bijgewerkt wanneer er een "updateTimeStamp" in de SAML2-assertie is met recentere gebruikersinformatie dan de huidige gegevens in Cisco WebEx.
UID-domeinachtervoegsel voor Active Directory UPN verwijderen	Selecteer deze optie om gebruikers te verifiëren zonder domeinachtervoegsel. De optie **UID-domeinachtervoegsel verwijderen voor Active Directory UPN** werkt in de volgende gevallen: • De NameId-indeling is e-mail, en UID-indeling is de X509-onderwerpnaam of User Principal Name (UPN). • De NameId-indeling is de X509-onderwerpnaam of UPN.

Stap 6 Selecteer **SSO inschakelen**.
De pagina **SSO-instellingen bekijken** verschijnt. Controleer uw instellingen en selecteer **Opslaan**.

SSO uitschakelen

Voordat u begint

Door SSO uit te schakelen, kunnen gebruikers niet aanmelden met hun bedrijfsgegevens. Zorg dat uw gebruikers op de hoogte zijn dat u SSO uitschakelt en dat ze nog steeds kunnen aanmelden met hun Cisco WebEx-gegevens.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **Gefedereerde SSO**.

Stap 3 Zoek de zin: "Als u SSO wilt uitschakelen, klik dan hier." Selecteer de koppeling **Klik hier**.

Stap 4 Selecteer **SSO uitschakelen** om te bevestigen.
De pagina **Gefedereerde SSO** verschijnt, met een vendel die bevestigt dat u SSO hebt uitgeschakeld.

Uw Cloud-functies configureren

U kunt uw systeem zo configureren dat uw gebruikers één versie van de Cisco WebEx Productivity Tools kunnen gebruiken, die kan worden gebruikt met hun accounts van zowel de Cisco WebEx Meetings Server als SaaS WebEx of om trainingsvideo's bekijken die online door Cisco WebEx worden gehost.

Opmerking Uw systeem ondersteunt Cisco WebEx SaaS versies WBS27, WBS28 en Cisco WebEx Meetings 1.2.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Instellingen** > **Beveiliging** > **Cloudfuncties**.

Stap 3 (Optioneel) Selecteer het selectievakje **Gebruikers toestaan zich aan te melden in de SaaS WebEx-accounts vanuit WebEx-productiviteitstools**.

Stap 4 Selecteer **Opslaan**.

Beveiliging van de virtuele machine configureren

De beveiligingsfuncties van uw virtuele machine omvatten het vermogen om uw encryptiesleutels bij te werken en FIPS-compatibele encryptie in of uit te schakelen.

Uw encryptiesleutels bijwerken

Cisco WebEx vergaderingsserver gebruikt intern gegenereerde coderingssleutels om alle communicatie tussen virtuele machines op ons systeem te beveiligen. Gebruik deze functie om uw coderingssleutels regelmatig bij te werken.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Virtuele Machines**.

Stap 4 Selecteer **Coderingssleutels bijwerken**.

Stap 5 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

Over FIPS

De Federal Information Processing Standard (FIPS) 140 is een norm van de Amerikaanse en Canadese overheid die beveiligingsvereisten voorschrift voor cryptografische modules. Een cryptografische module is een "reeks hardware, software, en/of firmware waarmee goedgekeurde beveiligingsfuncties (inclusief cryptografische algoritmen en sleutelgenerering) wordt geïmplementeerd en die binnen de cryptografische grens valt." De cryptografische module is datgene wat er gevalideerd word.

Vereisten van FIPS 140

Op een zeer hoog niveau zijn de FIPS 140-vereisten van toepassing op de volgende modulekenmerken:

- Implementatie van door FIPS goedgekeurde algoritmen
- Specifiek beheer van de belangrijkste levenscyclus
- Goedgekeurde generering van willekeurige getallen
- Zelftests van cryptografische algoritmen, beeldintegriteit en willekeurige generators (RNG's)

Cisco WebEx Meetings Server gebruikt CiscoSSL 2.0 om te voldoen aan FIPS 140-2 Niveau 2.

Met FIPS ingeschakeld

Het inschakelen van FIPS kan resulteren in een beperktere compatibiliteit met populaire webbrowsers en besturingssystemen. Enkele symptomen zijn andere problemen met de aanmelding bij het systeem, 404-fouten en het starten en bijwonen van vergaderingen.

Cisco beveelt aan de volgende acties te ondernemen:

- Ervoor zorgen dat uw Windows-pc's minimum op Windows XP SP3 of hoger draaien.
- Alle Windows-computers updaten naar Microsoft Internet Explorer 8 of hoger ongeacht of de gewenste webbrowser van uw gebruikers Internet Explorer, Mozilla Firefox of Google Chrome is. Uw gebruikers moeten over Internet Explorer 8 beschikken op alle computers, daar onze clients met FIPS (Cisco WebEx-vergaderingen, Productiviteitstools en WebEx-opnamespeler) gebruikmaken van systeembibliotheken met FIPS die alleen beschikbaar zijn op Internet Explorer 8 en beter.
- Configureer **Internetinstellingen** op alle gebruikerscomputers op TLS-encryptie. Selecteer op het bureaublad van uw computer Configuratiescherm > Internetopties > Geavanceerd > Beveiliging > TLS 1.0 gebruiken en TLS 1.2 gebruiken. We raden u aan beide opties te selecteren voor maximale compatibiliteit, maar u moet minstens **TLS 1.0 gebruiken** selecteren.
- Als uw gebruikers plannen om vergaderingen te hosten voor gasten (bijvoorbeeld mensen die niet werken voor uw bedrijf) moet u uw gastgebruikers informeren dat ze handmatig hun besturingssysteem en browser moeten bijwerken, zoals hierboven beschreven, voordat ze kunnen deelnemen aan uw Cisco WebEx-vergaderingen. Als ze de bovenstaande stappen niet uitvoeren, kunnen ze compatibiliteitsproblemen ondervinden. Wij adviseren dat u de bovenstaande instructies in uw uitnodigingen voor een vergadering opneemt. U kunt dit doen door de desbetreffende vergaderingsuitnodigingen beschikbaar op uw Beheersite te bewerken in **Instellingen** > **E-mail** > **Sjablonen.**

FIPS-compatibele codering inschakelen

Gebruik deze functie om FIPS-compatibele (Federal Information Processing Standard) encryptie op uw systeem te activeren.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Virtuele Machines**.

Stap 4 Selecteer **Inschakelen** om FIPS-compatibele encryptie te activeren en **Verdergaan** om te bevestigen.
FIPS-compatibele encryptie is geconfigureerd op uw systeem.

Stap 5 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.

FIPS-compatibele codering uitschakelen

Gebruik deze functie om FIPS-compatibele (Federal Information Processing Standard) encryptie op uw systeem te deactiveren.

Procedure

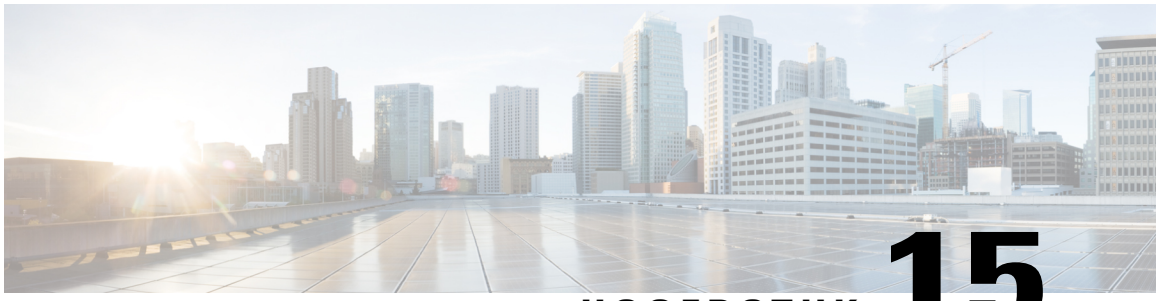
Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Instellingen** > **Beveiliging** > **Virtuele Machines**.

Stap 4 Selecteer **Uitschakelen** om FIPS-compatibele encryptie te deactiveren en **Verdergaan** om te bevestigen.
FIPS-compatibele encryptie is gedeactiveerd op uw systeem.

Stap 5 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.



HOOFDSTUK 15

Uw rapporten beheren

U kunt maandelijkse rapporten weergeven en rapporten aanpassen voor bepaalde datumbereiken. Uw rapporten gebruiken de instellingen voor taal, landinstelling en tijdzone die u op de pagina **Bedrijfsinformatie** hebt geconfigureerd. Zie Uw bedrijfsgegevens configureren, op pagina 188 voor meer informatie.

Opmerking Als uw systeem kort geleden is geïmplementeerd of geüpgrade, zijn er tot het einde van de eerste maand geen gegevens beschikbaar voor de rapporten, met uitzondering van het Aangepaste gegevensrapport. In dat geval zijn de **Download**koppelingen en alle andere rapporten die in dit gedeelte worden beschreven niet beschikbaar tot na het einde van de eerste maand.

- Maandelijkse rapporten downloaden, pagina 243
- Over maandelijkse rapporten, pagina 244
- Aangepaste gegevensrapporten genereren, pagina 246
- Informatie over aangepaste gegevensrapporten, pagina 246

Maandelijkse rapporten downloaden

U kunt de maandelijkse samenvattingsrapporten downloaden vanaf deze pagina. Rapporten worden weergegeven in PDF-indeling.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Rapporten**.

Stap 3 Selecteer de koppeling **Downloaden** voor het maandelijks rapport dat u wilt bekijken.

Over maandelijkse rapporten

Uw maandelijkse samenvattingsrapport bevat de volgende delen:

Samenvattingsrapport systeem

Uw samenvattingsrapport bevat de volgende rapporten:

- Serviceacceptatie-Dit rapport geeft een grafiek weer met het aantal unieke hosts en aanwezigen gedurende de vorige drie maanden en de verwachte groeisnelheid voor de volgende drie maanden.
- Gebruikerslicenties-Dit rapport geeft het percentage aangekochte licenties weer die u gebruikt en een grafiek met het aantal gebruikte licenties gedurende de vorige drie maanden en de verwachte groeisnelheid voor de volgende drie maanden. U kunt deze cijfers gebruiken om toekomstig licentiegebruik te voorspellen en uw licentieaankopen hierop te baseren. Zie Licenties uitvoeren met License Manager, op pagina 183 voor meer informatie.
- Systeemgrootte-Dit rapport geeft de piek in vergaderingsdeelnemers weer en het percentage systeemgrootte dat het piekgebruik heeft verbruikt. De grafiek toont de pieken in het aantal deelnemers aan vergaderingen tijdens de afgelopen drie maanden en de verwachte groeisnelheid voor de volgende drie maanden.
- Opslag-Dit rapport geeft het opslaggebruik weer van uw gegevensarchief en opnamen zowel als percentage van totale opslagruimte als totaal aantal gigabyte (GB). De grafiek toont de totale opslag van de afgelopen drie maanden en de verwachte groeisnelheid voor de volgende drie maanden. Gebruik dit rapport om uw opslaggebruik te bewaken. Als u aanvullende opslagruimte moet toevoegen, moet u uw bestaande opslaggegevensarchief en opnames handmatig naar uw nieuwe opslagserver kopiëren voordat u deze activeert.

  Opmerking Dit rapport wordt alleen weergegeven als u een opslagserver hebt geconfigureerd. Zie Een opslagserver configureren, op pagina 164 voor meer informatie.

- Netwerk-Dit rapport geeft het volgende weer:
  - Uw maximaal gebruik van netwerkbandbreedte in Mbps.
  - Een grafiek die het maximaal gebruik van netwerkbandbreedte in Mbps gedurende de afgelopen drie maanden weergeeft, en de verwachte groeisnelheid gedurende de volgende drie maanden (de rode balk geeft de maximale netwerkbandbreedte weer).
  - Een cirkeldiagram dat het percentage bandbreedte weergeeft dat door elk van uw systeembronnen wordt gebruikt.
- Geplande uitvaltijd systeem en ongeplande uitvaltijd-Dit rapport geeft het volgende weer:
  - Uw gemiddelde uptime van het systeem gedurende de afgelopen drie maanden.
  - De gemiddelde duur van uw ongeplande uitvaltijd van het systeem gedurende de afgelopen drie maanden.
  - Het gemiddeld aantal afgebroken vergaderingen door storingen gedurende de afgelopen drie maanden.

- De grafiek geeft de geplande uitvaltijd en de niet-geplande uitvaltijd weer gedurende de afgelopen drie maanden en de verwachte groeisnelheid voor de volgende drie maanden.

Opmerking Verhoogde uitvaltijd betekent soms dat het verbruik is verhoogd. Zorg ervoor dat u de statistieken van uw uitvaltijd vergelijkt met de statistieken van uw gebruik die in andere rapporten worden weergegeven.

Samenvattingsrapport vergadering

Uw samenvattingsrapport van vergaderingen bevat de volgende rapporten:

- Vergaderstatus-Dit rapport geeft een grafiek weer waarin de vergaderstatus van de afgelopen maand staat, het percentage vergaderingen dat problemen heeft ondervonden en het totaal aantal vergaderingen tijdens die maand. Raadpleeg uw dashboard voor realtime vergaderstatussen. Zie Informatie over uw dashboard, op pagina 115 voor meer informatie.
- Vergadergrootte-Dit rapport geeft een grafiek weer met daarin de grootte van de vergaderingen op uw systeem gedurende de afgelopen maand, een overzicht van de vergadergroottes en gedetailleerde informatie over de grootste vergadering die tijdens de maand werd gehouden.
- Gebruik vergaderfunctie-Dit rapport geeft het volgende weer:
  - De meest gebruikte functie gedurende de vorige maand, waaronder het totaal aantal minuten dat de functie is gebruikt.
  - De snelst groeiende functie op uw systeem tijdens de afgelopen maand, waaronder de groeisnelheid.
  - Een grafiek die verbruik in minuten aangeeft voor elke functie op uw systeem.
  - Een grafiek die de groeisnelheid van de snelst groeiende functie op uw systeem aangeeft.
- Meest actieve e-maildomeinen van de deelnemers-Dit rapport geeft het volgende weer:
  - Een grafiek met de meest actieve e-maildomeinen van de deelnemers.
  - Een overzicht van de e-maildomeinen van de deelnemers.
  - Een lijst met de drie vaakst gebruikte e-maildomeinen door deelnemers aan vergaderingen op uw systeem.
- Piekdag en -uur-Dit rapport geeft twee grafieken weer. De eerste grafiek geeft de drukste dag van de week weer tijdens de afgelopen maand. De tweede grafiek geeft het drukste tijdstip van de dag weer tijdens de afgelopen maand.

Aangepaste gegevensrapporten genereren

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Rapporten** > **Uw rapport aanpassen**.

Stap 3 Selecteer het datumbereik van de rapporten die u wilt weergeven en selecteer **Verzenden**.
De standaardwaarde is de meest recente maand. U kunt een datumbereik selecteren die tot zes maanden terug reikt.

De pagina **Aanvraag aangepast rapport ingediend** wordt weergegeven en toont de datums van uw aangepaste rapport. Er wordt een e-mail naar u verzonden met een koppeling naar uw aangepaste rapport in CSV-indeling.

Stap 4 Selecteer **Klaar**.

Informatie over aangepaste gegevensrapporten

Wanneer u aangepaste gegevensrapporten genereert, ontvangt u een e-mail met een archief dat de volgende rapporten in CSV-formaat bevat:

- Fraudepogingenrapport - Dit rapport bevat alle mislukte telefonietoegangspogingen waarbij de beller drie keer een verkeerde host- of deelnemertoegangscode of hostpincode invoert tijdens een poging om een Persoonlijke Conferentie-vergadering te starten of bij te wonen. Dit rapport bevat de volgende velden:
  - Gebeld toegangsnummer - Het inbelnummer van Cisco WebEx dat is gebeld om een Persoonlijke conferentie-vergadering te starten of bij te wonen.
  - Bellend nummer - Het telefoonnummer van de telefoon waarmee is gebeld.
  - Begintijd van de oproep - De datum en tijd van de oproep.
  - Toegangscode eerste poging - De eerste ongeldige toegangscode die de beller heeft ingevoerd.
  - E-mail van eerste toegang van code-eigenaar (indien beschikbaar) - Het e-mailadres van de gebruiker die de eerste ongeldige code heeft ingevoerd als de toegangscode is gekoppeld aan een geldig Cisco WebEx Meetings Server-account.
  - Toegangscode tweede poging - De tweede ongeldige toegangscode die de beller heeft ingevoerd.
  - E-mail van tweede toegang van code-eigenaar (indien beschikbaar) - Het e-mailadres van de gebruiker die de tweede ongeldige code heeft ingevoerd als de toegangscode is gekoppeld aan een geldig Cisco WebEx Meetings Server-account.
  - Toegangscode derde poging - De derde ongeldige toegangscode die de beller heeft ingevoerd.
  - E-mail van derde toegang van code-eigenaar (indien beschikbaar) - Het e-mailadres van de gebruiker die de derde ongeldige code heeft ingevoerd als de toegangscode is gekoppeld aan een geldig Cisco WebEx Meetings Server-account.

- Vergaderingsrapport-Dit rapport bevat informatie over alle vergaderingen die plaatsvonden tijdens de opgegeven periode en bevat de volgende velden:
    - VergaderingID-De unieke vergadering-id door uw systeem gegenereerd toen de vergadering is gepland.
    - Vergadernummer-Het Cisco WebEx-vergadernummer.
    - Onderwerp-De naam van de vergadering die de host heeft geconfigureerd.
    - Hostnaam-De host van de vergadering.
    - Begintijd—De begintijd en –datum van de vergadering.
    - Duur-De duur van de vergadering in minuten.
    - Aantal deelnemers - Het aantal deelnemers inclusief de host.
    - Status
    - Aantal audiominuten voor Inbellen
    - Aantal audiominuten voor Terugbellen
    - Aantal VoIP-minuten
    - Aantal videominuten
    - Aantal opnameminuten
    - Opname-interval-Geeft de begin- en eindtijd weer van elke opname die tijdens de vergadering is gemaakt.
    - Aantal WebSharing-minuten - Het totale aantal minuten dat alle deelnemers in de webvergadering doorbrengen (als bijvoorbeeld drie deelnemers een webvergadering van 10 minuten bijwonen, is het aantal WebSharing-minuten 30).
    - Deelnemers-Een lijst van de deelnemers aan de vergadering.
    - Hostplatform/-browser-De versie van het besturingssysteem en de browser die de host gebruikte toen hij of zij een Cisco WebEx-vergadering startte.
    - IP-adres host-Het IP-adres dat door de host werd gebruikt toen hij of zij een Cisco WebEx-vergadering startte.
    - Traceercodes-De traceercodes door de host toegepast bij het plannen van de vergadering.
- Gebruiksrapport netwerkbandbreedte-Dit rapport bevat een lijst van het gebruik van netwerkbandbreedte voor elke dag in de opgegeven periode voor elk van de volgende functies:
    - Maximaal bandbreedtegebruik voor audio (mbps)
    - Maximaal bandbreedtegebruik voor audio VoIP(mbps)
    - Maximaal bandbreedtegebruik voor video (mbps)
    - Maximaal bandbreedtegebruik voor zoeken op het web (mbps)

  Een verbruik van 0 (nul) geeft aan dat de functie op die datum niet is gebruikt. Een verbruik van minder dan 1 wordt weergegeven indien minder dan 1 Mbps is verbruikt op die bepaalde datum.

Het gebruik van netwerkbandbreedte voor video is inclusief video van camera's en het delen van videobestanden tijdens webvergaderingen. Wanneer video uitgeschakeld is voor uw site, kunt u geen camera inschakelen voor video, maar kunt u nog steeds videobestanden delen. Dit zorgt voor gebruik van netwerkbandbreedte voor video, wat inbegrepen is in rapporten. Dit is de enige situatie die zorgt voor gebruik van netwerkbandbreedte voor video wanneer video is uitgeschakeld voor een site.

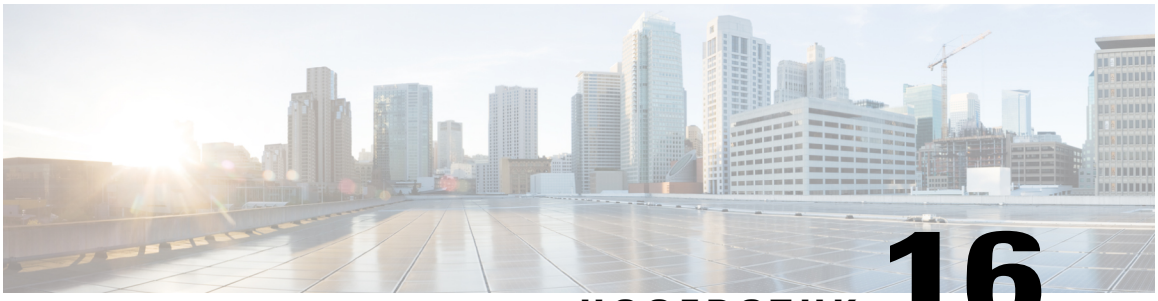
- Gebruiksrapport opslagcapaciteit-Dit rapport geeft de totale gebruikte schijfruimte weer op de weergegeven datum en het aantal opgenomen vergaderingen die op elke datum hebben plaatsgevonden.

Opmerking Dit rapport wordt alleen weergegeven als u een opslagserver hebt geconfigureerd. Zie Een opslagserver configureren voor meer informatie.

- Deelnemersrapport-In dit rapport wordt de geschiedenis van vergaderingen weergegeven, evenals de begintijd van elke vergadering en de traceercode die op elke vergadering is toegepast.
  - Vergaderings-id: de unieke conferentie-id die tijdens het plannen van de vergadering door uw systeem is gegenereerd.
  - Conferentienaam-De naam van de vergadering, die de host tijdens het plannen van de vergadering heeft ingevoerd in het veld **Wat**.
  - Gebruikersnaam-De gebruikersnaam van de host.
  - Tijd van deelnemen-De datum en tijd waarop een gebruiker aan een Cisco WebEx-vergadering heeft deelgenomen.
  - Tijd van verlaten-De datum en tijd waarop een gebruiker een Cisco WebEx-vergadering heeft verlaten.
  - Duur: het aantal minuten dat een gebruiker aan een Cisco WebEx-vergadering heeft deelgenomen.
  - Platform/browser-De versie van het besturingssysteem en de browser die de host gebruikte toen hij of zij een Cisco WebEx-vergadering startte.
  - Client IP-adres-Het IP-adres van de WebEx-client die door een host of deelnemer wordt gebruikt om een Cisco WebEx-vergadering te starten of aan een Cisco WebEx-vergadering deel te nemen.
  - Starttijd van sessie-Het tijdstip waarop de sessie is gestart.
  - Eindtijd sessie-Het tijdstip waarop de sessie is beëindigd.
  - Type sessie-Het sessietype kan video (het delen van de webbrowser), VoIP (een telefonische verbinding), inbellen of terugbellen zijn.
  - Duur sessie-De tijdsduur van de sessie.
  - Telefoonnummer: het telefoonnummer van de telefoon waarmee in de WebEx-vergadering is ingebeld.
  - Tel. Server-De telefoonserver.
- Rapport uitvaltijd systeem-Dit rapport bevat informatie over de uitvaltijd van het systeem voor de opgegeven periode en bevat de volgende velden:
  - Categorie-Buiten gebruik of Onderhoud. Buiten gebruik wijst op een storing. Onderhoud wijst op een geplande onderhoudsperiode.

- Service-Geeft de betrokken functies weer.
- Begin van uitvaltijd-Datum en tijdstip waarop de uitvaltijd is begonnen.
- Einde van uitvaltijd-Datum en tijdstip waarop de uitvaltijd is geëindigd.
- Aantal afgebroken vergaderingen-Geeft het aantal afgebroken vergaderingen weer. Dit veld is leeg voor uitvaltijd door onderhoud, aangezien dit wordt gepland. Indien er geen vergaderingen zijn gepland tijdens een uitvaltijd Buiten gebruik, is het nummer 0.

- Gebruiksrapport gebruikerslicenties: Er zijn twee versies beschikbaar van dit rapport. De ene versie geeft het licentiegebruik weer van de afgelopen 30 dagen en heet UserLicenseUtilizationReportForLastMonth.csv; de andere versie geeft het licentiegebruik weer van de huidige maand (vanaf de eerste dag van de maand tot en met de huidige dag) en heet UserLicenseUtilizationForThisMonth.csv. In beide rapporten zijn de volgende velden opgenomen:
  - Gebruikersnaam-De gebruikersnaam van de host van de vergadering.
  - E-mailadres-E-mailadres van de vergaderhost.
  - VergaderingID-De unieke vergadering-id door uw systeem gegenereerd toen de vergadering is gepland.
  - Vergadernummer-Het Cisco WebEx-vergadernummer.
  - Begintijd-Datum en tijdstip waarop de vergadering is begonnen.
  - Gelijktijdige vergadering-Geeft het aantal gelijktijdige vergaderingen aan, gepland door dezelfde gebruiker. Elke gelijktijdige vergadering die wordt opgenomen, zorgt voor een bijkomende regel die aan dit rapport wordt toegevoegd voor de gebruiker die de gelijktijdige vergadering heeft gepland.



HOOFDSTUK 16

De ondersteuningsfuncties gebruiken

- Uw logboek aanpassen, pagina 251
- Een account voor Remote Support instellen, pagina 253
- Een account voor Remote Support uitschakelen, pagina 253
- De vergaderingstest gebruiken, pagina 254
- De systeembrontest gebruiken, pagina 254

Uw logboek aanpassen

U kunt logbestanden maken die activiteit weergeven op uw volledig systeem of voor specifieke vergaderingen. Gebruik de logbestanden om problemen op te lossen of indien nodig hulp te vragen bij het Cisco Technical Assistance Center (TAC) wanneer u hulp nodig hebt

Opmerking We adviseren u uw logbestand buiten de kantooruren te genereren. Het grote formaat van het logbestand kan de prestaties van uw systeem beïnvloeden.

Opmerking Logboekgegevens worden 30 dagen bewaard. Als u echter een Cisco WebEx Meetings Server 1.x-implementatie upgradet naar versie 2.0, worden de logboekgegevens van versie 1.x niet overgebracht naar het Cisco WebEx Meetings Server 2.0-systeem. Deze gegevens zijn daarom niet meer beschikbaar na voltooiing van de upgrade naar versie 2.0.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Ondersteuning** > **Logs**.

Stap 3 Vul de velden in op de pagina **Uw logbestand aanpassen** en selecteer **Verzenden**.

Veld	Beschrijving
(Optioneel) Klasse-ID	Voer uw Cisco TAC klasse-ID in. Klasse-ID's worden vanuit het Cisco TAC toegekend wanneer zij u helpen met een probleem. Met deze functie kunt u de logbestanden koppelen die u met het klasse-ID genereert.
Type	Selecteer het type logbestand. U kunt **Logboek algemeen systeem** of **Logboek specifieke vergadering** selecteren. Een logbestand algemeen systeem bevat alle gespecificeerde loginformatie voor uw systeem en logbestand specifieke vergadering verzamelt logbestanden en gegevens van de database voor MATS-verwerking. **Standaard:** Logboek algemeen systeem
Bereik	Selecteer het bereik voor uw logbestand. U moet een begin- en einddatum en -tijd opgeven voor uw logbestand. De limiet is 24 uur. Loggegevens zijn alleen beschikbaar voor de laatste 30 dagen. **Opmerking** Om langer dan 24 uur logbestanden te maken, moet u deze bewerking herhalen en een opeenvolgend datum- en tijdbereik selecteren. Elke bewerking leidt tot het maken van een afzonderlijk logbestand. Bijvoorbeeld: Om logbestanden te maken van 1 januari tot 3 januari, selecteert u eerst een datumbereik van 1 januari tot 2 januari, selecteert u **Verzenden** en downloadt u het gemaakte logbestand. Selecteer vervolgens een datumbereik van 2 januari tot 3 januari. Selecteer **Verzenden** en download het gemaakte logbestand.
Opnemen	Geef de gegevens op die u wilt opnemen in uw log. **Standaard:** Alle activiteiten

Uw logbestand is gegenereerd en u ontvangt een e-mail met een koppeling om het logbestand te downloaden.

Een account voor Remote Support instellen

Als u technische problemen hebt en contact opneemt met de Cisco TAC voor assistentie, kunt u een remote support account opzetten om een TAC-vertegenwoordiger tijdelijk toegang tot uw systeem te geven. Dit product biedt geen CLI-toegang tot beheerders, waardoor een TAC-vertegenwoordiger nodig is om bepaalde problemen te kunnen oplossen.

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Ondersteuning** > **Remote Support-account**.

Stap 3 Selecteer **Remote Support inschakelen**.

Stap 4 Vul de velden in op de pagina **Account voor Remote Support** en selecteer **Account maken**.

Veld	Beschrijving
Naam account voor Remote Support	Voer een naam in voor uw remote support-account (6-30 tekens).
Levensduur account	Geef de tijdsduur van het account op in uren. Het maximum is 720 uur (30 dagen).
Decoderversie	Selecteer **2- Webex Meetings Server**. **Opmerking** Als u een Remote Support-account hebt dat actief was voor de release van Cisco WebEx Meetings Server versie 1.5, hoeft u deze instelling niet te configureren.

Het dialoogvenster **Account maken voor Remote Support** wordt weergegeven, met daarin uw wachtwoordzin. Neem contact op met de technische ondersteuning van Cisco en geef de medewerker daarvan de naam van het account voor Remote Support en de wachtwoordzin, zodat hij of zij toegang heeft tot uw systeem.

Een account voor Remote Support uitschakelen

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Ondersteuning** > **Remote Support-account**.

Stap 3 Naast het statusbericht, "Remote Support is ingeschakeld", selecteert u de koppeling **Uitschakelen**. Uw remote support account is gedeactiveerd.

De vergaderingstest gebruiken

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Ondersteuning** > **Vergaderingstest**.

Stap 3 Selecteer **Volgende**.
Uw systeem voert een vergaderingstest uit en controleert de mogelijkheden om een vergadering te plannen, te starten en bij te wonen. De resultaten van de test verschijnen over enkele minuten.

De systeembrontest gebruiken

Procedure

Stap 1 Meld u aan bij de Beheersite.

Stap 2 Selecteer **Onderhoudsmodus inschakelen** en **Doorgaan** om te bevestigen.

Stap 3 Selecteer **Ondersteuning** > **Systeembronnentest**.

Stap 4 Selecteer **Volgende**.
De resultaten van de test zijn opgenomen voor de volgende:

- CPU, geheugen, netwerk en opslag voor elke host op uw systeem
- Interne en externe verbindingscontroles voor de URL's van uw site en beheer

Stap 5 Selecteer **Onderhoudsmodus uitschakelen** en **Doorgaan** om te bevestigen.
Uw systeem start opnieuw op nadat u de onderhoudsmodus uitgeschakeld hebt. U kunt u terug aanmelden op de Beheersite nadat het opstarten voltooid is.