GCCSI

Ihr Dienstleister in:

Gürbüz Computer Consulting & Service International 1984-2007 l Önder Gürbüz l Aar Strasse 70 l 65232 Taunusstein
info@gccsi.com l +49 (6128) 757583 l +49 (6128) 757584 l +49 (171) 4213566

Handbuch für die Microsoft Lync Server 2010-Edgebereitstellung

Microsoft Lync Server 2010

Veröffentlichung: Juli 2011

Inhalt

Bereitstellen von Edgeservern 5
Übersicht über die Edgebereitstellung 5
Bereitstellungsprozess für den Zugriff durch externe Benutzer 6
Tools für die Edgebereitstellung 12
Bewährte Methoden für die Bereitstellung des Zugriffs durch externe Benutzer 12
Vorbereiten der Installation von Servern im Umkreisnetzwerk 13
Systemanforderungen für Edgekomponenten 14
Hardware- und Softwareanforderungen für Edgekomponenten 14
Unterstützte gemeinsame Serverausführung für Edgekomponenten 16
Konfigurieren von DNS für die Edgeunterstützung 16
Konfigurieren von DNS-Einträgen für die Edgeunterstützung 16
Konfigurieren des DNS-Suffixes für Edgeserver 18
Einrichten von Hardwaregeräten zum Lastenausgleich für eine skalierte Edgetopologie . 19
Konfigurieren von Firewalls und Ports für den externen Benutzerzugriff 19
Ermitteln der Anforderungen für A/V-Firewall und Ports 19
Anfordern von Edgezertifikaten 24
Anfordern von Zertifikaten von einer öffentlichen Zertifizierungsstelle 24
Anfordern von Zertifikaten von einer internen Unternehmenszertifizierungsstelle 25
Vorbereiten der Unterstützung von Verbindungen mit öffentlichen Instant Messaging-Diensten 25
Aufbau einer Edge- und Director-Topologie 26
Definieren des Directors 27
Definieren eines einzelnen Directors im Topologie-Generator 28
Definieren eines Pools mit mehreren Directors im Topologie-Generator 29
Definieren der Edgetopologie 31
Definieren der Topologie für einen einzelnen Edgeserver 31
Definieren der Topologie für einen Edgeserverpool mit DNS-Lastenausgleich 35
Definieren der Topologie für einen Edgeserverpool mit Hardwarelastenausgleich 40
Veröffentlichen der Topologie 44
Einrichten des Directors 45
Installieren des lokalen Konfigurationsspeichers 45
Installieren von Lync Server 2010 auf dem Director 47
Konfigurieren von Zertifikaten für den Director 47
Starten von Diensten auf dem Director 49
Testen des Directors 49
Konfigurieren der automatischen Clientanmeldung zur Verwendung des Directors 50
Einrichten von Edgeservern 51
Einrichten von Netzwerkschnittstellen für Edgeserver 51

Installieren der erforderlichen Software auf Edgeservern 53
Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation 53
Installieren von Edgeservern 54
Einrichten von Edgezertifikaten 56
Zertifikatanforderungen für den externen Benutzerzugriff 56
Einrichten der Zertifikate für die interne Edgeschnittstelle 59
Einrichten der Zertifikate für die externe Edgeschnittstelle 66
Einrichten der Zertifikate für den Reverseproxy 73
Starten der Edgeserver 74
Einrichten von Reverseproxyservern 74
Konfigurieren von Webfarm-FQDNs 76
Konfigurieren von Netzwerkadaptern 77
Anfordern und Konfigurieren eines Zertifikats für den HTTP-Reverseproxy 78
Konfigurieren von Webveröffentlichungsregeln für einen einzelnen internen Pool 79
Überprüfen oder Konfigurieren der Authentifizierung und Zertifizierung für virtuelle IIS-Verzeichnisse 83
Erstellen von DNS-Einträgen für Reverseproxyserver 83
Überprüfen des Zugriffs über den Reverseproxy 84
Konfigurieren der Unterstützung für den externen Benutzerzugriff 84
Aktivieren oder Deaktivieren des externen Benutzerzugriffs für Ihre Organisation 87
Aktivieren oder Deaktivieren des Zugriffs durch Remotebenutzer für Ihre Organisation 88
Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation 89
Aktivieren oder Deaktivieren des Zugriffs anonymer Benutzer für Ihre Organisation 92
Konfigurieren der Kommunikation mit externen Benutzern 93
Verwalten des Remotebenutzerzugriffs 95
Verwalten des Zugriffs durch Verbundpartnerbenutzer 97
Konfigurieren von Richtlinien zur Steuerung des Partnerbenutzerzugriffs 98
Steuern des Zugriffs durch einzelne Partnerdomänen 100
Verwalten der Unterstützung für Sofortnachrichtenanbieter 103
Konfigurieren von Richtlinien zur Steuerung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern 103
Angeben der unterstützten Sofortnachrichten-Dienstanbieter 105
Konfigurieren von Konferenzrichtlinien zur Unterstützung anonymer Benutzer 110
Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer 111
Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer 111
Anwenden von Konferenzrichtlinien zur Unterstützung anonymer Benutzer 113
Überprüfen der Edgebereitstellung 114
Überprüfen der Konnektivität zwischen internen Servern und Edgeservern 114
Überprüfen der Konnektivität für externe Benutzer 115

Bereitstellen von Edgeservern

Die Bereitstellung von Edgekomponenten für Microsoft Lync Server 2010 ermöglicht es externen Benutzern, die nicht beim internen Netzwerk Ihrer Organisation angemeldet sind, über Lync Server mit anderen Benutzern in Ihrer Organisation zu kommunizieren. Zu externen Benutzern gehören authentifizierte und anonyme Remotebenutzer, Verbundpartner sowie Benutzer von öffentlichen Instant Messaging-Diensten. Die Bereitstellungs- und Konfigurationsprozesse für Lync Server 2010 unterscheiden sich wesentlich von den Prozessen in vorherigen Versionen, da Lync Server 2010 neue Tools für die Installation und Verwaltung bereitstellt, welche die Arbeitsweise mit Lync Server-Komponenten verändern. Die Abschnitte im Thema Übersicht über die Edgebereitstellung erläutern den Bereitstellungsprozess, die neuen Tools und die Verwendung dieser Tools zur Bereitstellung von Edgekomponenten für den Zugriff durch externe Benutzer.

Bevor Sie beginnen, schauen Sie sich das kurze Video unter http://go.microsoft.com/fwlink/?LinkId=205566&clcid=0x407 an, um einen Überblick über die Verwendung des Topologie-Generators zum Hinzufügen eines Edgeservers zu einer vorhandenen Lync Server 2010-Bereitstellung zu erhalten.

Inhalt dieses Abschnitts

- Übersicht über die Edgebereitstellung
- Vorbereiten der Installation von Servern im Umkreisnetzwerk
- Aufbau einer Edge- und Director-Topologie
- Einrichten des Directors
- Einrichten von Edgeservern
- Konfigurieren der Unterstützung für den externen Benutzerzugriff
- Überprüfen der Edgebereitstellung

Übersicht über die Edgebereitstellung

Um Unterstützung für den Zugriff durch externe Benutzer, den Partnerverbund und die Integration in Verbindungen mit öffentlichen Instant Messaging-Diensten zu bieten, müssen Sie nicht nur die Netzwerk- und Firewallinfrastruktur für die Unterstützung dieser Komponenten vorbereiten, sondern zusätzlich Edgeserver und andere Komponenten im Umkreisnetzwerk bereitstellen.
Die Bereitstellungsschritte umfassen die Verwendung der in Microsoft Lync Server 2010 verfügbaren Tools, um mit der Bereitstellung von Edgeservern zu beginnen. Dieser Abschnitt

enthält eine Übersicht über die Schritte zur Bereitstellung von Edgeservern, die Tools zur Bereitstellung von Edgeservern und bewährte Methoden für die Bereitstellung von Komponenten zur Unterstützung des Zugriffs durch externe Benutzer.

Inhalt dieses Abschnitts

- Bereitstellungsprozess für den Zugriff durch externe Benutzer
- Tools für die Edgebereitstellung
- Bewährte Methoden für die Bereitstellung des Zugriffs durch externe Benutzer

Bereitstellungsprozess für den Zugriff durch externe Benutzer

Für eine effektive Planung des Zugriffs durch externe Benutzer muss Folgendes beachtet werden:

- Voraussetzungen für die Bereitstellung einer Edgetopologie
- Erforderliche Schritte für die Bereitstellung der Edgeserver und verknüpfter Komponenten

Bereitstellungsvoraussetzungen für den Zugriff durch externe Benutzer

Bevor Sie Ihr Umkreisnetzwerk bereitstellen und die Unterstützung für externe Benutzer implementieren, müssen Sie bereits Ihre internen Server mit Microsoft Lync Server 2010 bereitgestellt haben, einschließlich eines Front-End-Pools oder eines Standard Edition-Servers. Wenn Sie die Bereitstellung von Director-Servern in Ihrem internen Netzwerk planen, sollten Sie diese ebenfalls vor den Edgeservern bereitstellen. Ausführliche Informationen zum Director-Bereitstellungsprozess finden Sie unter „Director“ in der Planungsdokumentation.

Bereitstellungsprozess für Edgeserver

Die folgende Tabelle zeigt eine Übersicht über den Bereitstellungsprozess für Edgeserver. Ausführliche Informationen zu den erforderlichen Schritten für die Bereitstellung finden Sie unter Bereitstellen von Edgeservern.

Hinweis:
Die Informationen in der folgenden Tabelle gelten für eine neue Bereitstellung. Wenn Sie Edgeserver in einer Office Communications Server 2007 R2- oder Office Communications Server 2007-Umgebung bereitgestellt haben, finden Sie unter „Migration“ ausführliche Informationen über die Migration zu Lync Server 2010. Für Versionen vor Office Communications Server 2007, Live Communications Server 2005 und Live Communications Server 2003 eingeschlossen, wird eine Migration nicht unterstützt.

Bereitstellungsprozess für Edgeserver

Phase	Schritte	Berechtigungen	Dokumentation
Erstellen Sie die geeignete Edgetopologie, und ermitteln Sie die geeigneten Komponenten.	• Führen Sie den Topologie-Generator aus, um Einstellungen für Edgeserver zu konfigurieren und die Topologie zu erstellen und zu veröffentlichen. Verwenden Sie dann die Lync Server-Verwaltungsshell zum Exportieren der Topologiekonfigurationsdatei.	Gruppe **Domänen-Admins** und Gruppe **RTCUniversalServerAdmins** **Hinweis:** Sie können eine Topologie unter Verwendung eines Kontos definieren, das Mitglied der lokalen Benutzergruppe ist. Für die Veröffentlichung einer Topologie ist jedoch ein Konto erforderlich, das Mitglied der Gruppe **Domänen-Admins** und der Gruppe **RTCUniversalServer Admins** ist.	Definieren der Edgetopologie
Bereiten Sie das Setup vor.	1. Stellen Sie sicher, dass die Systemvoraussetzungen erfüllt sind. 2. Konfigurieren Sie IP-Adressen für die internen und die öffentlichen Netzwerkschnittstellen auf jedem Edgeserver. 3. Konfigurieren Sie interne und externe DNS-Einträge,	Je nach Organisationsanforderungen	Vorbereiten der Installation von Servern im Umkreisnetzwerk

Phase	Schritte	Berechtigungen	Dokumentation
	einschließlich Konfiguration des DNS-Suffixes auf dem Computer, der als Edgeserver bereitgestellt werden soll. 4. Konfigurieren Sie die Firewalls. 5. (Optional) Erstellen und installieren Sie öffentliche Zertifikate. Die zum Anfordern von Zertifikaten erforderliche Zeit richtet sich nach der Zertifizierungsstelle (Certification Authority, CA), die das Zertifikat ausgibt. Wenn Sie diesen Schritt jetzt überspringen, müssen Sie ihn während der Installation der Edgeserver ausführen. Der Edgeserverdienst kann erst gestartet werden, wenn Zertifikate angefordert wurden. 6. Konfigurieren Sie die Unterstützung zur Verbindung mit öffentlichen Instant Messaging-Diensten,		

Phase	Schritte	Berechtigungen	Dokumentation
	wenn Ihre Bereitstellung eine Kommunikation mit Benutzern von Windows Live, AOL oder Yahoo! unterstützen soll.		
Richten Sie den Reverseproxy ein.	• Richten Sie den Reverseproxy (z. B. für Microsoft Forefront Threat Management Gateway 2010 oder Microsoft Internet Security and Acceleration (ISA) Server mit Service Pack 1) im Umkreisnetzwerk ein, fordern Sie die benötigten öffentlichen Zertifikate an, und konfigurieren Sie die Webveröffentlichungsregeln auf dem Reverseproxyserver.	Gruppe **Administratoren**	Einrichten von Reverseproxyservern
Richten Sie einen Director ein (empfohlen).	• (Optional) Installieren und konfigurieren Sie einen oder mehrere Director-Server im internen Netzwerk.	Gruppe **Administratoren**	Einrichten des Directors

Phase	Schritte	Berechtigungen	Dokumentation
Richten Sie die Edgeserver ein.	1. Installieren Sie die erforderliche Software. 2. Übertragen Sie die exportierte Topologiekonfiguratio nsdatei auf jeden Edgeserver. 3. Installieren Sie die Lync Server 2010-Software auf jedem Edgeserver. 4. Konfigurieren Sie die Edgeserver. 5. Fordern Sie Zertifikate für alle Edgeserver an, und installieren Sie sie. 6. Starten Sie die Edgeserverdienste.	Gruppe **Administratoren**	Einrichten von Edgeservern
Konfigurieren Sie die Unterstützung für den Zugriff durch externe Benutzer.	1. Verwenden Sie die Lync Server 2010-Systemsteuerung, um die Unterstützung folgender Funktionen zu konfigurieren (sofern gewünscht): • Remotebenutzerzu griff • Partnerverbund • Verbindung mit öffentlichen Instant Messaging-Diensten	Gruppe **RTCUniversalServerAdmins** oder Benutzerkonto mit zugewiesener Rolle **CSAdministrator**	Konfigurieren der Unterstützung für den externen Benutzerzugriff

Phase	Schritte	Berechtigungen	Dokumentation
	• Anonyme Benutzer 2. Konfigurieren Sie Benutzerkonten für Remotebenutzerzugriff, Partnerverbund, die Verbindung mit öffentlichen Instant Messaging-Diensten und die Unterstützung anonymer Benutzer (sofern gewünscht).		
Überprüfen Sie Ihre Edgeserverkonfiguration.	1. Überprüfen Sie die Serverkonnektivität, und stellen Sie sicher, dass die Replikation der Konfigurationsdaten interner Server ordnungsgemäß funktioniert. 2. Stellen Sie sicher, dass externe Benutzer eine Verbindung herstellen können – Remotebenutzer, Benutzer in Partnerdomänen, Benutzer öffentlicher Instant Messaging-Dienste und anonyme Benutzer eingeschlossen (je nach Anforderungen für Ihre Bereitstellung).	Zum Überprüfen der Replikation: Gruppe **RTCUniversalServerAdmins** oder Benutzerkonto mit zugewiesener Rolle **CSAdministrator** Zum Überprüfen der Benutzerkonnektivität: Ein Benutzer für jede Art von externem Zugriff, der unterstützt wird Remotebenutzer	Überprüfen der Edgebereitstellung

Tools für die Edgebereitstellung

Microsoft Lync Server 2010 umfasst zwei Tools für eine vereinfachte Planung und Bereitstellung von internen Servern und Edgeservern. Es wird empfohlen, diese Tools zum Planen des Entwurfs zunächst auf einer lokalen Arbeitsstation auszuführen. Nach Abschluss der Topologie laden Sie die resultierende Topologiedefinition in Ihre Produktionsumgebung hoch. Um diese Aufgabe ausführen zu können, müssen Sie Mitglied der Gruppe **Domänen-Admins** und der Gruppe **RTCUniversalServerAdmins** sein.

- **Planungstool** Office Communications Server 2007 R2 enthält ein Planungstool und ein Edgeplanungstool, das die Erstellung des Topologieentwurfs vereinfachen kann. In Lync Server 2010 wurden diese beiden Tools zu einem einzigen Lync Server 2010-Planungstool zusammengefasst, das zusätzliche Funktionen bietet (u. a. die Möglichkeit, ein XML-basiertes Topologiedokument zu erstellen).

- **Topologie-Generator** Der Lync Server 2010-Topologie-Generator unterstützt Sie bei der Definition Ihrer Topologie und Komponenten. Der Topologie-Generator ist für die Bereitstellung von Servern mit Lync Server 2010 äußerst wichtig. Der Topologie-Generator kann die vom Planungstool bereitgestellte XML-Topologiedatei verwenden, um mit dem anfänglichen Entwurf Ihrer Topologie zu beginnen. Oder Sie überspringen die Verwendung des Planungstools und verwenden den Topologie-Generator zum Entwerfen Ihrer Bereitstellung. Der Topologie-Generator veröffentlicht die Ergebnisse in einem zentralen Verwaltungsspeicher, der zur Konfiguration aller Server mit Lync Server 2010 in Ihrer Organisation verwendet wird. Zur Installation von Lync Server 2010 auf Servern muss der Topologie-Generator verwendet werden.

Wenn Sie die Erstellung Ihrer Edgetopologie in der Planungsphase abgeschlossen haben (einschließlich Ausführung des Topologie-Generators zum Definieren der Edgetopologie), können Sie die Ergebnisse verwenden, um mit der Edgeserverbereitstellung zu beginnen. Wenn Sie die Erstellung Ihrer Edgetopologie noch nicht abgeschlossen haben oder die zuvor angegebenen Informationen ändern möchten, müssen Sie die Schritte des Topologie-Generators zunächst abschließen, bevor Sie mit anderen Bereitstellungsschritten fortfahren können. Ausführliche Informationen zum Erstellen Ihrer Topologie finden Sie unter „Topologien für den Zugriff durch externe Benutzer“.

Ausführliche Informationen zum Planungstool und zum Topologie-Generator finden Sie unter „Beginn des Planungsprozesses“ in der Planungsdokumentation.

Bewährte Methoden für die Bereitstellung des Zugriffs durch externe Benutzer

Halten Sie sich bei der Bereitstellung des Umkreisnetzwerks und der Edgeserver an folgende Richtlinien, um sowohl die Leistung und Sicherheit der Edgeserver zu erhöhen als auch die Bereitstellung zu erleichtern:

- Stellen Sie Edgeserver nur bereit, nachdem Sie die Microsoft Lync Server 2010-Kommunikationssoftware innerhalb Ihrer Organisation getestet und deren ordnungsgemäßen Betrieb sichergestellt haben.
- Es wird empfohlen, den Edgeserver nicht in einer Domäne, sondern in einer Arbeitsgruppe bereitzustellen. Dies vereinfacht die Installation und vermeidet eine Verbindung zwischen Active Directory-Domänendiensten (AD DS) und dem Umkreisnetzwerk. Eine Verbindung zwischen AD DS und dem Umkreisnetzwerk kann ein ernsthaftes Sicherheitsproblem darstellen.
- Ein Edgeserver kann einer Domäne hinzugefügt werden, die sich ganz im Umkreisnetzwerk befindet. Dies wird jedoch nicht empfohlen. Edgeserver sollten nie Teil einer Domäne im internen Netzwerk sein.

Vorbereiten der Installation von Servern im Umkreisnetzwerk

Vor dem Einrichten von Edgeserverkomponenten müssen Sie sicherstellen, dass die Computer die Systemanforderungen erfüllen. Darüber hinaus müssen Sie einige vorbereitende Schritte für die Bereitstellung von Edgeserverkomponenten ausführen.

Bevor Sie beginnen, sollten Sie in der Planungsdokumentation die folgenden Themen für die Referenzarchitektur lesen, die Sie bereitstellen möchten:

- Referenzarchitektur 1: Einzelner konsolidierter Edgeserver
- Referenzarchitektur 2: Skalierte konsolidierte Edgetopologie (DNS-Lastenausgleich)
- Referenzarchitektur 3: Skalierte konsolidierte Edgetopologie (Hardwarelastenausgleich)

Inhalt dieses Abschnitts

- Systemanforderungen für Edgekomponenten
- Konfigurieren von DNS-Einträgen für die Edgeunterstützung
- Einrichten von Hardwaregeräten zum Lastenausgleich für eine skalierte Edgetopologie
- Konfigurieren von Firewalls und Ports für den externen Benutzerzugriff
- Anfordern von Edgezertifikaten
- Vorbereiten der Unterstützung von Verbindungen mit öffentlichen Instant Messaging-Diensten

Systemanforderungen für Edgekomponenten

Die Systemanforderungen für Edgekomponenten umfassen Hardware- und Softwareanforderungen sowie Anforderungen in Bezug auf die gemeinsame Ausführung. Diese Anforderungen gelten für Edgeserver sowie für alle Director- und Reverseproxyserver, die Sie bereitstellen möchten.

Inhalt dieses Abschnitts

- Hardware- und Softwareanforderungen für Edgekomponenten
- Unterstützte gemeinsame Serverausführung für Edgekomponenten

Hardware- und Softwareanforderungen für Edgekomponenten

Für Edgekomponenten müssen die Hardware- und Softwareanforderungen der Komponenten der Microsoft Lync Server 2010-Kommunikationssoftware (einschließlich Edgeserver und Directors) sowie die Anforderungen für andere Komponenten (einschließlich Reverseproxyserver, Firewalls und Lastenausgleichskomponenten) erfüllt werden, die im Umkreisnetzwerk zur Unterstützung des externen Benutzerzugriffs bereitgestellt werden sollen. Ausführliche Informationen zu den erforderlichen Komponenten für die Unterstützung des externen Benutzerzugriffs und für unterstützte Topologien finden Sie unter „Erforderliche Komponenten für den Zugriff durch externe Benutzer“.

Hardware- und Softwareanforderungen für Edgeserver und Directors

Für Edgeserver müssen dieselben Betriebssystemanforderungen erfüllt werden wie für andere Lync Server 2010-Rollen: 64-Bit-Version von Windows Server 2008 SP2 oder Windows Server 2008 R2. Zusätzlich muss das Betriebssystem für die Anwendungsserverrolle konfiguriert werden und .NET Framework 3.5 Service Pack 1 (SP1) ausführen. Directors sind interne Komponenten, die als Teil des internen Netzwerks vor der Bereitstellung von Edgeservern installiert werden. Informationen zu den Hardware- und Softwareanforderungen für Directors finden Sie unter „Technische Anforderungen für Director-Server“.

Die folgende Tabelle zeigt die Hardwareanforderungen für Edgeserver.

Hardwaresystemanforderungen für Edgeserver

Hardwarekomponente	Mindestanforderung
CPU	Eine der folgenden Optionen: • 64-Bit-Dualprozessor, Quad-Core, mindestens 2,0 GHz • 64-Bit-4-Wege-Prozessor, Dual-Core, mindestens 2,0 GHz

Hardwarekomponente	Mindestanforderung
Arbeitsspeicher	12 GB empfohlen
Datenträger	Lokaler Speicher mit mindestens 30 GB freiem Speicherplatz
Netzwerk	Zwei Netzwerkadapter erforderlich, entweder ein Netzwerkadapter mit 2 Ports und 1 GBit/s oder zwei Netzwerkadapter mit je 1 Port und 1 GBit/s.

Lync Server 2010 ist nur als 64-Bit-Version verfügbar, sodass für jeden Edgeserver und Director eines der folgenden Betriebssysteme erforderlich ist.

- Die 64-Bit-Version von Windows Server 2008 Enterprise Edition mit SP2 oder die 64-Bit-Version von Windows Server 2008 Standard Edition mit SP2.
- Die 64-Bit-Version von Windows Server 2008 R2 Enterprise oder die 64-Bit-Version von Windows Server 2008 R2 Standard.

Lync Server 2010 erfordert zudem die Installation der folgenden Programme und Updates:

- Microsoft .NET Framework 3.5 SP1
- Windows PowerShell-Befehlszeilenschnittstelle, Version 2.0
- Das Windows Server 2008 R2-Update, das über den Microsoft Knowledge Base-Artikel 2028827, „Anwendungen, die den TDI-Treiber für Netzwerkdatenverkehr verwenden, reagieren in Windows Server 2008 R2 oder in Windows 7 möglicherweise nicht mehr“, auf der folgenden Website verfügbar ist: http://go.microsoft.com/fwlink/?LinkId=205459&clcid=0x407.
- Das Windows 2008 SP2-Update ist erforderlich, um die steigende Speicherauslastung auf Webkonferenz-Edgeservern zu verhindern. Ausführliche Informationen finden Sie im Microsoft Knowledge Base-Artikel 979231, „Speicherauslastung steigt, wenn nach der Installation von Update 968389 in Windows Vista oder Windows Server 2008 die SChannel-Authentifizierung verwendet wird“, unter http://go.microsoft.com/fwlink/?LinkId=200747&clcid=0x407. Nach dem Anwenden dieses Updates sollte die steigende Speicherauslastung nicht länger auftreten.
- Das Windows Server 2008-Update, das über den Microsoft Knowledge Base-Artikel 2029048, „Anwendungen, die den TDI-Treiber für Netzwerkdatenverkehr verwenden, reagieren in

Windows Server 2008 oder in Windows Vista möglicherweise nicht mehr“,
auf der folgenden Website verfügbar ist:
http://go.microsoft.com/fwlink/?LinkId=205458&clcid=0x407.

Zusätzlich erfordert Lync Server Microsoft Visual C++ 2008C Redistributable, diese Komponente wird jedoch im Rahmen der Edgeserverinstallation automatisch installiert.

Unterstützte gemeinsame Serverausführung für Edgekomponenten

Zugriffs-Edgedienst, Webkonferenz-Edgedienst und A/V-Edgedienst werden gemeinsam auf demselben Server ausgeführt. Die folgenden Edgekomponenten können nicht gemeinsam oder zusammen mit einer anderen Microsoft Lync Server 2010-Serverrolle ausgeführt werden:

- Edgeserver
- Director
- Reverseproxy

Es ist kein dedizierter Reverseproxy für Lync Server erforderlich. Wenn Sie bereits über einen unterstützten Reverseproxyserver im Umkreisnetzwerk verfügen, der andere Geräte unterstützt, können Sie diesen für Lync Server verwenden.

Ausführliche Informationen finden Sie unter „Unterstützung“.

Konfigurieren von DNS für die Edgeunterstützung

Für die Konfiguration von DNS (Domain Name System) müssen Sie DNS-Einträge und ein DNS-Suffix für den Computernamen jedes Edgeservers konfigurieren, der nicht Mitglied einer Domäne ist.

Inhalt dieses Abschnitts

- Konfigurieren von DNS-Einträgen für die Edgeunterstützung
- Konfigurieren des DNS-Suffixes für Edgeserver

Konfigurieren von DNS-Einträgen für die Edgeunterstützung

Sie müssen DNS-Einträge (Domain Name System) für interne und externe Edgeschnittstellen konfigurieren, sowohl für Edgeserver- als auch für Reverseproxyschnittstellen.

Hinweis:
Standardmäßig verwendet DNS einen Roundrobin-Algorithmus für die Rotation von Ressourceneintragsdaten, die in Abfrageantworten zurückgegeben werden, wenn für einen abgefragten DNS-Domänennamen mehrere Ressourceneinträge desselben Typs vorhanden sind. Der DNS-Lastenausgleich in Lync Server 2010 stützt sich auf diesen Mechanismus. Stellen Sie sicher, dass diese Einstellung nicht deaktiviert ist. Stellen Sie

bei Verwendung eines DNS-Servers ohne Windows-Betriebssystem außerdem sicher, dass die Roundrobin-Verteilungsreihenfolge für Ressourceneinträge aktiviert ist.

Verwenden Sie die folgenden Verfahren, um alle erforderlichen DNS-SRV- und DNS-A-Einträge zu erstellen und zu überprüfen, die für den externen Benutzerzugriff erforderlich sind. Ausführliche Informationen zu jedem erforderlichen Eintrag für den externen Benutzerzugriff finden Sie unter „Ermitteln der DNS-Anforderungen“.

So erstellen Sie einen DNS-SRV-Eintrag

1. Klicken Sie auf dem geeigneten DNS-Server nacheinander auf **Start**, **Systemsteuerung**, **Verwaltung** und dann auf **DNS**.

   Wichtig:
   Sie müssen DNS so konfigurieren, dass Folgendes vorhanden ist: 1) Externe DNS-Einträge für externe DNS-Lookups durch Remotebenutzer und Verbundpartner; 2) Einträge für DNS-Lookups zur Verwendung durch die Edgeserver innerhalb des Umkreisnetzwerks (auch als überwachtes Subnetz bezeichnet), einschließlich A-Einträgen für die internen Server mit Lync Server 2010; und 3) interne DNS-Einträge für DNS-Lookups durch interne Clients und Server mit Lync Server 2010.

2. Erweitern Sie in der Konsolenstruktur für Ihre SIP-Domäne den Knoten **Forward-Lookupzonen**, und klicken Sie dann mit der rechten Maustaste auf die Domäne, in der Lync Server 2010 installiert ist.

3. Klicken Sie auf **Weitere neue Einträge**.

4. Klicken Sie unter **Wählen Sie einen Ressourceneintragstyp** auf **Dienstidentifizierung (SRV)** und dann auf **Eintrag erstellen**.

5. Stellen Sie alle erforderlichen Informationen für den DNS-SRV-Eintrag bereit.

So erstellen Sie einen DNS-A-Eintrag

1. Klicken Sie auf dem DNS-Server nacheinander auf **Start**, **Systemsteuerung**, **Verwaltung** und dann auf **DNS**.

2. Erweitern Sie in der Konsolenstruktur für Ihre SIP-Domäne den Knoten **Forward-Lookupzonen**, und klicken Sie dann mit der rechten Maustaste auf die Domäne, in der Lync Server 2010 installiert ist.

3. Klicken Sie auf **Neuer Host (A)**.
4. Stellen Sie alle erforderlichen Informationen für den DNS-SRV-Eintrag bereit.

So überprüfen Sie einen DNS-Eintrag

1. Melden Sie sich an einem Clientcomputer in der Domäne an.
2. Klicken Sie auf **Start** und dann auf **Ausführen**.
3. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

   ```
   nslookup <FQDN edge interface>
   ```
4. Stellen Sie sicher, dass eine Antwort zurückgegeben wird, in welcher der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) in die zugehörige IP-Adresse aufgelöst wurde.

Konfigurieren des DNS-Suffixes für Edgeserver

Der Computername eines Edgeservers, der nicht Mitglied einer Domäne ist, ist standardmäßig kein vollqualifizierter Domänenname (Fully Qualified Domain Name, FQDN), sondern ein Kurzname. Der Topologie-Generator verwendet jedoch keine Kurznamen, sondern FQDNs, und der interne Name auf dem Edgeserver muss mit dem vom Topologie-Generator verwendeten FQDN übereinstimmen. Daher müssen Sie den Kurznamen in einen FQDN ändern, indem Sie dem Namen jedes Edgeservers, der nicht Mitglied einer Domäne ist, ein DNS-Suffix hinzufügen. Führen Sie die folgenden Schritte aus, um das DNS-Suffix dem Computernamen hinzuzufügen.

So fügen Sie das DNS-Suffix dem Computernamen auf einem Edgeserver hinzu, der nicht Mitglied einer Domäne ist

1. Klicken Sie auf dem Computer auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie unter **Einstellungen für Computernamen, Domäne und Arbeitsgruppe** auf **Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Computername** auf **Ändern**.
4. Klicken Sie in **Ändern des Computernamens bzw. der Domäne** auf **Weitere**.
5. Geben Sie in **DNS-Suffix und NetBIOS-Computername** unter **Primäres DNS-Suffix des Computers** den Namen Ihrer internen Domäne (z. B. corp.contoso.com) ein, und klicken

Sie dann dreimal auf **OK**.

6. Starten Sie den Computer neu.

   Hinweis:
   Wenn Sie diese Schritte ausgeführt haben, ist der DNS-Lastenausgleich funktionsfähig.

Einrichten von Hardwaregeräten zum Lastenausgleich für eine skalierte Edgetopologie

Wenn Sie eine skalierte Edgetopologie unter Verwendung eines Hardwaregeräts zum Lastenausgleich verwenden, finden Sie unter „Referenzarchitektur 3: Skalierte konsolidierte Edgetopologie (Hardwarelastenausgleich) “ in der Planungsdokumentation weitere Informationen.

Konfigurieren von Firewalls und Ports für den externen Benutzerzugriff

Zum Konfigurieren von Firewalls und Ports müssen Sie diese für Edgeserver, Reverseproxyserver und (in einer skalierten Bereitstellung, in der kein DNS-Lastenausgleich verwendet wird) möglicherweise für Hardwaregeräte zum Lastenausgleich konfigurieren. In diesem Abschnitt werden Informationen zu den Firewall- und Portanforderungen für alle Edgeserverkomponenten und zur Konfiguration der Firewallports für Edgeserver bereitgestellt. Ausführliche Informationen zum Konfigurieren von Ports für Reverseproxyserver finden Sie unter Einrichten von Reverseproxyservern. Wenn Sie eine skalierte Edgetopologie bereitstellen und anstelle des DNS-Lastenausgleichs ein Hardwaregerät zum Lastenausgleich verwenden, finden Sie unter „Referenzarchitektur 3: Skalierte konsolidierte Edgetopologie (Hardwarelastenausgleich) “ in der Planungsdokumentation ausführliche Informationen zum Konfigurieren von Ports für Hardwaregeräte zum Lastenausgleich.

Inhalt dieses Abschnitts

- Ermitteln der Anforderungen für A/V-Firewall und Ports

Ermitteln der Anforderungen für A/V-Firewall und Ports

Ermitteln Sie anhand der folgenden Firewall- und Porttabelle, welche Firewallanforderungen gelten und welche Ports geöffnet werden müssen. Lesen Sie anschließend die Hinweise zur Netzwerkadressenübersetzung (Network Address Translation, NAT), da NAT auf viele verschiedene Arten implementiert werden kann. Ein detailliertes Beispiel zu den Firewallporteinstellungen finden Sie in den Referenzarchitekturen unter „Topologien für den Zugriff durch externe Benutzer“.

Anforderungen für A/V-Firewall und Ports

Partnerverbund mit	Feature	TCP/443	UDP/3478	RTP/UDP 50.000-59.999	RTP/TCP 50.000-59.999
Windows Live Messenger 2011	Punkt-zu-Punkt Audio/Video (A/V)	Geöffnet, eingehend	Geöffnet, eingehend Geöffnet, ausgehend	Nicht geöffnet in beide Richtungen	Geöffnet, ausgehend
Lync Server 2010	Lync Server 2010	Geöffnet, eingehend	Geöffnet, eingehend Geöffnet, ausgehend	Nicht geöffnet in beide Richtungen	Geöffnet, ausgehend
Lync Server 2010	Anwendungsfreigabe/ Desktopfreigabe	Geöffnet, eingehend	Geöffnet, eingehend Geöffnet, ausgehend	Nicht geöffnet in beide Richtungen	Geöffnet, ausgehend
Lync Server 2010	Dateiübertragung	Geöffnet, eingehend	Geöffnet, eingehend Geöffnet, ausgehend	Nicht geöffnet in beide Richtungen	Geöffnet, ausgehend
Office Communications Server 2007 R2	A/V	Geöffnet, eingehend	Geöffnet, eingehend Geöffnet, ausgehend	Nicht geöffnet in beide Richtungen	Geöffnet, ausgehend
Office Communications Server 2007 R2	Desktopfreigabe	Geöffnet, eingehend	Geöffnet, eingehend Geöffnet, ausgehend	Nicht geöffnet in beide Richtungen	Geöffnet, ausgehend
Office Communications	Dateiübertragung	–	–	–	–

Partnerverbund mit	Feature	TCP/443	UDP/3478	RTP/UDP 50.000-59.999	RTP/TCP 50.000-59.999
Server 2007 R2					
Office Communications Server 2007	A/V	Geöffnet, eingehend	Geöffnet, eingehend	Geöffnet, eingehend Geöffnet, ausgehend	Geöffnet, eingehend Geöffnet, ausgehend
Office Communications Server 2007	Desktopfreigabe	–	–	–	–
Office Communications Server 2007	Dateiübertragung	–	–	–	–

Hinweis:
(eingehend) bezieht sich auf RTP/TCP- und RTP/UDP-Datenverkehr vom Internet zur externen A/V-Edgeschnittstelle.

(ausgehend) bezieht sich auf RTP/TCP- und RTP/UDP-Datenverkehr von der externen A/V-Edgeschnittstelle zum Internet.

Portanforderungen für die externe A/V-Firewall für den externen Benutzerzugriff

Die Anforderungen in Bezug auf Firewallports für externe (und interne) SIP- und Konferenzschnittstellen (PowerPoint-Präsentationen, Whiteboardverwendung und Abrufe) sind gleich, unabhängig von der vom Verbundpartner ausgeführten Version.

Dies gilt nicht für die externe A/V-Edgeschnittstelle (Audio/Video). In den meisten Fällen erfordert der A/V-Edgedienst, dass die externen Firewallregeln RTP/TCP- und RTP/UDP-Datenverkehr im Portbereich 50.000 bis 59.999 in beide Richtungen zulassen. Das Öffnen dieses Portbereichs ist beispielsweise erforderlich, um bestimmte Partnerverbundszenarien zu unterstützen. Die oben stehende Tabelle liefert Details für jedes Szenario. In der Tabelle wird davon ausgegangen, dass Lync Server 2010 den primären Verbundpartner darstellt und zur Kommunikation mit einer der vier Verbundpartnertypen konfiguriert ist.

Hinweis:
Als bewährte Methode für Lync Server 2010 sollte der Portbereich von 50.000 bis 59.999 ausgehend für „beliebigen“ RDP/TCP-Datenverkehr für die externe A/V-Edgeschnittstelle geöffnet werden, sofern die Unternehmensrichtlinien dies zulassen.

NAT-Anforderungen für den externen Benutzerzugriff

NAT ist typischerweise eine Routingfunktion, aber neuere Geräte – beispielsweise Firewalls und sogar Hardwaregeräte zum Lastenausgleich – können für NAT konfiguriert werden. Statt einer Beschreibung, welches Gerät die Netzwerkadressenübersetzung durchführt, wird in diesem Thema das erwartete NAT-Verhalten erläutert.

Die Microsoft Lync Server 2010-Kommunikationssoftware bietet keine NAT-Unterstützung für Datenverkehr von der oder zur internen Edgeschnittstelle, für die externe Edgeschnittstelle ist jedoch das folgende NAT-Verhalten erforderlich. In dieser Dokumentation werden die Akronyme „ChangeDST“ und „ChangeSRC“ in Tabellen und Abbildungen zum Definieren des folgenden erforderlichen Verhaltens verwendet:

- **ChangeDST** Der Vorgang der Änderung der Ziel-IP-Adresse für Pakete an das Netzwerk mit NAT-Verwendung. Auch bekannt als Transparenz, Portweiterleitung, Ziel-NAT-Modus oder Halb-NAT-Modus.

- **ChangeSRC** Der Vorgang der Änderung der Quell-IP-Adresse für Pakete an das Netzwerk mit NAT-Verwendung. Auch bekannt als Proxy, sichere Netzwerkadressenübersetzung, NAT mit Statusinformationen, Quell-NAT oder Voll-NAT-Modus.

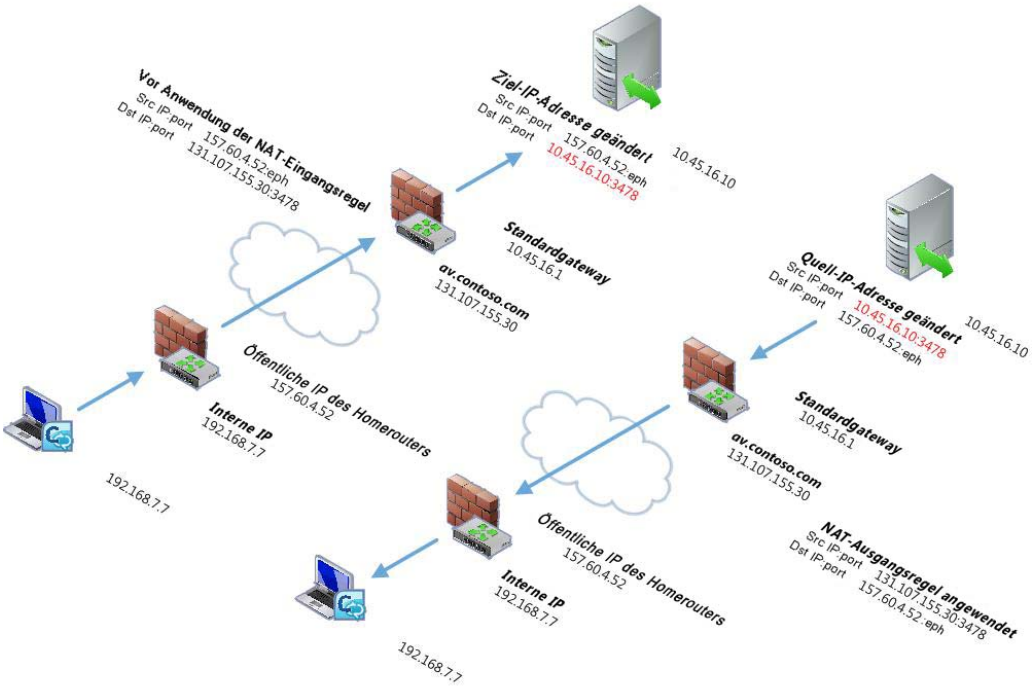
Unabhängig von der verwendeten Namenskonvention lautet das für die externe Schnittstelle des Edgeservers erforderliche NAT-Verhalten wie folgt:

- Für Datenverkehr vom Internet zur externen Edgeschnittstelle:
    - Änderung der Ziel-IP-Adresse des eingehenden Pakets von der öffentlichen IP-Adresse der externen Edgeschnittstelle in die übersetzte IP-Adresse der externen Edgeschnittstelle.
    - Beibehaltung der Quell-IP-Adresse, sodass eine Rückroute für den Datenverkehr vorhanden ist.
- Für Datenverkehr von der externen Edgeschnittstelle zum Internet:
    - Änderung der Quell-IP-Adresse des von der externen Edgeschnittstelle ausgehenden Pakets von der übersetzten IP-Adresse in die öffentliche IP-Adresse der externen Edgeschnittstelle, sodass die interne (nicht routingfähige) IP-Adresse der Edgeschnittstelle nicht offengelegt wird.

- Beibehaltung der Ziel-IP-Adresse für die ausgehenden Pakete.

Die folgende Abbildung zeigt den Unterschied zwischen der Änderung der Ziel-IP-Adresse (ChangeDST) für eingehenden Datenverkehr und der Änderung der Quell-IP-Adresse (ChangeSRC) für ausgehenden Datenverkehr am Beispiel der A/V-Edgeschnittstelle.

Änderung der Ziel-IP-Adresse (ChangeDST) für eingehenden Datenverkehr und Änderung der Quell-IP-Adresse (ChangeSRC)



Die wichtigsten Punkte hierbei sind:

- Für an der A/V-Edgeschnittstelle eingehenden Datenverkehr werden Quell-IP-Adresse und Port nicht geändert, die Ziel-IP-Adresse ändert sich jedoch von 63.123.155.30 in die übersetzte IP-Adresse 10.45.16.10.

- Für von der A/V-Edgeschnittstelle zur Arbeitsstation ausgehenden Datenverkehr ändert sich die Quell-IP-Adresse von der öffentlichen IP-Adresse der Arbeitsstation in die öffentliche Adresse der A/V-Edgeschnittstelle. Als Ziel-IP-Adresse wird die öffentliche IP-Adresse der Arbeitsstation beibehalten. Nachdem das Paket das erste NAT-Gerät ausgehend passiert hat, ändert die Regel auf dem NAT-Gerät die Quell-IP-Adresse von der IP-Adresse der externen A/V-Edgeschnittstelle (10.45.16.10) in die zugehörige öffentliche IP-Adresse (63.123.155.30).

Anfordern von Edgezertifikaten

Die erforderlichen Zertifikate für die Unterstützung des Zugriffs durch externe Benutzer umfassen Zertifikate, die von einer öffentlichen Zertifizierungsstelle (Certification Authority, CA) ausgestellt wurden, sowie Zertifikate, die von einer internen Unternehmenszertifizierungsstelle ausgestellt wurden:

- Die für die externe Schnittstelle von Edgeservern und den Reverseproxy erforderlichen Zertifikate müssen von einer öffentlichen Zertifizierungsstelle ausgestellt werden.
- Die für die interne Schnittstelle benötigten Zertifikate können entweder von einer öffentlichen Zertifizierungsstelle oder von einer internen Unternehmenszertifizierungsstelle ausgestellt werden. Um die Kosten bei der Verwendung öffentlicher Zertifikate zu reduzieren, wird zur Erstellung dieser Zertifikate die Verwendung einer internen Windows Server 2008- oder Windows Server 2008 R2-Zertifizierungsstelle empfohlen.

Da die Verarbeitung von Zertifikatsanforderungen (insbesondere bei Anforderungen an öffentliche Zertifizierungsstellen) mit einem gewissen Zeitaufwand verbunden sein kann, sollten Sie die Zertifikate für Ihre Edgeserver frühzeitig anfordern, um ihre Verfügbarkeit sicherzustellen, wenn Sie mit der Bereitstellung Ihrer Edgeserverkomponenten beginnen. Eine Zusammenfassung der Anforderungen für Edgeserverzertifikate finden Sie unter Zertifikatanforderungen für den externen Benutzerzugriff.

Inhalt dieses Abschnitts

- Anfordern von Zertifikaten von einer öffentlichen Zertifizierungsstelle
- Anfordern von Zertifikaten von einer internen Unternehmenszertifizierungsstelle

Anfordern von Zertifikaten von einer öffentlichen Zertifizierungsstelle

Für Ihre Edgeserverbereitstellung ist ein einzelnes öffentliches Zertifikat für die externen Schnittstellen der Edgeserver erforderlich, das für den Zugriffs-Edgedienst, den Webkonferenz-Edgedienst und für den A/V-Authentifizierungsdienst verwendet wird. Dieses Zertifikat erfordert einen exportierbaren privaten Schlüssel, um sicherzustellen, dass der A/V-Authentifizierungsdienst für alle Edgeserver in einem Pool dieselben Schlüssel verwendet. Für den Reverseproxy, der mit Microsoft Internet Security and Acceleration (ISA) Server 2006 oder Microsoft Forefront Threat Management Gateway 2010 eingesetzt wird, ist ebenfalls ein öffentliches Zertifikat erforderlich.

Wenngleich Sie eine öffentliche Zertifizierungsstelle für das interne Edgezertifikat verwenden können, wird die Verwendung einer internen Unternehmenszertifizierungsstelle für diese anderen Zertifikate empfohlen, um die Kosten für Zertifikate zu minimieren. Eine Zusammenfassung der Anforderungen für Edgeserverzertifikate finden Sie unter Zertifikatanforderungen für den externen Benutzerzugriff. Ausführliche Informationen zur Verwendung einer internen

Unternehmenszertifizierungsstelle zum Anfordern der internen Zertifikate für Edgeserver und A/V-Authentifizierung finden Sie unter Anfordern von Zertifikaten von einer internen Unternehmenszertifizierungsstelle.

Hinweis:
Bei der Installation eines Edgeservers umfasst Setup einen Zertifikat-Assistenten, der die Aufgaben zum Anfordern, Zuweisen und Installieren von Zertifikaten vereinfacht (eine Beschreibung finden Sie im Abschnitt Einrichten von Edgezertifikaten). Wenn Sie die Zertifikate vor der Installation eines Edgeservers anfordern möchten (um bei der eigentlichen Bereitstellung der Edgeserverkomponenten Zeit zu sparen), können Sie zu diesem Zweck interne Server verwenden. Sie müssen lediglich sicherstellen, dass die Zertifikate exportierbar sind und alle erforderlichen alternativen Antragstellernamen enthalten. Die Verfahren zur Verwendung interner Server zum Anfordern von Zertifikaten sind in dieser Dokumentation nicht beschrieben.

Anfordern von Zertifikaten von einer internen Unternehmenszertifizierungsstelle

Die für die interne Edgeschnittstelle benötigten Zertifikate können entweder von einer öffentlichen oder von einer internen Zertifizierungsstelle ausgestellt werden. Mithilfe einer internen Unternehmenszertifizierungsstelle können Sie die Kosten für Zertifikate minimieren. Wenn in Ihrer Organisation eine interne Zertifizierungsstelle bereitgestellt wurde, sollten die Zertifikate für die interne Edgeschnittstelle durch die interne Zertifizierungsstelle ausgestellt werden. Das Verwenden einer internen Unternehmenszertifizierungsstelle für interne Zertifikate kann zu einer erheblichen Senkung der Kosten für Zertifikate beitragen.

Eine Zusammenfassung der Zertifikatanforderungen für Edgekomponenten finden Sie unter Zertifikatanforderungen für den externen Benutzerzugriff. Ausführliche Informationen zum Verwenden einer öffentlichen Zertifizierungsstelle für das Abrufen von Zertifikaten finden Sie unter Anfordern von Zertifikaten von einer öffentlichen Zertifizierungsstelle. Ausführliche Informationen zum Anfordern, Installieren und Zuweisen von Zertifikaten finden Sie unter Einrichten von Edgezertifikaten.

Vorbereiten der Unterstützung von Verbindungen mit öffentlichen Instant Messaging-Diensten

Die Unterstützung von Benutzern öffentlicher Sofortnachrichtendienste in Ihrer Organisation erfordert, dass eine geeignete Lizenzierung vorhanden ist und dass der Bereitstellungsvorgang für die zu unterstützenden öffentlichen Sofortnachrichtendienste abgeschlossen wurde. Die Bereitstellung kann bis zu 30 Tage in Anspruch nehmen. Planen Sie daher genügend Zeit ein, damit die Bereitstellung zum gewünschten Zeitpunkt der Implementierung abgeschlossen ist. Ausführliche Informationen zu Lizenzierungsanforderungen und zum Abschließen des Bereitstellungsvorgangs finden Sie auf der Seite „Public IM Connectivity Provisioning Guide for Microsoft Lync Server,

Office Communications Server, and Live Communications Server“ unter http://go.microsoft.com/fwlink/?LinkId=155970&clcid=0x407.

Wenn Sie einen A/V-Partnerverbund (Audio/Video) mit Windows Live Messenger implementieren, müssen Sie zwei Parameter ändern, nämlich die Microsoft Lync Server 2010-Verschlüsselungsstufe und die Richtlinie „EnablePublicCloudAccess“. Standardmäßig lautet die Verschlüsselungsstufe **Erforderlich**. Sie müssen diese Einstellung in **Unterstützt** ändern. Die Richtlinie „EnablePublicCloudAccess“ ist auf „False“ festgelegt und muss auf „True“ festgelegt werden. Sie können diese Änderung mithilfe der Lync Server-Verwaltungsshell ausführen.

1. Starten der Lync Server-Verwaltungsshell: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Verwaltungsshell**.

2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
Set-CsMediaConfiguration –EncryptionLevel SupportEncryption
Set-CsExternalAccessPolicy Global –EnablePublicCloudAccess $true
-EnablePublicCloudAudioVideoAccess $true
```

   Hinweis:
   In diesem Beispiel wird die globale Richtlinie geändert. Ändern Sie dies in Ihrer Umgebung in die entsprechende Richtlinie.

Siehe auch

Set-CsMediaConfiguration

Aufbau einer Edge- und Director-Topologie

Das Bereitstellen der Topologie umfasst die folgenden Planungs- und Bereitstellungsaufgaben:

- **Planung** Sie müssen eine geeignete Topologie für Ihre Organisation definieren und die erforderlichen Komponenten zu ihrer Bereitstellung identifizieren. Dies sind die Standardschritte im Planungsprozess. Das Microsoft Lync Server 2010-Planungstool erleichtert Ihnen den Start des Planungsprozesses, einschließlich der Möglichkeit zur einfachen Durchführung von Änderungen, wenn Anforderungen und Pläne finalisiert wurden.

- **Bereitstellung** Die Topologie, die Sie mit dem Topologie-Generator definieren, ist wesentlich für die Bereitstellung eines beliebigen Servers mit Lync Server 2010. Wenn Sie Ihre Topologie im Rahmen der Planung nicht mit dem Topologie-Generator definieren und veröffentlichen, müssen Sie sie vervollständigen und die Informationen auf den Edgeservern zur Verfügung stellen, bevor Sie die Edgeserver bereitstellen.

Sie können Edgeserverkomponenten erst bereitstellen, wenn mindestens ein interner Pool bereitgestellt wurde, und Sie müssen den Topologie-Generator installieren, um einen internen Pool bereitzustellen. In diesem Abschnitt wird die Installation des Topologie-Generators nicht abgedeckt, da diese Aufgabe Bestandteil des Installationsvorgangs für den internen Pool ist.

Ausführliche Informationen zu diesen Tools finden Sie unter Tools für die Edgebereitstellung.

Hinweis:
Wenn Sie den Topologie-Generator zum Definieren einer vollständigen Topologie (einschließlich Edgetopologie) verwendet haben, können Sie die Aufgaben Definieren der Edgetopologie und Veröffentlichen der Topologie in diesem Abschnitt überspringen.
Sie müssen jedoch die Aufgabe Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation ausführen.

Inhalt dieses Abschnitts

- Definieren des Directors
- Definieren der Edgetopologie
- Veröffentlichen der Topologie

Definieren des Directors

Wenn Sie den Zugriff durch externe Benutzer über die Bereitstellung von Edgeservern aktivieren, sollten Sie auch einen Director bereitstellen. Ein Director ist ein Server mit Microsoft Lync Server 2010, der Benutzeranforderungen authentifiziert, jedoch keine Benutzerkonten verwaltet. Wenn Sie einen Director zur Authentifizierung externer Benutzer verwenden, übernimmt dieser die folgenden Aufgaben:

- Der Director senkt die Datenlast für die Server im Front-End-Pool, da die Authentifizierung dieser Benutzer über den Pool entfällt.
- Der Director trägt dazu bei, interne Front-End-Pools vor möglicherweise bösartigem Datenverkehr zu schützen, beispielsweise bei DoS-Angriffen (Denial of Service).
- Wenn das Netzwerk während eines solchen Angriffs mit ungültigem externen Datenverkehr überflutet wird, endet der Datenverkehr beim Director. Interne Benutzer sollten daher keine Auswirkungen auf die Leistung wahrnehmen.

Zur Bereitstellung eines beliebigen Servers mit Lync Server 2010 müssen Sie zunächst mit dem Topologie-Generator Ihre Topologie, einschließlich Director- und Edgeservertopologie, definieren und veröffentlichen.

Inhalt dieses Abschnitts

- Definieren eines einzelnen Directors im Topologie-Generator
- Definieren eines Pools mit mehreren Directors im Topologie-Generator

Definieren eines einzelnen Directors im Topologie-Generator

Lync Server 2010-Directors können als Einzelinstanzserver bereitgestellt oder zur Verbesserung von Verfügbarkeit und Kapazität als Lastenausgleichspool mit mehreren Directors installiert werden. Sowohl Hardwarelastenausgleich als auch DNS-Lastenausgleich (Domain Name System) werden unterstützt. In diesem Thema wird erläutert, wie Sie den DNS-Lastenausgleich für Directorpools konfigurieren.

Für eine erfolgreiche Veröffentlichung, Aktivierung oder Deaktivierung einer Topologie beim Hinzufügen oder Entfernen einer Serverrolle müssen Sie als Mitglied der Gruppen **RTCUniversalServerAdmins** und **Domänen-Admins** angemeldet sein. Es ist auch möglich, die geeigneten Administratorrechte und -berechtigungen für das Hinzufügen von Serverrollen zu delegieren. Ausführliche Informationen finden Sie unter „Delegieren von Setupberechtigungen“ in der Bereitstellungsdokumentation für Standard Edition-Server oder Enterprise Edition-Server. Für andere Konfigurationsänderungen müssen Sie lediglich Mitglied der Gruppe **RTCUniversalServerAdmins** sein.

So definieren Sie den Director (Einzelinstanz)

1. Starten des Topologie-Generators: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Topologie-Generator**.
2. Klicken Sie auf der Willkommensseite auf **Topologie aus vorhandener Bereitstellung herunterladen**.
3. Geben Sie im Dialogfeld **Topologie speichern unter** den Namen und den Speicherort für die lokale Kopie der vorhandenen Topologie ein, und klicken Sie auf **Speichern**.
4. Erweitern Sie den Standort, an dem der Director hinzugefügt werden soll, klicken Sie mit der rechten Maustaste auf **Directorpools**, und klicken Sie anschließend auf **Neuer Directorpool**.
5. Führen Sie im Dialogfeld **FQDN des Directorpools definieren** die folgenden Schritte aus:
   - Geben Sie in **Pool-FQDN** den FQDN für den Directorpool ein.
   - Klicken Sie auf **Pool mit einem Computer** und dann auf **Weiter**.
6. Führen Sie im Dialogfeld **Dateifreigabe definieren** einen der folgenden Schritte aus:
   a. Zum Verwenden einer vorhandenen Dateifreigabe klicken Sie auf **Zuvor definierte**

Dateifreigabe verwenden, wählen Sie eine Dateifreigabe aus der Liste aus, und klicken Sie auf **Weiter**.

b. Zum Erstellen einer neuen Dateifreigabe klicken Sie auf **Neue Dateifreigabe definieren**, geben Sie in **Dateiserver-FQDN** den FQDN für das Verzeichnis der Dateifreigabe ein, geben Sie in **Dateifreigabe** den Namen der Freigabe ein, und klicken Sie anschließend auf **Weiter**.

Wichtig:
Die Dateifreigabe, die Sie in diesem Schritt angeben oder erstellen, muss vor der Veröffentlichung der Topologie vorhanden sein oder erstellt werden.

7. Geben Sie im Dialogfeld **Webdienste-URL angeben** in **Externe Basis-URL** den FQDN für die Directors an, und klicken Sie anschließend auf **Fertig stellen**.

Wichtig:
Der Name muss von Internet-DNS-Servern aufgelöst werden können und auf die öffentliche IP-Adresse des Reverseproxys verweisen, der an diese URL gesendete HTTP/HTTPS-Anforderungen überwacht und diese an das virtuelle Verzeichnis der externen Webdienste auf diesem Director weiterleitet.

8. Veröffentlichen Sie die Topologie.

Definieren eines Pools mit mehreren Directors im Topologie-Generator

Lync Server 2010-Directors können als Einzelinstanzserver bereitgestellt oder zur Verbesserung von Verfügbarkeit und Kapazität als Lastenausgleichspool mit mehreren Directors installiert werden. Sowohl Hardwarelastenausgleich als auch DNS-Lastenausgleich (Domain Name System) werden unterstützt. In dieser Dokumentation wird erläutert, wie Sie den DNS-Lastenausgleich für Directorpools konfigurieren.

Für eine erfolgreiche Veröffentlichung, Aktivierung oder Deaktivierung einer Topologie beim Hinzufügen oder Entfernen einer Serverrolle müssen Sie als Mitglied der Gruppen **RTCUniversalServerAdmins** und **Domänen-Admins** angemeldet sein. Es ist auch möglich, die geeigneten Administratorrechte und -berechtigungen für das Hinzufügen von Serverrollen zu delegieren. Ausführliche Informationen finden Sie unter „Delegieren von Setupberechtigungen“ in der Bereitstellungsdokumentation für Standard Edition-Server oder Enterprise Edition-Server. Für andere Konfigurationsänderungen müssen Sie lediglich Mitglied der Gruppe **RTCUniversalServerAdmins** sein.

So definieren Sie den Director (Pool mit mehreren Directors)

1. Starten des Topologie-Generators: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Topologie-Generator**.

2. Klicken Sie auf der Willkommensseite auf **Topologie aus vorhandener Bereitstellung herunterladen**.

3. Geben Sie im Dialogfeld **Topologie speichern unter** den Namen und den Speicherort für die lokale Kopie der vorhandenen Topologie ein, und klicken Sie auf **Speichern**.

4. Erweitern Sie den Standort, an dem der Director hinzugefügt werden soll, klicken Sie mit der rechten Maustaste auf **Directorpools**, und klicken Sie anschließend auf **Neuer Directorpool**.

5. Führen Sie im Dialogfeld **FQDN des Directorpools definieren** die folgenden Schritte aus:

   - Geben Sie in **Pool-FQDN** den FQDN für den Directorpool ein.

   - Klicken Sie auf **Pool mit mehreren Computern** und dann auf **Weiter**.

6. Führen Sie im Dialogfeld **Computer in diesem Pool definieren** die folgenden Schritte aus:

   - Geben Sie den Computer-FQDN des ersten Mitglieds im Pool an, und klicken Sie anschließend auf **Hinzufügen**.

   - Wiederholen Sie diesen Schritt für jeden Computer, den Sie hinzufügen möchten, und klicken Sie zum Schluss auf **Weiter**.

7. Führen Sie im Dialogfeld **Dateifreigabe definieren** einen der folgenden Schritte aus:

   - Zum Verwenden einer vorhandenen Dateifreigabe klicken Sie auf **Zuvor definierte Dateifreigabe verwenden**, wählen Sie eine Dateifreigabe aus der Liste aus, und klicken Sie auf **Weiter**.

   - Zum Erstellen einer neuen Dateifreigabe klicken Sie auf **Neue Dateifreigabe definieren**, geben Sie in **Dateiserver-FQDN** den FQDN für das Verzeichnis der Dateifreigabe ein, geben Sie in **Dateifreigabe** den Namen der Freigabe ein, und klicken Sie anschließend auf **Weiter**.

Wichtig:
Die Dateifreigabe, die Sie in diesem Schritt angeben oder erstellen, muss vor der Veröffentlichung der Topologie vorhanden sein oder erstellt werden.

Die einem Director zugewiesene Dateifreigabe wird nicht tatsächlich verwendet, Sie können dem Director also die Dateifreigabe jedes Pools in der Organisation zuweisen.

8. Geben Sie im Dialogfeld **Webdienste-URL angeben** in **Externe Basis-URL** den FQDN für

die Directors an, und klicken Sie anschließend auf **Fertig stellen**.

Wichtig:
Der Name muss von Internet-DNS-Servern aufgelöst werden können und auf die öffentliche IP-Adresse des Reverseproxys verweisen, der an diese URL gesendete HTTP/HTTPS-Anforderungen überwacht und diese an das virtuelle Verzeichnis der externen Webdienste in diesem Directorpool weiterleitet.

9. Veröffentlichen Sie die Topologie.

Definieren der Edgetopologie

Zur Bereitstellung eines beliebigen Servers mit Lync Server 2010 müssen Sie zunächst mit dem Topologie-Generator Ihre Topologie, einschließlich Edgetopologie, definieren und veröffentlichen.

Inhalt dieses Abschnitts

- Definieren der Topologie für einen einzelnen Edgeserver
- Definieren der Topologie für einen Edgeserverpool mit DNS-Lastenausgleich
- Definieren der Topologie für einen Edgeserverpool mit Hardwarelastenausgleich

Definieren der Topologie für einen einzelnen Edgeserver

Sie müssen den Topologie-Generator zum Erstellen Ihrer Topologie verwenden und mindestens einen internen Front-End-Pool oder Standard Edition-Server einrichten, bevor Sie Ihre Edgeserver bereitstellen können. Verwenden Sie das folgende Verfahren, um Ihre Edgetopologie für einen einzelnen Edgeserver zu definieren, und anschließend die Verfahren in Veröffentlichen der Topologie und Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation, um die Topologie zu veröffentlichen und für Ihren Edgeserver zur Verfügung zu stellen.

Für eine erfolgreiche Veröffentlichung, Aktivierung oder Deaktivierung einer Topologie beim Hinzufügen oder Entfernen einer Serverrolle müssen Sie als Mitglied der Gruppen „RTCUniversalServerAdmins“ und „Domänen-Admins“ angemeldet sein. Es ist auch möglich, die geeigneten Administratorrechte und -berechtigungen für das Hinzufügen von Serverrollen zu delegieren. Ausführliche Informationen finden Sie unter „Delegieren von Setupberechtigungen“ in der Bereitstellungsdokumentation für Standard Edition-Server oder Enterprise Edition-Server. Für andere Konfigurationsänderungen müssen Sie lediglich Mitglied der Gruppe „RTCUniversalServerAdmins“ sein.

Wenn Sie Ihre Edgetopologie beim Definieren und Veröffentlichen Ihrer internen Topologie definiert haben und an der zuvor definierten Edgetopologie keine Änderungen erforderlich sind, müssen Sie die Topologie nicht erneut definieren und veröffentlichen. Folglich können Sie die

folgende Vorgehensweise überspringen. Sie müssen die zuvor definierte und veröffentlichte Topologie jedoch für Ihre Edgeserver zur Verfügung stellen. Zu diesem Zweck führen Sie die Schritte unter Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation aus.

Wichtig:
Der Topologie-Generator kann nicht auf einem Edgeserver ausgeführt werden.
Der Topologie-Generator muss entweder auf Ihrem Front-End-Server oder auf Standard Edition-Servern ausgeführt werden.

So definieren Sie die Topologie für einen einzelnen Edgeserver

1. Starten des Topologie-Generators: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Topologie-Generator**.

2. Erweitern Sie in der Konsolenstruktur den Standort, an dem ein Edgeserver bereitgestellt werden soll.

3. Klicken Sie mit der rechten Maustaste auf **Edgepools**, und klicken Sie dann auf **Neuer Edgepool**.

4. Klicken Sie in **Neuen Edgepool definieren** auf **Weiter**.

5. Führen Sie in **FQDN des Edgepools definieren** die folgenden Schritte aus:

   - Geben Sie im Feld **Pool-FQDN** den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der internen Schnittstelle für den Edgeserver ein.

     Wichtig:
     Der angegebene Name muss mit dem auf dem Server konfigurierten Computernamen übereinstimmen. Der Name eines Computers, der nicht Mitglied einer Domäne ist, ist standardmäßig kein FQDN, sondern ein Kurzname. Der Topologie-Generator verwendet keine Kurznamen, sondern FQDNs. Sie müssen deshalb ein DNS-Suffix für den Namen des Computers konfigurieren, der als Edgeserver bereitgestellt werden soll und nicht Mitglied einer Domäne ist. Verwenden Sie nur Standardzeichen (einschließlich A–Z, a–z, 0–9 und Bindestrichen) beim Zuweisen von FQDNs für die Lync-Server, Edgeserver und Pools. Verwenden Sie keine Unicode-Zeichen oder Unterstriche. Andere als die genannten Zeichen in einem FQDN werden von externen DNS und öffentlichen Zertifizierungsstellen (wenn der FQDN dem SN im Zertifikat zugewiesen werden muss) häufig nicht unterstützt. Ausführliche Informationen zum Hinzufügen eines DNS-Suffixes zu einem Computernamen finden Sie unter Konfigurieren von DNS-Einträgen für die Edgeunterstützung.

- Klicken Sie auf **Pool mit einem Computer** und dann auf **Weiter**.

6. Führen Sie unter **Funktionen auswählen** die folgenden Schritte aus:

   - Wenn ein einziger FQDN und eine einzige IP-Adresse für den SIP-Zugriffsdienst, den Lync Server-Webkonferenzdienst und den A/V-Edgedienst verwendet werden soll, aktivieren Sie das Kontrollkästchen **Einen FQDN und eine IP-Adresse verwenden**.
   - Wenn der Partnerverbund aktiviert werden soll, aktivieren Sie das Kontrollkästchen **Partnerverbund aktivieren (Port 5061)**.

     Hinweis:
     Sie können diese Option auswählen, es kann jedoch nur ein Edgepool oder Edgeserver in Ihrer Organisation extern für den Partnerverbund veröffentlicht werden. Der Zugriff durch Partnerbenutzer, einschließlich Benutzer öffentlicher Sofortnachrichtendienste, erfolgt stets über denselben Edgepool oder einzelnen Edgeserver. Wenn Ihre Bereitstellung beispielsweise je einen Edgepool oder einzelnen Edgeserver in New York und in London umfasst und Sie die Unterstützung des Partnerverbunds für den Edgepool oder einzelnen Edgeserver in New York aktivieren, erfolgt der Signaldatenverkehr für Partnerbenutzer über den Edgepool oder einzelnen Edgeserver in New York. Dies gilt auch für die Kommunikation mit Benutzern in London, wenngleich ein interner Benutzer in London, der einen Partnerbenutzer in London anruft, für den A/V-Datenverkehr den Pool oder Edgeserver in London verwendet.

   - Wenn Sie die Netzwerkadressenübersetzung (Network Address Translation, NAT) für Ihre öffentlichen IP-Adressen verwenden möchten, aktivieren Sie das Kontrollkästchen **Externe IP-Adresse dieses Edgepools von der NAT übersetzen**.

7. Führen Sie in **Externe FQDNs** die folgenden Schritte aus:

   - Wenn Sie in **Funktionen auswählen** festlegen, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Edgedienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie in **SIP-Zugriff** den externen FQDN ein.

     Hinweis:
     Wenn Sie diese Option aktivieren, müssen Sie für jeden Edgedienst eine andere Portnummer angeben (die empfohlenen Porteinstellungen lauten: 5061 für den Zugriffs-Edgedienst, 444 für den Webkonferenz-Edgedienst und 443 für den A/V-Edgedienst). Durch Auswahl dieser Option können Sie potenzielle Konnektivitätsprobleme verhindern und die Konfiguration vereinfachen, indem Sie dieselbe Portnummer (z. B. 443) für alle drei

Dienste verwenden.

- Wenn Sie in **Funktionen auswählen** nicht festgelegt haben, dass ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie die externen FQDNs für **SIP-Zugriff**, **Webkonferenzen** und **Audio/Video** ein. Behalten Sie dabei die Standardports bei.

8. Klicken Sie auf **Weiter**.

9. Geben Sie unter **Interne IP-Adresse definieren** in **Interne IP-Adresse** die IP-Adresse Ihres Edgeservers ein, und klicken Sie anschließend auf **Weiter**.

10. Führen Sie in **Externe IP-Adresse definieren** die folgenden Schritte aus:

    - Wenn Sie festgelegt haben, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Edgedienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie in **SIP-Zugriff** die externe IP-Adresse des Edgeservers ein. Klicken Sie anschließend auf **Weiter**.

    - Wenn Sie nicht festgelegt haben, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Edgedienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie in **SIP-Zugriff**, **Webkonferenzen** und **A/V-Konferenzen** die externen IP-Adressen der Edgeserver ein. Klicken Sie anschließend auf **Weiter**.

11. Wenn Sie die Verwendung der Netzwerkadressenübersetzung festgelegt haben, wird ein Dialogfeld angezeigt. Geben Sie in **Öffentliche IP-Adresse** die öffentliche IP-Adresse ein, die mithilfe der Netzwerkadressenübersetzung übersetzt werden soll, und klicken Sie anschließend auf **Weiter**.

    Hinweis:
    Dies sollte die externe IP-Adresse des AV-Edgedienst sein.

12. Wählen Sie in **Nächsten Hop definieren** in der Liste **Nächster Hoppool** den Namen des internen Pools aus, bei dem es sich entweder um einen Front-End-Pool oder um einen Standard Edition-Pool handeln kann. Oder, wenn Ihre Bereitstellung einen Director umfasst, geben Sie den Namen des Directors ein. Klicken Sie anschließend auf **Weiter**.

13. Geben Sie in **Front-End-Pools zuordnen** einen oder mehrere interne Pools an (diese können Front-End-Pools und Standard Edition-Server umfassen), die diesem Edgeserver zugeordnet werden sollen. Wählen Sie dazu die Namen der internen Pools aus, die diesen Edgeserver für die Kommunikation mit unterstützten externen Benutzern verwenden.

    Hinweis:
    Jedem internen Pool kann für A/V-Datenverkehr nur ein Edgepool mit

Lastenausgleich oder einzelner Edgeserver zugeordnet werden. Wenn einem internen Pool bereits ein Edgepool oder Edgeserver zugeordnet ist, werden Sie in einer Warnmeldung darüber informiert. Bei Auswahl eines Pools, der bereits einem anderen Edgeserver zugeordnet ist, wird die Zuordnung geändert.

14. Klicken Sie auf **Fertig stellen**.

15. Veröffentlichen Sie die Topologie.

Definieren der Topologie für einen Edgeserverpool mit DNS-Lastenausgleich

Sie müssen den Topologie-Generator zum Erstellen Ihrer internen Topologie und Edgetopologie verwenden und mindestens einen internen Front-End-Pool oder Standard Edition-Server einrichten, bevor Sie Edgeserver bereitstellen können. Verwenden Sie das folgende Verfahren, um Ihre Edgetopologie für einen Edgepool mit Lastenausgleich zu definieren, und anschließend die Verfahren in Veröffentlichen der Topologie und Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation, um die Topologie zu veröffentlichen und für Edgeserver zur Verfügung zu stellen.

Für eine erfolgreiche Veröffentlichung, Aktivierung oder Deaktivierung einer Topologie beim Hinzufügen oder Entfernen einer Serverrolle müssen Sie als Mitglied der Gruppen „RTCUniversalServerAdmins“ und „Domänen-Admins“ angemeldet sein. Es ist auch möglich, die geeigneten Administratorrechte und -berechtigungen für das Hinzufügen von Serverrollen zu delegieren. Ausführliche Informationen finden Sie unter „Delegieren von Setupberechtigungen“ in der Bereitstellungsdokumentation für Standard Edition-Server oder Enterprise Edition-Server. Für andere Konfigurationsänderungen müssen Sie lediglich Mitglied der Gruppe „RTCUniversalServerAdmins“ sein.

Wenn Sie Ihre Edgetopologie beim Definieren und Veröffentlichen Ihrer internen Topologie definiert haben und an der zuvor definierten Edgetopologie keine Änderungen erforderlich sind, müssen Sie die Topologie nicht erneut definieren und veröffentlichen. Folglich können Sie die folgende Vorgehensweise überspringen. Sie müssen die zuvor definierte und veröffentlichte Topologie jedoch für Ihre Edgeserver zur Verfügung stellen. Zu diesem Zweck führen Sie die Schritte unter Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation aus.

Wichtig:
Der Topologie-Generator kann nicht auf einem Edgeserver ausgeführt werden. Der Topologie-Generator muss in Ihrem Front-End-Pool oder auf Standard Edition-Servern ausgeführt werden.

So definieren Sie die Topologie für einen Edgeserverpool mit DNS-Lastenausgleich

1. Starten des Topologie-Generators: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft**

Lync Server 2010 und anschließend auf **Lync Server-Topologie-Generator**.

2. Erweitern Sie in der Konsolenstruktur den Standort, an dem Edgeserver bereitgestellt werden sollen.

3. Klicken Sie mit der rechten Maustaste auf **Edgepools**, und klicken Sie dann auf **Neuer Edgepool**.

4. Klicken Sie in **Neuen Edgepool definieren** auf **Weiter**.

5. Führen Sie in **FQDN des Edgepools definieren** die folgenden Schritte aus:

   - Geben Sie in **Pool-FQDN** den vollqualifizierten Domänennamen ein, den Sie für die interne Seite des Edgepools ausgewählt haben.

     Wichtig:
     Der angegebene Name muss mit dem auf dem Server konfigurierten Computernamen übereinstimmen. Der Name eines Computers, der nicht Mitglied einer Domäne ist, ist standardmäßig kein FQDN, sondern ein Kurzname. Der Topologie-Generator verwendet keine Kurznamen, sondern FQDNs. Sie müssen deshalb ein DNS-Suffix für den Namen des Computers konfigurieren, der als Edgeserver bereitgestellt werden soll und nicht Mitglied einer Domäne ist. Verwenden Sie nur Standardzeichen (einschließlich A–Z, a–z, 0–9 und Bindestrichen) beim Zuweisen von FQDNs für die Lync-Server, Edgeserver und Pools. Verwenden Sie keine Unicode-Zeichen oder Unterstriche. Andere als die genannten Zeichen in einem FQDN werden von externen DNS und öffentlichen Zertifizierungsstellen (wenn der FQDN dem SN im Zertifikat zugewiesen werden muss) häufig nicht unterstützt. Ausführliche Informationen zum Hinzufügen eines DNS-Suffixes zu einem Computernamen finden Sie unter Konfigurieren von DNS-Einträgen für die Edgeunterstützung.

   - Klicken Sie auf **Pool mit mehreren Computern** und dann auf **Weiter**.

6. Führen Sie unter **Funktionen auswählen** die folgenden Schritte aus:

   - Wenn ein einziger FQDN und eine einzige IP-Adresse für den SIP-Zugriffsdienst, den Lync Server-Webkonferenzdienst und den A/V-Edgedienst verwendet werden soll, aktivieren Sie das Kontrollkästchen **Einen FQDN und eine IP-Adresse verwenden**.

   - Wenn der Partnerverbund aktiviert werden soll, aktivieren Sie das Kontrollkästchen **Partnerverbund aktivieren (Port 5061)**.

     Hinweis:

Sie können diese Option auswählen, es kann jedoch nur ein Edgepool oder Edgeserver in Ihrer Organisation extern für den Partnerverbund veröffentlicht werden. Der Zugriff durch Partnerbenutzer, einschließlich Benutzer öffentlicher Sofortnachrichtendienste, erfolgt stets über denselben Edgepool oder einzelnen Edgeserver. Wenn Ihre Bereitstellung beispielsweise je einen Edgepool oder einzelnen Edgeserver in New York und in London umfasst und Sie die Unterstützung des Partnerverbunds für den Edgepool oder einzelnen Edgeserver in New York aktivieren, erfolgt der Signaldatenverkehr für Partnerbenutzer über den Edgepool oder einzelnen Edgeserver in New York. Dies gilt auch für die Kommunikation mit Benutzern in London, wenngleich ein interner Benutzer in London, der einen Partnerbenutzer in London anruft, für den A/V-Datenverkehr den Pool oder Edgeserver in London verwendet.

- Wenn Sie die Netzwerkadressenübersetzung (Network Address Translation, NAT) für Ihre öffentlichen IP-Adressen verwenden möchten, aktivieren Sie das Kontrollkästchen **Externe IP-Adresse dieses Edgepools von der NAT übersetzen**.

7. Klicken Sie auf **Weiter**.

8. Führen Sie in **Externe FQDNs** die folgenden Schritte aus:

   - Wenn Sie in **Funktionen auswählen** festlegen, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Edgedienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie in **SIP-Zugriff** den externen FQDN ein.

     Hinweis:
     Wenn Sie diese Option aktivieren, müssen Sie für jeden Edgedienst eine andere Portnummer angeben (die empfohlenen Porteinstellungen lauten: 5061 für den Zugriffs-Edgedienst, 444 für den Webkonferenz-Edgedienst und 443 für den A/V-Edgedienst). Durch Auswahl dieser Option können Sie potenzielle Konnektivitätsprobleme verhindern und die Konfiguration vereinfachen, indem Sie dieselbe Portnummer (z. B. 443) für alle drei Dienste verwenden.

   - Wenn Sie unter **Funktionen auswählen** nicht festgelegt haben, dass nur ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie den FQDN für die öffentliche Seite des Edgepools in **SIP-Zugriff** ein. Geben Sie in **Webkonferenzen** den FQDN ein, den Sie für die öffentliche Seite des Edgepools ausgewählt haben. Geben Sie in **Audio/Video** den FQDN ein, den Sie für die öffentliche Seite des Edgepools ausgewählt haben. Verwenden Sie die Standardports.

9. Klicken Sie auf **Weiter**.

10. Klicken Sie in **Computer in diesem Pool definieren** auf **Hinzufügen**.

11. Führen Sie in **Interner FQDN und interne IP-Adresse** die folgenden Schritte aus:

    - Geben Sie in **Interne IP-Adresse** die IP-Adresse des ersten Edgeservers ein, der in diesem Pool erstellt werden soll.

    - Geben Sie in **Interner FQDN** den FQDN des ersten Edgeservers ein, der in diesem Pool erstellt werden soll.

      Hinweis:
      Der angegebene Name muss mit dem auf dem Server konfigurierten Computernamen übereinstimmen. Der Name eines Computers, der nicht Mitglied einer Domäne ist, ist standardmäßig kein FQDN, sondern ein Kurzname. Der Topologie-Generator verwendet keine Kurznamen, sondern FQDNs. Sie müssen deshalb ein DNS-Suffix für den Namen des Computers konfigurieren, der als Edgeserver bereitgestellt werden soll und nicht Mitglied einer Domäne ist. Verwenden Sie nur Standardzeichen (einschließlich A–Z, a–z, 0–9 und Bindestrichen) beim Zuweisen von FQDNs für die Lync-Server, Edgeserver, Pools und Arrays. Verwenden Sie keine Unicode-Zeichen oder Unterstriche. Andere als die genannten Zeichen in einem FQDN werden von externen DNS und öffentlichen Zertifizierungsstellen (wenn der FQDN dem SN im Zertifikat zugewiesen werden muss) häufig nicht unterstützt. Ausführliche Informationen zum Hinzufügen eines DNS-Suffixes zu einem Computernamen finden Sie unter Konfigurieren von DNS-Einträgen für die Edgeunterstützung.

12. Klicken Sie auf **Weiter**.

13. Führen Sie in **Externe IP-Adressen definieren** die folgenden Schritte aus:

    - Wenn Sie festgelegt haben, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Edgedienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie in **SIP-Zugriff** die externe IP-Adresse des Edgeservers ein.

    - Wenn Sie nicht festgelegt haben, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Konferenzdienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie für **SIP-Zugriff** die IP-Adresse ein, die Sie für die öffentliche Seite dieses Edgepoolservers ausgewählt haben. Geben Sie in **Webkonferenzen** die IP-Adresse ein, die Sie für die öffentliche Seite des Edgepools ausgewählt haben. Geben Sie in **A/V-Konferenzen** die IP-Adresse ein, die Sie für die öffentliche Seite des Edgepools ausgewählt haben.

14. Klicken Sie auf **Fertig stellen**.

    Hinweis:
    Der erste Edgeserver, den Sie in Ihrem Pool erstellt haben, wird nun im Dialogfeld **Computer in diesem Pool definieren** angezeigt.

15. Klicken Sie in **Computer in diesem Pool definieren** auf **Hinzufügen**, und wiederholen Sie die Schritte 11 bis 14 für den zweiten Edgeserver, der dem Edgepool hinzugefügt werden soll.

16. Nachdem Sie die Schritte 11 bis 14 wiederholt haben, klicken Sie in **Computer in diesem Pool definieren** auf **Weiter**.

    Hinweis:
    Die beiden Edgeserver werden nun in Ihrem Pool angezeigt.

17. Wenn Sie die Verwendung der Netzwerkadressenübersetzung festgelegt haben, wird ein Dialogfeld angezeigt. Geben Sie in **Öffentliche IP-Adresse** die öffentliche IP-Adresse ein, die mithilfe der Netzwerkadressenübersetzung übersetzt werden soll, und klicken Sie anschließend auf **Weiter**.

    Hinweis:
    Dies sollte die externe IP-Adresse des AV-Edgedienst sein.

18. Wählen Sie in **Nächsten Hop definieren** in der Liste **Nächster Hoppool** den Namen des internen Pools aus, bei dem es sich entweder um einen Front-End-Pool oder um einen Standard Edition-Pool handeln kann. Oder, wenn Ihre Bereitstellung einen Director umfasst, wählen Sie den Namen des Directors aus. Klicken Sie anschließend auf **Weiter**.

19. Geben Sie in **Front-End-Pools zuordnen** einen oder mehrere interne Pools an (diese können Front-End-Pools und Standard Edition-Server umfassen), die diesem Edgeserver zugeordnet werden sollen. Wählen Sie dazu die Namen der internen Pools aus, die diesen Edgeserver für die Kommunikation mit unterstützten externen Benutzern verwenden.

    Hinweis:
    Jedem internen Pool kann für A/V-Datenverkehr nur ein Edgepool mit Lastenausgleich oder einzelner Edgeserver zugeordnet werden. Wenn einem internen Pool bereits ein Edgepool oder Edgeserver zugeordnet ist, werden Sie in einer Warnmeldung darüber informiert. Bei Auswahl eines Pools, der bereits einem anderen Edgeserver zugeordnet ist, wird die Zuordnung geändert.

20. Klicken Sie auf **Fertig stellen**.

21. Veröffentlichen Sie die Topologie.

Definieren der Topologie für einen Edgeserverpool mit Hardwarelastenausgleich

Sie müssen den Topologie-Generator zum Erstellen Ihrer Topologie verwenden und mindestens einen internen Front-End-Pool oder Standard Edition-Server einrichten, bevor Sie Ihre Edgeserver bereitstellen können. Verwenden Sie das folgende Verfahren, um Ihre Edgetopologie für einen Edgepool mit Hardwaregerät zum Lastenausgleich zu definieren, und anschließend die Verfahren in Veröffentlichen der Topologie und Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation, um die Topologie zu veröffentlichen und für Edgeserver zur Verfügung zu stellen.

Für eine erfolgreiche Veröffentlichung, Aktivierung oder Deaktivierung einer Topologie beim Hinzufügen oder Entfernen einer Serverrolle müssen Sie als Mitglied der Gruppen „RTCUniversalServerAdmins“ und „Domänen-Admins“ angemeldet sein. Es ist auch möglich, die geeigneten Administratorrechte und -berechtigungen für das Hinzufügen von Serverrollen zu delegieren. Ausführliche Informationen finden Sie unter „Delegieren von Setupberechtigungen“ in der Bereitstellungsdokumentation für Standard Edition-Server oder Enterprise Edition-Server. Für andere Konfigurationsänderungen müssen Sie lediglich Mitglied der Gruppe „RTCUniversalServerAdmins“ sein.

Wenn Sie Ihre Edgetopologie beim Definieren und Veröffentlichen Ihrer internen Topologie definiert haben und an der zuvor definierten Edgetopologie keine Änderungen erforderlich sind, müssen Sie die Topologie nicht erneut definieren und veröffentlichen. Folglich können Sie die folgende Vorgehensweise überspringen. Sie müssen die zuvor definierte und veröffentlichte Topologie jedoch für Ihre Edgeserver zur Verfügung stellen. Zu diesem Zweck führen Sie die Schritte unter Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation aus.

Wichtig:
Der Topologie-Generator kann nicht auf einem Edgeserver ausgeführt werden.
Der Topologie-Generator muss entweder auf Ihrem Front-End-Server oder auf Standard Edition-Servern ausgeführt werden.

So definieren Sie die Topologie für einen Edgeserverpool mit Hardwaregerät zum Lastenausgleich

1. Starten des Topologie-Generators: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Topologie-Generator**.
2. Erweitern Sie in der Konsolenstruktur den Standort, an dem Edgeserver bereitgestellt werden sollen.
3. Klicken Sie mit der rechten Maustaste auf **Edgepools**, und klicken Sie dann auf **Neuer Edgepool**.

4. Klicken Sie in **Neuen Edgepool definieren** auf **Weiter**.

5. Führen Sie in **FQDN des Edgepools definieren** die folgenden Schritte aus:

   - Geben Sie in **FQDN** den vollqualifizierten Domänennamen ein, den Sie für die interne Seite des Edgepools ausgewählt haben.

     Wichtig:
     Der angegebene Name muss mit dem auf dem Server konfigurierten Computernamen übereinstimmen. Der Name eines Computers, der nicht Mitglied einer Domäne ist, ist standardmäßig kein FQDN, sondern ein Kurzname. Der Topologie-Generator verwendet keine Kurznamen, sondern FQDNs. Sie müssen deshalb ein DNS-Suffix für den Namen des Computers konfigurieren, der als Edgeserver bereitgestellt werden soll und nicht Mitglied einer Domäne ist. Verwenden Sie nur Standardzeichen (einschließlich A–Z, a–z, 0–9 und Bindestrichen) beim Zuweisen von FQDNs für die Lync-Server, Edgeserver und Pools. Verwenden Sie keine Unicode-Zeichen oder Unterstriche. Andere als die genannten Zeichen in einem FQDN werden von externen DNS und öffentlichen Zertifizierungsstellen (wenn der FQDN dem SN im Zertifikat zugewiesen werden muss) häufig nicht unterstützt. Ausführliche Informationen zum Hinzufügen eines DNS-Suffixes zu einem Computernamen finden Sie unter Konfigurieren von DNS-Einträgen für die Edgeunterstützung.

   - Klicken Sie auf **Pool mit mehreren Computern** und dann auf **Weiter**.

6. Führen Sie unter **Funktionen auswählen** die folgenden Schritte aus:

   - Wenn ein einziger FQDN und eine einzige IP-Adresse für den SIP-Zugriffsdienst, den Lync Server-Webkonferenzdienst und den A/V-Edgedienst verwendet werden soll, aktivieren Sie das Kontrollkästchen **Einen FQDN und eine IP-Adresse verwenden**.

   - Wenn der Partnerverbund aktiviert werden soll, aktivieren Sie das Kontrollkästchen **Partnerverbund aktivieren (Port 5061)**.

     Hinweis:
     Sie können diese Option auswählen, es kann jedoch nur ein Edgepool oder Edgeserver in Ihrer Organisation extern für den Partnerverbund veröffentlicht werden. Der Zugriff durch Partnerbenutzer, einschließlich Benutzer öffentlicher Sofortnachrichtendienste, erfolgt stets über denselben Edgepool oder einzelnen Edgeserver. Wenn Ihre Bereitstellung beispielsweise je einen Edgepool oder einzelnen Edgeserver in New York und in London umfasst und

Sie die Unterstützung des Partnerverbunds für den Edgepool oder einzelnen Edgeserver in New York aktivieren, erfolgt der Signaldatenverkehr für Partnerbenutzer über den Edgepool oder einzelnen Edgeserver in New York. Dies gilt auch für die Kommunikation mit Benutzern in London, wenngleich ein interner Benutzer in London, der einen Partnerbenutzer in London anruft, für den A/V-Datenverkehr den Pool oder Edgeserver in London verwendet.

Wichtig:
Aktivieren Sie **nicht** das Kontrollkästchen **Externe IP-Adresse dieses Edgepools von der NAT übersetzen**. Die Netzwerkadressenübersetzung wird bei Verwendung eines Hardwaregeräts zum Lastenausgleich nicht unterstützt.

7. Klicken Sie auf **Weiter**.

8. Führen Sie in **Externe FQDNs** die folgenden Schritte aus:

   - Wenn Sie in **Funktionen auswählen** festlegen, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Edgedienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie in **SIP-Zugriff** den externen FQDN ein.

     Hinweis:
     Wenn Sie diese Option aktivieren, müssen Sie für jeden Edgedienst eine andere Portnummer angeben (die empfohlenen Porteinstellungen lauten: 5061 für den Zugriffs-Edgedienst, 444 für den Webkonferenz-Edgedienst und 443 für den A/V-Edgedienst). Durch Auswahl dieser Option können Sie potenzielle Konnektivitätsprobleme verhindern und die Konfiguration vereinfachen, indem Sie dieselbe Portnummer (z. B. 443) für alle drei Dienste verwenden.

   - Wenn Sie unter **Funktionen auswählen** nicht festgelegt haben, dass nur ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie den FQDN für die öffentliche Seite des Edgepools in **SIP-Zugriff** ein. Geben Sie in **Webkonferenzen** den FQDN ein, den Sie für die öffentliche Seite des Edgepools ausgewählt haben. Geben Sie in **Audio/Video** den FQDN ein, den Sie für die öffentliche Seite des Edgepools ausgewählt haben. Verwenden Sie die Standardports.

     Hinweis:
     Dabei handelt es sich um die FQDNs der virtuellen IP-Adressen (VIP) für die öffentliche Seite des Pools.

9. Klicken Sie auf **Weiter**.

10. Klicken Sie in **Computer in diesem Pool definieren** auf **Hinzufügen**.

11. Führen Sie in **Interner FQDN und interne IP-Adresse** die folgenden Schritte aus:

    - Geben Sie in **Interne IP-Adresse** die IP-Adresse des ersten Edgeservers ein, der in diesem Pool erstellt werden soll.

    - Geben Sie in **Interner FQDN** den FQDN des ersten Edgeservers ein, der in diesem Pool erstellt werden soll.

      Hinweis:
      Der angegebene Name muss mit dem auf dem Server konfigurierten Computernamen übereinstimmen. Der Name eines Computers, der nicht Mitglied einer Domäne ist, ist standardmäßig kein FQDN, sondern ein Kurzname. Der Topologie-Generator verwendet keine Kurznamen, sondern FQDNs. Sie müssen deshalb ein DNS-Suffix für den Namen des Computers konfigurieren, der als Edgeserver bereitgestellt werden soll und nicht Mitglied einer Domäne ist. Ausführliche Informationen zum Hinzufügen eines DNS-Suffixes zu einem Computernamen finden Sie unter Konfigurieren von DNS-Einträgen für die Edgeunterstützung.

12. Klicken Sie auf **Weiter**.

13. Führen Sie in **Externe IP-Adressen definieren** die folgenden Schritte aus:

    - Wenn Sie festgelegt haben, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Edgedienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie in **SIP-Zugriff** die externe IP-Adresse des Edgeservers ein.

    - Wenn Sie nicht festgelegt haben, dass für den SIP-Zugriff, den Webkonferenzdienst und den A/V-Konferenzdienst ein einziger FQDN und eine einzige IP-Adresse verwendet werden soll, geben Sie für **SIP-Zugriff** die IP-Adresse ein, die Sie für die öffentliche Seite dieses Edgepoolservers ausgewählt haben. Geben Sie in **Webkonferenzen** die IP-Adresse ein, die Sie für die öffentliche Seite des Edgepools ausgewählt haben. Geben Sie in **A/V-Konferenzen** die IP-Adresse ein, die Sie für die öffentliche Seite des Edgepools ausgewählt haben.

14. Klicken Sie auf **Fertig stellen**.

    Hinweis:
    Der erste Edgeserver, den Sie in Ihrem Pool erstellt haben, wird nun im Dialogfeld **Computer in diesem Pool definieren** angezeigt.

15. Klicken Sie in **Computer in diesem Pool definieren** auf **Hinzufügen**, und wiederholen Sie die Schritte 11 bis 14 für den zweiten Edgeserver, der dem Edgepool hinzugefügt werden soll.

16. Nachdem Sie die Schritte 11 bis 14 wiederholt haben, klicken Sie in **Computer in diesem Pool definieren** auf **Weiter**.

    Hinweis:
    Die beiden Edgeserver werden nun in Ihrem Pool angezeigt.

17. Wählen Sie in **Nächsten Hop definieren** in der Liste **Nächster Hoppool** den Namen des internen Pools aus, bei dem es sich entweder um einen Front-End-Pool oder um einen Standard Edition-Pool handeln kann. Oder, wenn Ihre Bereitstellung einen Director umfasst, wählen Sie den Namen des Directors aus. Klicken Sie anschließend auf **Weiter**.

18. Geben Sie in **Front-End-Pools zuordnen** einen oder mehrere interne Pools an (diese können Front-End-Pools und Standard Edition-Server umfassen), die diesem Edgeserver zugeordnet werden sollen. Wählen Sie dazu die Namen der internen Pools aus, die diesen Edgeserver für die Kommunikation mit unterstützten externen Benutzern verwenden.

    Hinweis:
    Jedem internen Pool kann für A/V-Datenverkehr nur ein Edgepool mit Lastenausgleich oder einzelner Edgeserver zugeordnet werden. Wenn einem internen Pool bereits ein Edgepool oder Edgeserver zugeordnet ist, werden Sie in einer Warnmeldung darüber informiert. Bei Auswahl eines Pools, der bereits einem anderen Edgeserver zugeordnet ist, wird die Zuordnung geändert.

19. Klicken Sie auf **Fertig stellen**.

20. Veröffentlichen Sie die Topologie.

Veröffentlichen der Topologie

Jedes Mal, wenn Sie den Topologie-Generator zum Erstellen einer Topologie verwenden, müssen Sie die Topologie in einer Datenbank im zentralen Verwaltungsspeicher veröffentlichen, sodass die Daten für die Bereitstellung von Lync Server 2010 verwendet werden können. Führen Sie die folgenden Schritte aus, um Ihre Topologie zu veröffentlichen.

So veröffentlichen Sie die Topologie

1. Starten des Topologie-Generators: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Topologie-Generator**.

2. Klicken Sie im Topologie-Generator in der Konsolenstruktur mit der rechten Maustaste auf **Lync Server 2010**, und klicken Sie dann auf **Topologie veröffentlichen**.

3. Klicken Sie auf der Seite **Willkommen** des Assistenten auf **Weiter**.

4. Klicken Sie auf der Seite **Topologie-Generator hat einen zentralen Verwaltungsspeicher gefunden** auf **Weiter**.

5. Klicken Sie auf der Seite **Weitere Datenbanken erstellen** auf **Weiter**.

6. Wenn die erfolgreiche Erstellung der Datenbank angezeigt wird, führen Sie folgende Schritte aus:

    - Klicken Sie zum Anzeigen des Protokolls auf **Protokoll anzeigen**.

    - Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Einrichten des Directors

Wenn Sie den Zugriff durch externe Benutzer über die Bereitstellung von Edgeservern aktivieren, sollten Sie auch einen Director bereitstellen. Ein Director ist ein Server mit Microsoft Lync Server 2010, der Benutzeranforderungen authentifiziert, jedoch keine Benutzerkonten verwaltet. Die grundlegenden Schritte zum Einrichten eines Directors oder Directorpools ähneln denen bei der Einrichtung eines Enterprise Edition-Front-End-Pools oder Standard Edition-Servers. Nachdem Sie einen Director (oder mehrere) im Topologie-Generator definiert haben, müssen Sie die in diesem Abschnitt genannten Schritte ausführen.

Inhalt dieses Abschnitts

- Installieren des lokalen Konfigurationsspeichers
- Installieren von Lync Server 2010 auf dem Director
- Konfigurieren von Zertifikaten für den Director
- Starten von Diensten auf dem Director
- Testen des Directors
- Konfigurieren der automatischen Clientanmeldung zur Verwendung des Directors

Installieren des lokalen Konfigurationsspeichers

Zum erfolgreichen Durchführen dieses Verfahrens müssen Sie mindestens als lokaler Administrator am Server angemeldet sein und ein Domänenbenutzerkonto verwenden, das mindestens Mitglied der Gruppe „RTCUniversalReadOnlyAdmins“ ist.

Der erste Schritt im Lync Server-Bereitstellungs-Assistent ist die Installation des lokalen Konfigurationsspeichers. Als lokaler Konfigurationsspeicher dient SQL Server Express.

Das Programm installiert eine lokale Datenbank, in der eine schreibgeschützte Kopie des zentralen Verwaltungsspeichers gespeichert wird. Der vorhandenen SQL Server-Datenbank, die in der auf Standard Edition-Server SQL Server Express basierenden Datenbank gespeichert ist, müssen Sie den zentralen Verwaltungsspeicher hinzufügen.

Wichtig:
Wenn Sie Microsoft Lync Server 2010-Setup zum ersten Mal auf diesem Server ausgeführt haben, werden Sie zur Eingabe eines Laufwerks und Pfads zum Installieren von Lync Server 2010 aufgefordert. Wenn sich in Ihrer Organisation Internetinformationsdienste (Internet Information Services, IIS) und alle Webdienste auf einem anderen als dem Systemlaufwerk befinden müssen, können Sie den Installationspfad für die Lync Server-Dateien im Dialogfeld „Setup“ ändern. Für den Fall, dass Sie die Setupdateien in diesem Pfad installieren, einschließlich „OCSCore.msi“, werden die restlichen Dateien für Lync Server 2010 ebenfalls auf diesem Laufwerk installiert.

So installieren Sie den lokalen Konfigurationsspeicher

1. Wechseln Sie auf dem Installationsdatenträger zu „\setup\amd64\Setup.exe“, und klicken Sie dann auf **OK**.
2. Klicken Sie auf **Ja**, wenn Sie zur Installation von Microsoft Visual C++ 2008 Distributable aufgefordert werden.
3. Klicken Sie auf der Seite **Installationsspeicherort von Lync Server 2010** auf **OK**.
4. Lesen Sie sich auf der Seite **Endbenutzer-Lizenzvertrag** die Lizenzbedingungen durch, klicken Sie auf **Ich stimme den Bedingungen des Lizenzvertrags zu**, und klicken Sie auf **OK**. Dieser Schritt ist erforderlich, um den Vorgang fortsetzen zu können.
5. Klicken Sie im Bereitstellungs-Assistenten auf **Lync Server-System installieren oder aktualisieren**.
6. Klicken Sie auf der Seite **Lync Server 2010** neben **Schritt 1: Lokalen Konfigurationsspeicher installieren** auf **Ausführen**.
7. Vergewissern Sie sich auf der Seite **Lokale Serverkonfiguration**, dass die Option **Konfiguration automatisch aus dem zentralen Verwaltungsspeicher abrufen** ausgewählt ist, und klicken Sie dann auf **Weiter**.
8. Klicken Sie nach Abschluss der Installation der lokalen Serverkonfiguration auf **Fertig stellen**.

Installieren von Lync Server 2010 auf dem Director

Führen Sie die folgenden Schritte aus, um die Lync Server 2010-Komponenten auf einem Director zu installieren.

So installieren Sie Lync Server-Komponenten auf einem Director

1. Klicken Sie im Lync Server-Bereitstellungs-Assistenten auf der Lync Server 2010-Seite neben **Schritt 2: Lync Server-Komponenten einrichten oder entfernen** auf **Ausführen**.
2. Klicken Sie auf der Seite **Lync Server-Komponenten einrichten** auf **Weiter**, um die Komponenten gemäß Definition in der veröffentlichten Topologie einzurichten.
3. Klicken Sie nach Abschluss der Lync Server-Komponenteneinrichtung auf **Fertig stellen**.

Konfigurieren von Zertifikaten für den Director

Für jeden Director wird ein Standardzertifikat, ein internes Webzertifikat und ein externes Webzertifikat benötigt. Ausführliche Informationen zu den Zertifikatanforderungen für Director-Server finden Sie unter „Anforderungen an Zertifikate für interne Server“ in der Planungsdokumentation.

Verwenden Sie das folgende Verfahren, um Director-Zertifikate zu konfigurieren. Wiederholen Sie das Verfahren für jeden Director. Die Schritte in diesem Verfahren beschreiben, wie Sie ein Zertifikat einer internen Stammzertifizierungsstelle konfigurieren, die in Ihrem Unternehmen eingesetzt wird. Zertifikatsanforderungen werden in diesem Verfahren offline verarbeitet. Ausführliche Informationen zum Anfordern von Zertifikaten bei einer externen Zertifizierungsstelle erhalten Sie von Ihrem Supportteam.

So konfigurieren Sie Zertifikate für den Director oder Directorpool

1. Klicken Sie im Lync Server-Bereitstellungs-Assistenten neben **Schritt 3: Zertifikate anfordern, installieren oder zuweisen** auf **Ausführen**.
2. Klicken Sie auf der Seite **Zertifikat-Assistent** auf **Anfordern**.
3. Klicken Sie auf der Seite **Zertifikatsanforderung** auf **Weiter**.
4. Akzeptieren Sie auf der Seite **Verzögerte oder sofortige Anforderungen** die Standardeinstellung **Anforderung unmittelbar an eine Onlinezertifizierungsstelle senden**, und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite **Zertifizierungsstelle auswählen** auf die interne Windows-Zertifizierungsstelle, die Sie verwenden möchten, und klicken Sie dann auf **Weiter**.

6. Geben Sie auf der Seite **Zertifizierungsstellenkonto** alternative Anmeldeinformationen für den Fall an, dass das zur Anmeldung verwendete Konto keine ausreichenden Berechtigungen zum Anfordern des Zertifikats besitzt, und klicken Sie anschließend auf **Weiter**.
7. Klicken Sie auf der Seite **Alternative Zertifikatvorlage angeben** auf **Weiter**.
8. Geben Sie auf der Seite **Namens- und Sicherheitseinstellungen** einen Wert für **Anzeigename** ein, akzeptieren Sie die Schlüssellänge von 2.048 Bit, und klicken Sie auf **Weiter**.
9. Überprüfen Sie optional die Informationen auf der Seite **Organisationsinformationen**, und klicken Sie anschließend auf **Weiter**.
10. Überprüfen Sie optional die Informationen auf der Seite **Geographische Informationen**, und klicken Sie anschließend auf **Weiter**.
11. Klicken Sie auf der Seite **Antragstellername/Alternative Antragstellernamen** auf **Weiter**.

    Hinweis:
    Die Liste der alternativen Antragstellernamen sollte den Namen des Computers enthalten, auf dem Sie den Director installieren (falls nur ein Director vorhanden ist), andernfalls den Namen des Directorpools und die Namen der einfachen URLs, die für die Organisation konfiguriert wurden.

12. Wählen Sie auf der Seite **SIP-Domäneneinstellung** die Option **Konfigurierte SIP-Domänen** für alle Domänen aus, die der Director verarbeiten soll, und klicken Sie dann auf **Weiter**.
13. Geben Sie auf der Seite **Weitere alternative Antragstellernamen konfigurieren** zusätzlich erforderliche alternative Antragstellernamen an, und klicken Sie auf **Weiter**.
14. Klicken Sie auf der Seite **Zusammenfassung über Zertifikatsanforderungen** auf **Weiter**.
15. Klicken Sie auf der Seite **Befehle werden ausgeführt** nach Abschluss der Befehlsausführung auf **Weiter**.
16. Klicken Sie auf der Seite **Status der Onlinezertifikatsanforderung** auf **Fertig stellen**.
17. Klicken Sie auf der Seite **Zertifikatzuweisung** auf **Weiter**.

    Hinweis:
    Wenn Sie das Zertifikat anzeigen möchten, doppelklicken Sie auf das Zertifikat in der Liste.

18. Klicken Sie auf der Seite **Zusammenfassung der Zertifikatzuweisung** auf **Weiter**.
19. Klicken Sie auf der Seite **Befehle werden ausgeführt** nach Abschluss der Befehlsausführung auf **Fertig stellen**.
20. Klicken Sie auf der Seite **Zertifikat-Assistent** auf **Schließen**.

Starten von Diensten auf dem Director

Nachdem Sie den lokalen Konfigurationsspeicher und die Lync Server-Komponenten installiert und Zertifikate auf einem Director konfiguriert haben, müssen Sie die Lync Server-Dienste auf dem Server starten. Verwenden Sie das folgende Verfahren, um die Dienste auf jedem Director in Ihrer Umgebung zu starten.

So starten Sie Dienste auf einem Director

1. Klicken Sie im Lync Server-Bereitstellungs-Assistenten auf der Seite **Lync Server 2010** auf die Schaltfläche **Ausführen** neben **Schritt 4: Dienste starten**.
2. Klicken Sie auf der Seite **Dienste starten** auf **Weiter**, um die Lync Server-Dienste auf dem Server zu starten.
3. Klicken Sie nach dem erfolgreichen Start aller Dienste auf der Seite **Befehle werden ausgeführt** auf **Fertig stellen**.
4. Klicken Sie unterhalb von **Schritt 4: Dienste starten** auf **Dienststatus (optional)**.
5. Überprüfen Sie mithilfe der MMC-Konsole **Dienste** auf dem Server, ob alle Lync Server 2010-Dienste ausgeführt werden.

Testen des Directors

Zu diesem Zeitpunkt haben Sie einen Director oder einen Directorpool konfiguriert, Ihre DNS-SRV-Einträge (Domain Name System) verweisen Clients jedoch noch immer an die Anmeldung über einen Pool- oder einen Standard Edition-Server. Bevor Sie den DNS-Eintrag so ändern, dass Microsoft Lync 2010-Clients sich automatisch über den Director anmelden, testen Sie einen Client, indem sie ihn manuell an den Director verweisen.

So testen Sie die Bereitstellung

1. Melden Sie sich an dem Computer an, auf dem Sie die Lync Server-Systemsteuerung mit einem Domänenkonto installiert haben, das der Gruppe **CSAdministrator** angehört.
2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

Klicken Sie im Navigationsbereich auf **Topologie**, und vergewissern Sie sich, dass in der Spalte **Status** ein grüner Server mit einem Pfeil () für Ihren Director oder Directorpool angezeigt wird.

4. Stellen Sie eine Verbindung auf zwei Computern her, auf denen der Lync Server 2010-Client installiert ist, und melden Sie sich an jedem Computer mit einem anderen Benutzerkonto an, das für Lync Server 2010 aktiviert ist.

5. Klicken Sie auf einem der Clientcomputer im Menü **Optionen** auf die Einstellungsgruppe **Persönlich**, klicken Sie auf **Erweitert**, dann auf **Manuelle Konfiguration**, und legen Sie dann die Option **Interner Servername oder IP-Adresse** auf den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des neuen Directors oder Directorpools fest.

6. Melden Sie sich an beiden Clients an, und stellen Sie sicher, dass die Anmeldung auf dem Client, der sich über den Director anmeldet, erfolgreich verläuft. Beachten Sie den Anwesenheitsstatus des anderen Benutzers, und prüfen Sie, ob beide Sofortnachrichten austauschen können.

Konfigurieren der automatischen Clientanmeldung zur Verwendung des Directors

Wenn Sie einen Microsoft Lync Server 2010-Director oder -Directorpool bereitstellen, wird die Verwendung der automatischen Clientanmeldung empfohlen. Ausführliche Informationen zur Konfiguration von DNS-Servern für die automatische Clientanmeldung finden Sie unter „DNS-Anforderungen für die automatische Clientanmeldung“ in der Planungsdokumentation.

Wenn Sie die automatische Clientanmeldung bereits bereitgestellt haben, finden Sie in den folgenden Abschnitten Informationen zur Konfiguration dieser Funktion für Ihre Director-Server.

Einzelne Director-Instanz

Wenn Sie die automatische Clientanmeldung bereits bereitgestellt haben und diese auf einen Standard Edition-Server in einem Front-End-Pool der Enterprise Edition zeigt, müssen Sie den DNS-SRV-Eintrag so ändern, dass dieser auf den Director zeigt.

Directorpool

Wenn Sie die automatische Clientanmeldung bereits bereitgestellt haben und diese auf einen Standard Edition-Server in einem Front-End-Pool der Enterprise Edition zeigt, müssen Sie den DNS-SRV-Eintrag so ändern, dass dieser auf den Directorpool zeigt.

Einrichten von Edgeservern

Die Aufgaben zum Einrichten von Edgeservern entsprechen grundsätzlich denen zum Installieren eines einzelnen Edgeservers oder eines Edgeserverpools mit Lastenausgleich. Bei einem Pool von Edgeservern mit Lastenausgleich müssen jedoch zusätzlich die Lastenausgleichsmodule bereitgestellt und weitere Schritte ausgeführt werden, um die Einrichtung auf mehrere Edgeserver zu replizieren.

Inhalt dieses Abschnitts

- Einrichten von Netzwerkschnittstellen für Edgeserver
- Installieren der erforderlichen Software auf Edgeservern
- Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation
- Installieren von Edgeservern
- Einrichten von Edgezertifikaten
- Starten der Edgeserver
- Einrichten von Reverseproxyservern

Einrichten von Netzwerkschnittstellen für Edgeserver

Bei jedem Edgeserver handelt es sich um einen mehrfach vernetzten Computer mit externen und internen Schnittstellen. Die DNS-Einstellungen (Domain Name System) des Netzwerkadapters richten sich danach, ob im Umkreisnetzwerk DNS-Server vorhanden sind. Wenn im Umkreisnetzwerk DNS-Server vorhanden sind, müssen diese über eine Zone mit mindestens einem DNS-A-Eintrag für den Server oder Pool für den nächsten Hop verfügen (hierbei handelt es sich entweder um einen Director oder einen festgelegten Front-End-Pool). Für externe Abfragen werden Namelookups über andere öffentliche DNS-Server durchgeführt. Wenn im Umkreisnetzwerk keine DNS-Server vorhanden sind, verwenden der oder die Edgeserver externe DNS-Server zur Durchführung von Namelookups im Internet, und jeder Edgeserver verwendet eine HOST-Datei, um die Namen der Server für den nächsten Hop in IP-Adressen aufzulösen.

noteDSDOC112778PADS Sicherheitshinweis

Aus Sicherheitsgründen wird empfohlen, dass die Edgeserver nicht auf einen DNS-Server zugreifen können, der sich im internen Netzwerk befindet.

So konfigurieren Sie Schnittstellen mit DNS-Servern im Umkreisnetzwerk

1. Installieren Sie zwei Netzwerkadapter für jeden Edgeserver, einen für die interne und einen für die externe Schnittstelle.

Wichtig:
Ein Routing vom internen Subnetz zum externen Subnetz (und umgekehrt) darf nicht möglich sein.

2. Konfigurieren Sie für die externe Schnittstelle drei statische IP-Adressen im externen Subnetz des Umkreisnetzwerks (auch als überwachtes Subnetz bezeichnet), und verweisen Sie das Standardgateway auf die interne Schnittstelle der externen Firewall. Konfigurieren Sie die DNS-Einstellungen des Netzwerkadapters, sodass diese auf ein DNS-Umkreisserverpaar verweisen.

   Hinweis:
   Es ist möglich, für diese Schnittstelle nur eine einzige IP-Adresse zu verwenden, hierfür müssen Sie allerdings die Portzuweisungen in nicht standardmäßige Werte ändern. Dies wird beim Erstellen der Topologie im Topologie-Generator festgelegt.

3. Konfigurieren Sie in der internen Schnittstelle eine statische IP-Adresse im internen Subnetz des Umkreisnetzwerks, und geben Sie kein Standardgateway an. Konfigurieren Sie die DNS-Einstellungen des Netzwerkadapters, sodass diese mindestens auf einen DNS-Server, jedoch vorzugsweise auf ein DNS-Umkreisserverpaar verweisen.

4. Erstellen Sie in der internen Schnittstelle beständige statische Routen zu allen internen Netzwerken, in denen sich Clients, Server mit Lync Server 2010 und Exchange UM-Server befinden.

So konfigurieren Sie Schnittstellen ohne DNS-Server im Umkreisnetzwerk

1. Installieren Sie zwei Netzwerkadapter für jeden Edgeserver, einen für die interne und einen für die externe Schnittstelle.

   Wichtig:
   Ein Routing vom internen Subnetz zum externen Subnetz (und umgekehrt) darf nicht möglich sein.

2. Konfigurieren Sie in der externen Schnittstelle drei statische IP-Adressen im externen Subnetz des Umkreisnetzwerks, und verweisen Sie das Standardgateway auf die interne Schnittstelle der externen Firewall. Konfigurieren Sie die DNS-Einstellungen des Netzwerkadapters, sodass diese mindestens auf einen DNS-Server, jedoch vorzugsweise auf ein externes DNS-Serverpaar verweisen.

   Hinweis:
   Es ist möglich, für diese Schnittstelle nur eine einzige IP-Adresse zu verwenden,

hierfür müssen Sie allerdings die Portzuweisungen in nicht standardmäßige Werte ändern. Dies wird beim Erstellen der Topologie im Topologie-Generator festgelegt.

3. Konfigurieren Sie in der internen Schnittstelle eine statische IP-Adresse im internen Subnetz des Umkreisnetzwerks, und geben Sie kein Standardgateway an. Lassen Sie die DNS-Einstellungen des Netzwerkadapters leer.

4. Erstellen Sie in der internen Schnittstelle beständige statische Routen zu allen internen Netzwerken, in denen sich Clients oder Server mit Lync Server 2010 befinden.

5. Fügen Sie einen Eintrag für den Server für den nächsten Hop oder eine virtuelle IP (VIP) in die HOST-Datei auf jedem Edgeserver ein (bei diesem Eintrag handelt es sich um einen Director, Standard Edition-Server oder Front-End-Pool, der im Topologie-Generator als Adresse für den nächsten Hop des Edgeservers konfiguriert wurde). Wenn Sie den DNS-Lastenausgleich verwenden, fügen Sie eine Zeile für jedes Mitglied im Pool für den nächsten Hop ein.

Installieren der erforderlichen Software auf Edgeservern

Vor der Installation von Lync Server 2010 müssen Sie auf jedem Edgeserver, den Sie bereitstellen, erforderliche Softwarekomponenten installieren. Dies umfasst die Installation des Betriebssystems auf einem Server, der die Systemanforderungen erfüllt. Ausführliche Informationen zu den Systemanforderungen, einschließlich der unterstützten Betriebssysteme, finden Sie unter Systemanforderungen für Edgekomponenten.

Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation

Nachdem Sie Ihre Topologie veröffentlicht haben, benötigt der Lync Server-Bereitstellungs-Assistent Zugriff auf die Dateien im zentralen Verwaltungsspeicher, um den Bereitstellungsprozess auf dem Server zu starten. Im internen Netzwerk kann direkt von den Servern auf die Daten zugegriffen werden, jedoch haben Edgeserver, die sich nicht in der internen Domäne befinden, keinen Zugriff auf die Daten. Um die Daten der Topologiekonfiguration für eine Edgeserverbereitstellung verfügbar zu machen, müssen Sie die Topologiedaten in eine Datei exportieren und diese auf einen externen Datenträger kopieren (dies kann z. B. ein USB-Laufwerk oder eine Netzwerkfreigabe sein, das bzw. die vom Edgeserver aus zugänglich ist), bevor Sie den Lync Server-Bereitstellungs-Assistenten auf dem Edgeserver ausführen. Verwenden Sie das folgende Verfahren, um die Daten der Topologiekonfiguration für den bereitzustellenden Edgeserver verfügbar zu machen.

Hinweis:
Nachdem Sie Lync Server 2010 auf einem Edgeserver installiert haben, können Sie den Edgeserver unter Verwendung der Verwaltungstools im internen Netzwerk verwalten. So wird die Konfiguration automatisch auf jeden bereitgestellten Edgeserver repliziert. Die einzigen Aufgaben, die auf dem Edgeserver ausgeführt werden müssen, sind das Zuweisen und Installieren von Zertifikaten sowie das Beenden und Starten von Diensten.

So stellen Sie Ihre Topologiedaten mithilfe der Lync Server-Verwaltungsshell auf einem Edgeserver zur Verfügung

1. Starten der Lync Server-Verwaltungsshell: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Verwaltungsshell**.
2. Führen Sie in der Lync Server-Verwaltungsshell das folgende Cmdlet aus:

   ```
   Export-CsConfiguration -FileName <ConfigurationFilePath.zip>
   ```
3. Kopieren Sie die exportierte Datei auf einen externen Datenträger (z. B. auf ein USB-Laufwerk oder eine Netzwerkfreigabe, das bzw. die während der Bereitstellung für den Edgeserver zugänglich ist).

Installieren von Edgeservern

Lync Server 2010 installieren Sie auf Edgeservern mithilfe des Lync Server-Bereitstellungs-Assistenten. Durch Ausführung des Bereitstellungs-Assistenten auf jedem Edgeserver können Sie die meisten Aufgaben ausführen, die zur Einrichtung des Edgeservers erforderlich sind. Zur Bereitstellung von Lync Server 2010 auf einem Edgeserver müssen Sie bereits den Topologie-Generator ausgeführt haben, um Ihre Edgeservertopologie zu definieren und zu veröffentlichen, und Sie müssen die Topologie auf Medien kopiert haben, auf die vom Edgeserver aus zugegriffen werden kann. Ausführliche Informationen finden Sie unter „Topologien für den Zugriff durch externe Benutzer“ und Exportieren der Topologie und Kopieren auf externe Medien zur Edgeinstallation.

Wenn Sie alle Edgeserver mit dem Bereitstellungs-Assistenten installiert und die erforderlichen Zertifikate installiert und zugewiesen haben, können Sie das Setup mithilfe der Informationen unter Konfigurieren der Unterstützung für den externen Benutzerzugriff dazu verwenden, den externen Benutzerzugriff zu aktivieren und zu konfigurieren. Mithilfe der Informationen unter Überprüfen der Edgebereitstellung können Sie das Setup einschließlich Server- und Clientkonnektivität überprüfen.

So installieren Sie einen Edgeserver

1. Melden Sie sich als Mitglied der lokalen Administratorgruppe an dem Computer an, auf dem Sie den Edgeserver installieren möchten, oder verwenden Sie ein Konto mit gleichwertigen Benutzerrechten und -berechtigungen.

2. Stellen Sie sicher, dass die Topologiekonfigurationsdatei, die Sie mit dem Topologie-Generator erstellt und auf externe Medien kopiert haben, auf dem Edgeserver verfügbar ist (schließen Sie beispielsweise das USB-Laufwerk, auf das Sie die Topologiekonfigurationsdatei kopiert haben, an den Edgeserver an, oder gewähren Sie Zugriff auf die Netzwerkfreigabe, auf die die Datei kopiert wurde).

3. Starten Sie den Bereitstellungs-Assistenten.

   Hinweis:
   Wenn Sie in einer Meldung dazu aufgefordert werden, Microsoft Visual C++ Redistributable zu installieren, klicken Sie auf **Ja**. Im nächsten Dialogfeld können Sie den vorgegebenen **Installationsspeicherort** akzeptieren oder auf **Durchsuchen** klicken, um einen alternativen Speicherort anzugeben. Klicken Sie anschließend auf **Installieren**. Aktivieren Sie im nächsten Dialogfeld das Kontrollkästchen **Ich stimme den Bedingungen des Lizenzvertrags zu**, und klicken Sie auf **OK**.

4. Klicken Sie im Bereitstellungs-Assistenten auf **Lync Server-System installieren oder aktualisieren**.

5. Klicken Sie nach Abschluss der Bereitstellungsphase durch den Assistenten unter **Schritt 1. Lokalen Konfigurationsspeicher installieren** auf **Ausführen**, und führen Sie die folgenden Schritte aus:

   - Klicken Sie im Dialogfeld **Lokales Replikat des zentralen Verwaltungsspeichers konfigurieren** auf **Aus Datei importieren (empfohlen für Edgeserver)**, wechseln Sie zum Speicherort der exportierten Topologiekonfigurationsdatei, wählen Sie die ZIP-Datei aus, klicken Sie auf **Öffnen** und anschließend auf **Weiter**.
   - Der Bereitstellungs-Assistent liest die Konfigurationsinformationen aus der Konfigurationsdatei aus und schreibt die XML-Konfigurationsdatei auf den lokalen Computer.
   - Nachdem der Prozess **Befehle werden ausgeführt** abgeschlossen wurde, klicken Sie auf **Fertig stellen**.

6. Klicken Sie im Bereitstellungs-Assistenten auf **Schritt 2: Lync Server-Komponenten einrichten oder entfernen**, um die Lync Server-Edgekomponenten zu installieren, die in der lokal gespeicherten XML-Konfigurationsdatei angegeben sind.

7. Verwenden Sie nach Abschluss der Installation die Informationen unter Einrichten von Edgezertifikaten, um vor dem Start der Dienste die erforderlichen Zertifikate zu installieren und zuzuweisen.

Einrichten von Edgezertifikaten

Wenn Sie einen Edgeserver installieren, müssen Sie die erforderlichen Zertifikate für die externen und internen Schnittstellen anfordern, installieren und zuweisen.

Inhalt dieses Abschnitts

- Zertifikatanforderungen für den externen Benutzerzugriff
- Einrichten der Zertifikate für die interne Edgeschnittstelle
- Einrichten der Zertifikate für die externe Edgeschnittstelle
- Einrichten der Zertifikate für den Reverseproxy

Zertifikatanforderungen für den externen Benutzerzugriff

Die Microsoft Lync Server 2010-Kommunikationssoftware unterstützt die Verwendung eines einzelnen öffentlichen Zertifikats für die externen Edgeschnittstellen für Zugriff und Webkonferenzen sowie für die interne Edgeschnittstelle für die A/V-Authentifizierung. Für die interne Edgeschnittstelle wird üblicherweise ein von einer internen Zertifizierungsstelle ausgestelltes privates Zertifikat verwendet, es kann jedoch auch ein öffentliches Zertifikat verwendet werden, wenn dieses von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle stammt.
Der Reverseproxy in Ihrer Bereitstellung verschlüsselt mithilfe eines öffentlichen Zertifikats die Kommunikation vom Reverseproxy zu Clients und vom Reverseproxy zu internen Servern mit HTTP (d. h. Transport Layer Security über HTTP).

Im Folgenden finden Sie die Anforderungen für das öffentliche Zertifikat, das für die externen Edgeschnittstellen für Zugriff und Webkonferenzen sowie für die interne Edgeschnittstelle für die A/V-Authentifizierung verwendet wird:

- Das Zertifikat muss von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle ausgestellt werden, die alternative Antragstellernamen unterstützt. Ausführliche Informationen finden Sie im Microsoft Knowledge Base-Artikel 929395, „Partner für Unified Communications-Zertifikate für Exchange Server und Communications Server“, unter http://go.microsoft.com/fwlink/?LinkId=202834&clcid=0x407.
- Wenn das Zertifikat in einem Edgepool verwendet werden soll, muss es als exportierbares Zertifikat erstellt werden, und es muss auf jedem Edgeserver im Edgepool das gleiche

Zertifikat verwendet werden. Der exportierbare private Schlüssel ist für den A/V-Authentifizierungsdienst erforderlich, der den gleichen privaten Schlüssel auf allen Edgeservern im Pool verwenden muss.

- Der Antragstellername für das Zertifikat ist der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) oder die virtuelle IP-Adresse (VIP) eines Hardwaregeräts zum Lastenausgleich (z. B. „access.contoso.com“).

  Hinweis:
  Für Lync Server 2010 ist dies nicht mehr zwingend erforderlich, wird jedoch aus Gründen der Kompatibilität mit Office Communications Server weiterhin empfohlen.

- Die Liste der alternativen Antragstellernamen enthält folgende FQDNs:

  - Die externe Edgeschnittstelle für den Zugriff oder die VIP eines Hardwaregeräts zum Lastenausgleich (z. B. „access.contoso.com“)

    Hinweis:
    Auch wenn der Antragstellername des Zertifikats dem FQDN des Zugriffsedges entspricht, muss der alternative Antragstellername auch den FQDN des Zugriffs-Edgeservers enthalten, da TLS (Transport Layer Security) den Antragstellernamen ignoriert und zur Überprüfung die Einträge für alternative Antragstellernamen verwendet.

  - Die externe Edgeschnittstelle für Webkonferenzen oder die VIP eines Hardwaregeräts zum Lastenausgleich (z. B. „webcon.contoso.com“).

  - Wenn Sie die automatische Clientkonfiguration oder Partnerverbundfunktionen nutzen, geben Sie auch alle in Ihrem Unternehmen verwendeten FQDNs der SIP-Domäne an (z. B. „sip.contoso.com“, „sip.fabrikam.com“).

  - Die Einträge für den Antragstellernamen oder die alternativen Antragstellernamen werden vom A/V-Authentifizierungsdienst nicht verwendet.

  Hinweis:
  Die Reihenfolge der FQDNs in den alternativen Antragstellernamen spielt keine Rolle.

Wenn Sie an einem Standort mehrere Edgeserver mit Lastenausgleich bereitstellen, müssen alle auf den Edgeservern installierten Zertifikate für die externe A/V-Edgeschnittstelle von der gleichen Zertifizierungsstelle stammen und den gleichen privaten Schlüssel verwenden. Beachten Sie, dass der private Schlüssel des Zertifikats exportierbar sein muss, unabhängig davon, ob das Zertifikat auf einem oder mehreren Edgeservern verwendet wird. Dies gilt auch, wenn Sie das Zertifikat von einem anderen Computer als dem Edgeserver anfordern. Da der Antragstellername

oder alternative Antragstellername vom A/V-Authentifizierungsdienst nicht verwendet wird, können Sie das Zugriffs-Edgezertifikat wiederverwenden, soweit die Anforderungen an den Antragstellernamen oder den alternativen Antragstellernamen für die Edgeschnittstellen für Zugriff und Webkonferenzen erfüllt sind und der private Schlüssel des Zertifikats exportierbar ist.

Folgende Anforderungen gelten für das private (oder öffentliche) Zertifikat für die interne Edgeschnittstelle:

- Das Zertifikat kann von einer internen Zertifizierungsstelle oder einer vertrauenswürdigen öffentlichen Zertifizierungsstelle ausgestellt werden.
- Beim Antragstellernamen des Zertifikats handelt es sich üblicherweise um den FQDN der internen Edgeschnittstelle oder um die VIP eines Hardwaregeräts zum Lastenausgleich (z. B. „lsedge.contoso.com“). Für die interne Edgeschnittstelle können Sie jedoch auch ein Platzhalterzertifikat verwenden.
- Eine Liste mit alternativen Antragstellernamen ist nicht erforderlich.

Für den Reverseproxy in Ihren Bereitstellungsdiensten ist Folgendes erforderlich:

- Externer Benutzerzugriff auf Besprechungsinhalte für Besprechungen
- Externer Benutzerzugriff zum Erweitern und Anzeigen der Elemente von Verteilergruppen
- Externer Benutzerzugriff auf herunterladbare Dateien über den Adressbuchdienst
- Externer Benutzerzugriff auf den Lync Web App-Client
- Externer Benutzerzugriff auf die Webseite „Einstellungen für Einwahlkonferenzen“
- Externer Benutzerzugriff auf den Standortinformationsdienst
- Externer Gerätezugriff auf den Geräteupdatedienst und Abrufen von Updates

Der Reverseproxy veröffentlicht die internen Server-URLs der Webkomponenten. Die URLs der Webkomponenten werden im Director, Front-End-Server oder Front-End-Pool als **Externe Webdienste** im Topologie-Generator definiert.

Platzhaltereinträge werden im Feld für den alternativen Antragstellernamen des Zertifikats unterstützt, das dem Reverseproxy zugewiesen ist. Ausführliche Informationen zum Konfigurieren der Zertifikatsanforderung für den Reverseproxy finden Sie unter Anfordern und Konfigurieren eines Zertifikats für den HTTP-Reverseproxy.

Einrichten der Zertifikate für die interne Edgeschnittstelle

Ein einzelnes Zertifikat ist für die interne Schnittstelle jedes Edgeservers erforderlich.
Die Zertifikate für die interne Schnittstelle können von einer internen Unternehmenszertifizierungsstelle oder von einer öffentlichen Zertifizierungsstelle ausgestellt werden. Wenn Ihre Organisation eine interne Zertifizierungsstelle bereitstellt, können Sie die Ausgaben für die Verwendung öffentlicher Zertifikate einsparen, indem Sie das Zertifikat für die interne Schnittstelle von der internen Zertifizierungsstelle ausstellen lassen. Zum Erstellen dieser Zertifikate können Sie eine interne Windows Server 2008- oder Windows Server 2008 R2-Zertifizierungsstelle verwenden.

Ausführliche Informationen hierzu und zu anderen Anforderungen an Zertifikate finden Sie unter Zertifikatanforderungen für den externen Benutzerzugriff.

Führen Sie die Schritte in diesem Abschnitt aus, um Zertifikate für die interne Edgeschnittstelle an einem Standort einzurichten:

1. Laden Sie die Zertifikatskette der Zertifizierungsstelle für die interne Schnittstelle auf die einzelnen Edgeserver herunter.
2. Importieren Sie die Zertifikatskette der Zertifizierungsstelle auf den einzelnen Edgeservern für die interne Schnittstelle.
3. Erstellen Sie die Zertifikatsanforderung für die interne Schnittstelle auf einem Edgeserver, der dann als erster Edgeserver bezeichnet wird.
4. Importieren Sie das Zertifikat für die interne Schnittstelle auf dem ersten Edgeserver.
5. Importieren Sie das Zertifikat auf den anderen Edgeservern an diesem Standort (bzw. auf Edgeservern, die hinter diesem Hardwaregerät zum Lastenausgleich bereitgestellt werden).
6. Weisen Sie das Zertifikat für die interne Schnittstelle jedes Edgeservers zu.

Falls Sie über mehrere Standorte mit Edgeservern verfügen (also über eine Edgetopologie mit mehreren Standorten) oder falls Sie separate Gruppen von Edgeservern hinter verschiedenen Hardwaregeräten zum Lastenausgleich bereitstellen, müssen Sie diese Schritte für jeden Standort, der über Edgeserver verfügt, sowie für jede Gruppe von Edgeservern, die hinter einem Hardwaregerät zum Lastenausgleich bereitgestellt wird, separat ausführen.

Hinweis:
Die Schritte der Verfahren in diesem Abschnitt basieren auf der Verwendung einer Windows Server 2008 Enterprise-Zertifizierungsstelle oder einer Windows Server 2008 R2-Zertifizierungsstelle zum Erstellen eines Zertifikats für jeden Edgeserver. Eine Schritt-für-Schritt-Anleitung für andere Zertifizierungsstellen finden Sie in der Dokumentation für die jeweilige Zertifizierungsstelle.

Standardmäßig besitzen alle authentifizierten Benutzer die entsprechenden Rechte zum Anfordern von Zertifikaten.

Die Verfahren in diesem Abschnitt basieren auf der Erstellung von Zertifikatsanforderungen auf dem Edgeserver im Rahmen des Edgeserver-Bereitstellungsprozesses. Zertifikatsanforderungen können mithilfe des Front-End-Servers erstellt werden. Dies ist möglich, um die Zertifikatsanforderung zu einem frühen Zeitpunkt im Planungs- und Bereitstellungsprozess vor der Bereitstellung der Edgeserver abzuschließen. Hierzu müssen Sie sicherstellen, dass das angeforderte Zertifikat exportiert werden kann.

Die Verfahren in diesem Abschnitt beschreiben die Verwendung einer CER-Datei für das Zertifikat. Wenn Sie einen anderen Dateityp verwenden, ändern Sie diese Verfahren entsprechend ab.

So laden Sie die Zertifikatskette der Zertifizierungsstelle für die interne Schnittstelle herunter

1. Melden Sie sich an einem Server mit Lync Server 2010 im internen Netzwerk (also nicht am Edgeserver) als Mitglied der Gruppe **Administratoren** an.

2. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus, indem Sie auf **Start** und dann auf **Ausführen** klicken und Folgendes eingeben:

   ```
   https://<name of your Issuing CA Server>/certsrv
   ```

   Hinweis:
   Wenn Sie eine Windows Server 2008- oder Windows Server 2008 R2-Unternehmenszertifizierungsstelle verwenden, müssen Sie „https“ anstelle von „http“ einsetzen.

3. Klicken Sie auf der Webseite der ausstellenden Zertifizierungsstelle unter **Task auswählen** auf **Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifikatsperrliste**.

4. Klicken Sie unter **Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifikatsperrliste** auf **Download der Zertifizierungsstellen-Zertifikatkette**.

5. Klicken Sie im Dialogfeld **Dateidownload** auf **Speichern**.

6. Speichern Sie die P7B-Datei auf der Festplatte auf dem Server, und kopieren Sie die Datei dann in einen Ordner auf jedem Edgeserver.

   Hinweis:
   Die P7B-Datei enthält alle Zertifikate, die sich unter dem Zertifizierungspfad

befinden. Zum Anzeigen des Zertifizierungspfads öffnen Sie das Serverzertifikat, und klicken Sie auf den Zertifizierungspfad.

So importieren Sie die Zertifikatskette der Zertifizierungsstelle für die interne Schnittstelle

1. Öffnen Sie auf jedem Edgeserver die MMC (Microsoft Management Console), indem Sie auf **Start** und dann auf **Ausführen** klicken, im Feld **Öffnen** den Befehl **mmc** eingeben und dann auf **OK** klicken.
2. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen** und dann auf **Hinzufügen**.
3. Klicken Sie im Feld **Eigenständiges Snap-In hinzufügen** auf **Zertifikate** und anschließend auf **Hinzufügen**.
4. Klicken Sie im Dialogfeld **Zertifikat-Snap-In** auf **Computerkonto** und anschließend auf **Weiter**.
5. Stellen Sie im Dialogfeld **Computer auswählen** sicher, dass das Kontrollkästchen **Lokalen Computer: (Computer, auf dem diese Konsole ausgeführt wird)** aktiviert ist, und klicken Sie dann auf **Fertig stellen**.
6. Klicken Sie auf **Schließen** und dann auf **OK**.
7. Erweitern Sie in der Konsolenstruktur den Eintrag **Zertifikate (Lokaler Computer)**, klicken Sie mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen** zeigen Sie auf **Alle Aufgaben**, und klicken Sie anschließend auf **Importieren**.
8. Geben Sie im Assistenten unter **Zu importierende Datei** den Dateinamen des Zertifikats ein (also den Namen, den Sie im vorherigen Verfahren beim Herunterladen der Zertifikatskette der Zertifizierungsstelle für die interne Schnittstelle angegeben haben).
9. Wiederholen Sie dieses Verfahren für jeden Edgeserver.

So erstellen Sie die Zertifikatsanforderung für die interne Schnittstelle

1. Starten Sie auf einem der Edgeserver den Bereitstellungs-Assistenten, und klicken Sie neben **Schritt 3: Zertifikate anfordern, installieren oder zuweisen** auf **Ausführen**.

Hinweis:

Wenn Sie in einem Pool über mehrere Edgeserver an einem Standort verfügen, können Sie den Zertifikat-Assistenten auf jedem dieser Edgeserver ausführen.

Nachdem Sie Schritt 3 erstmals ausgeführt haben, ändert sich die Schaltfläche in **Erneut ausführen**, und ein grünes Häkchen, das auf den erfolgreichen Abschluss der Aufgabe hinweist, wird erst angezeigt, wenn alle erforderlichen Zertifikate angefordert, installiert und zugewiesen wurden.

2. Klicken Sie auf der Seite **Verfügbare Zertifikataufgaben** auf **Neue Zertifikatsanforderung erstellen**.

3. Klicken Sie auf der Seite **Zertifikatsanforderung** auf **Weiter**.

4. Klicken Sie auf der Seite **Verzögerte oder sofortige Anforderungen** auf **Anforderung jetzt vorbereiten, jedoch später senden**.

5. Geben Sie auf der Seite **Zertifikatsanforderungsdatei** den vollständigen Pfad und Namen der Datei ein, in der die Anforderung gespeichert werden soll (Beispiel: **c:\cert_internal_edge.cer**).

6. Aktivieren Sie auf der Seite **Alternative Zertifikatvorlage angeben** das Kontrollkästchen **Alternative Zertifikatvorlage für ausgewählte Zertifizierungsstelle verwenden**, um eine andere Vorlage als die Standardvorlage „WebServer“ zu verwenden.

7. Führen Sie auf der Seite **Namens- und Sicherheitseinstellungen** die folgenden Schritte aus:

   - Geben Sie im Feld **Anzeigename** einen Anzeigenamen für das Zertifikat ein (Beispiel: „Interner Edge“).

   - Geben Sie in **Bitlänge** die Bitlänge ein (typischerweise wird der Standardwert **2048** verwendet).

     Hinweis:
     Hohe Bitlängen bieten mehr Sicherheit, beeinträchtigen jedoch die Geschwindigkeit.

   - Wenn das Zertifikat exportierbar sein muss, aktivieren Sie das Kontrollkästchen **Privaten Schlüssel des Zertifikats als exportierbar markieren**.

8. Geben Sie auf der Seite **Organisationsinformationen** den Namen für die Organisation und die Organisationseinheit ein (z. B. eine Gruppe oder Abteilung).

9. Geben Sie auf der Seite **Geographische Informationen** die Standortinformationen ein.

10. Auf der Seite **Antragstellername/Alternative Antragstellernamen** werden die Informationen angezeigt, die automatisch vom Assistenten aufgefüllt werden.

11. Geben Sie auf der Seite **Weitere alternative Antragstellernamen konfigurieren** zusätzliche alternative Antragstellernamen an, die benötigt werden.

12. Überprüfen Sie auf der Seite **Zusammenfassung über Zertifikatsanforderungen** die Zertifikatinformationen, die zum Generieren der Anforderung verwendet werden sollen.

13. Nachdem die Befehle ausgeführt wurden, gehen Sie folgendermaßen vor:

    - Klicken Sie zum Anzeigen des Protokolls auf **Protokoll anzeigen**.
    - Klicken Sie auf **Weiter**, um die Zertifikatsanforderung abzuschließen.

14. Führen Sie auf der Seite **Zertifikatsanforderungsdatei** die folgenden Schritte aus:

    - Klicken Sie auf **Anzeigen**, um die generierte CSR-Datei (Certificate Signing Request, Zertifikatsignieranforderung) anzuzeigen.
    - Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

15. Senden Sie diese Datei an die Zertifizierungsstelle (per E-Mail oder mit einer anderen von Ihrer Organisation für die Zertifizierungsstelle des Unternehmens unterstützten Methode), und kopieren Sie, nachdem Sie die Antwortdatei erhalten haben, das neue Zertifikat auf diesen Computer, sodass es für einen Import zur Verfügung steht.

So importieren Sie das Zertifikat für die interne Schnittstelle

1. Melden Sie sich als Mitglied der Administratorgruppe an demselben Edgeserver an, auf dem Sie die Zertifikatsanforderung erstellt haben.

2. Klicken Sie im Bereitstellungs-Assistenten neben **Schritt 3: Zertifikate anfordern, installieren oder zuweisen** auf **Erneut ausführen**.

   Nachdem Sie Schritt 3 erstmals ausgeführt haben, ändert sich die Schaltfläche in **Erneut ausführen**. Ein grünes Häkchen, das auf den erfolgreichen Abschluss der Aufgabe hinweist, wird jedoch erst angezeigt, wenn alle erforderlichen Zertifikate angefordert, installiert und zugewiesen wurden.

3. Klicken Sie auf der Seite **Verfügbare Zertifikataufgaben** auf **Zertifikat aus einer P7B-, PFX- oder CER-Datei importieren**.

4. Geben Sie auf der Seite **Zertifikat importieren** den vollständigen Pfad und Dateinamen des Zertifikats an, das Sie für die interne Schnittstelle des Edgeservers angefordert und erhalten haben (oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen und sie auszuwählen).

5. Wenn Sie Zertifikate für andere Mitglieder des Pools importieren und ein Zertifikat einen privaten Schlüssel enthält, aktivieren Sie das Kontrollkästchen **Zertifikatdatei enthält den privaten Schlüssel des Zertifikats**, und geben Sie das Kennwort an.

So exportieren Sie das Zertifikat mit dem privaten Schlüssel für Edgeserver in einem Pool

1. Melden Sie sich als Mitglied der Administratorgruppe an demselben Edgeserver an, auf dem Sie das Zertifikat importiert haben.
2. Klicken Sie auf **Start** und dann auf **Ausführen**, und geben Sie **MMC** ein.
3. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf der Seite „Snap-Ins hinzufügen bzw. entfernen“ auf **Zertifikate** und dann auf **Hinzufügen**.
5. Wählen Sie im Dialogfeld „Zertifikat-Snap-In“ die Option **Computerkonto** aus. Klicken Sie auf **Weiter**. Wählen Sie im Dialogfeld „Computer auswählen“ die Option **Lokalen Computer: (Computer, auf dem diese Konsole ausgeführt wird)** aus. Klicken Sie auf **Fertig stellen**. Klicken Sie auf **OK**, um die Konfiguration der MMC-Konsole abzuschließen.
6. Doppelklicken Sie auf **Zertifikate (Lokaler Computer)**, um die Zertifikatspeicher zu erweitern. Doppelklicken Sie auf **Eigene Zertifikate**, und doppelklicken Sie dann auf **Zertifikate**.

   Wichtig:
   Falls im persönlichen Zertifikatspeicher für den lokalen Computer keine Zertifikate vorhanden sind, ist dem importierten Zertifikat kein privater Schlüssel zugeordnet. Überprüfen Sie die Anforderungs- und Importschritte. Falls das Problem weiterhin besteht, wenden Sie sich an den Administrator oder Anbieter Ihrer Zertifizierungsstelle.
7. Klicken Sie im persönlichen Zertifikatspeicher für den lokalen Computer mit der rechten Maustaste auf das Zertifikat, das Sie exportieren. Klicken Sie auf **Alle Aufgaben** und dann auf **Exportieren**.
8. Klicken Sie im Zertifikatexport-Assistenten auf **Weiter**. Wählen Sie **Ja, privaten Schlüssel exportieren** aus. Klicken Sie auf **Weiter**.

   Hinweis:
   Falls die Option **Ja, privaten Schlüssel exportieren** nicht verfügbar ist, wurde der private Schlüssel für dieses Zertifikat nicht für den Export markiert. Sie müssen das Zertifikat erneut anfordern und sicherstellen, dass das Zertifikat für den

Export markiert ist, um den Export des privaten Schlüssels zu ermöglichen. Erst dann können Sie den Export fortsetzen. Wenden Sie sich an den Administrator oder Anbieter Ihrer Zertifizierungsstelle.

9. Wählen Sie im Dialogfeld „Format der zu exportierenden Datei“ die Option **Privater Informationsaustausch – PKCS #12 (.PFX)** aus, und wählen Sie dann Folgendes aus:

   - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
   - Alle erweiterten Eigenschaften exportieren

   Warnung:
   Wählen Sie beim Exportieren des Zertifikats von einem Edgeserver nicht **Privaten Schlüssel nach erfolgreichem Export löschen** aus. Bei Auswahl dieser Option müssen Sie das Zertifikat und den privaten Schlüssel auf diesem Edgeserver importieren.

   Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.

10. Geben Sie ein Kennwort für den privaten Schlüssel ein. Geben Sie das Kennwort zur Bestätigung erneut ein. Klicken Sie auf **Weiter**.

11. Geben Sie einen Pfad und einen Dateinamen mit der Dateierweiterung PFX für das exportierte Zertifikat ein. Der Pfad muss entweder für alle anderen Edgeserver im Pool zugänglich sein oder für den Transport mithilfe von Wechselmedien (z. B. USB-Speicherstick) verfügbar sein. Klicken Sie auf **Weiter**.

12. Überprüfen Sie die Zusammenfassung im Dialogfeld „Fertigstellen des Assistenten“. Klicken Sie auf **Fertig stellen**.

13. Klicken Sie im Dialogfeld mit dem Hinweis auf den erfolgreichen Export auf **OK**.

14. Importieren Sie die exportierte Zertifikatdatei auf den anderen Edgeservern mithilfe der unter Einrichten der Zertifikate für die externe Edgeschnittstelle beschriebenen Schritte.

So weisen Sie das interne Zertifikat auf den Edgeservern zu

1. Klicken Sie auf jedem Edgeserver im Bereitstellungs-Assistenten neben **Schritt 3: Zertifikate anfordern, installieren oder zuweisen** auf **Erneut ausführen**.

2. Klicken Sie auf der Seite **Verfügbare Zertifikataufgaben** auf **Vorhandenes Zertifikat zuweisen**.

3. Wählen Sie auf der Seite **Zertifikatzuweisung** in der Liste den Eintrag **Interner Edge** aus.
4. Wählen Sie auf der Seite **Zertifikatspeicher** das Zertifikat aus, das Sie (im vorherigen Verfahren) für den internen Edge importiert haben.
5. Überprüfen Sie auf der Seite **Zusammenfassung der Zertifikatzuweisung** die Einstellungen, und klicken Sie dann auf **Weiter**, um die Zertifikate zuzuweisen.
6. Klicken Sie auf der Seite zum Abschließen des Assistenten auf **Fertig stellen**.
7. Nachdem Sie das interne Edgezertifikat über diese Schritte zugewiesen haben, öffnen Sie auf jedem Server das Zertifikat-Snap-In, erweitern Sie den Eintrag **Zertifikate (Lokaler Computer)** sowie den Eintrag **Eigene Zertifikate**, und klicken Sie auf **Zertifikate**. Überprüfen Sie dann im Detailbereich, ob das interne Edgezertifikat aufgeführt ist.
8. Wenn Ihre Bereitstellung mehrere Edgeserver umfasst, wiederholen Sie dieses Verfahren für jeden Edgeserver.

Einrichten der Zertifikate für die externe Edgeschnittstelle

Jeder Edgeserver benötigt ein öffentliches Zertifikat für die Schnittstelle zwischen dem Umkreisnetzwerk und dem Internet. Der alternative Antragstellername des Zertifikats muss die externen Namen des Zugriffs-Edgedienstes und die vollqualifizierten Domänennamen des Webkonferenz-Edgedienstes enthalten.

Ausführliche Informationen hierzu und zu anderen Anforderungen an Zertifikate finden Sie unter Zertifikatanforderungen für den externen Benutzerzugriff.

Eine Liste öffentlicher Zertifizierungsstellen, die Zertifikate entsprechend den speziellen Anforderungen an Unified Communications-Zertifikate bereitstellen und die eine Partnerschaft mit Microsoft eingegangen sind, um sicherzustellen, dass ihre Zertifikate mit dem Zertifikat-Assistenten von Lync Server verwendet werden können, finden Sie im Microsoft Knowledge Base-Artikel 929395, „Partner für Unified Communications-Zertifikate für Exchange Server und Communications Server“, unter http://go.microsoft.com/fwlink/?linkid=202834&clcid=0x407.

Konfigurieren von Zertifikaten für die externen Schnittstellen

Führen Sie die Schritte in diesem Abschnitt aus, um ein Zertifikat für die externe Edgeschnittstelle an einem Standort einzurichten:

- Erstellen Sie die Zertifikatsanforderung für die externe Schnittstelle des Edgeservers.
- Senden Sie die Anforderung an die öffentliche Zertifizierungsstelle.

- Importieren Sie das Zertifikat für die externe Schnittstelle jedes Edgeservers.
- Weisen Sie das Zertifikat für die externe Schnittstelle jedem Edgeserver zu.
- Wenn Ihre Bereitstellung mehrere Edgeserver umfasst, exportieren Sie das Zertifikat gemeinsam mit seinem privaten Schlüssel, und kopieren Sie es auf die anderen Edgeserver. Importieren Sie das Zertifikat anschließend für jeden Edgeserver, und weisen Sie es wie zuvor beschrieben zu. Wiederholen Sie dieses Verfahren für jeden Edgeserver.

Sie können öffentliche Zertifikate direkt von einer öffentlichen Zertifizierungsstelle anfordern (z. B. über die Website einer öffentlichen Zertifizierungsstelle). Bei den Verfahren in diesem Abschnitt wird für die meisten Aufgaben im Zusammenhang mit Zertifikaten der Zertifikat-Assistent verwendet. Wenn Sie ein Zertifikat direkt von einer öffentlichen Zertifizierungsstelle anfordern, ändern Sie die einzelnen Vorgehensweisen zum Anfordern, Transportieren und Importieren des Zertifikats sowie zum Importieren der Zertifikatkette entsprechend.

Wenn Sie ein Zertifikat von einer externen Zertifizierungsstelle anfordern, müssen die angegebenen Anmeldeinformationen mit den erforderlichen Rechten zum Anfordern eines Zertifikats von dieser Zertifizierungsstelle verknüpft sein. Jede Zertifizierungsstelle verfügt über eine Sicherheitsrichtlinie zur Definition, über welche Anmeldeinformationen (also bestimmte Benutzer- und Gruppennamen) Zertifikate angefordert, ausgestellt, verwaltet oder gelesen werden dürfen.

Wenn Sie die Microsoft Management Console (MMC) zum Importieren der Zertifikatkette und des Zertifikats verwenden, müssen Sie diese Elemente in den Zertifikatspeicher für den Computer importieren. Wenn Sie diese Elemente in den Zertifikatspeicher des Benutzers oder Diensts importieren, kann das Zertifikat nicht im Zertifikat-Assistenten von Lync Server zugewiesen werden.

So erstellen Sie die Zertifikatsanforderung für die externe Schnittstelle des Edgeservers

1. Klicken Sie auf dem Edgeserver im Bereitstellungs-Assistenten neben **Schritt 3: Zertifikate anfordern, installieren oder zuweisen** auf **Erneut ausführen**.

Hinweis:
Wenn Ihre Organisation Verbindungen mit öffentlichen Instant Messaging-Diensten über AOL unterstützen möchte, können Sie das Zertifikat nicht mit dem Lync Server-Bereitstellungs-Assistenten anfordern. Führen Sie stattdessen die weiter unten in diesem Thema beschriebenen Schritte unter „So erstellen Sie eine Zertifikatsanforderung für die externe Schnittstelle des Edgeservers zur Unterstützung von Verbindungen mit

öffentlichen Instant Messaging-Diensten über AOL“ aus.

Wenn Sie an einem Standort über mehrere Edgeserver in einem Pool verfügen, können Sie den Lync Server-Zertifikat-Assistenten auf jedem dieser Edgeserver ausführen.

2. Klicken Sie auf der Seite **Verfügbare Zertifikataufgaben** auf **Neue Zertifikatsanforderung erstellen**.

3. Klicken Sie auf der Seite **Zertifikatsanforderung** auf **Externes Edgezertifikat**.

4. Aktivieren Sie auf der Seite **Verzögerte oder sofortige Anforderung** das Kontrollkästchen **Anforderung jetzt vorbereiten, jedoch später senden**.

5. Geben Sie auf der Seite **Zertifikatsanforderungsdatei** den vollständigen Pfad und Namen der Datei ein, in der die Anforderung gespeichert werden soll (Beispiel: „c:\cert_exernal_edge.cer“).

6. Aktivieren Sie auf der Seite **Alternative Zertifikatvorlage angeben** das Kontrollkästchen **Alternative Zertifikatvorlage für ausgewählte Zertifizierungsstelle verwenden**, um eine andere Vorlage als die Standardvorlage „WebServer“ zu verwenden.

7. Führen Sie auf der Seite **Namens- und Sicherheitseinstellungen** die folgenden Schritte aus:

    - Geben Sie im Feld **Anzeigename** einen Anzeigenamen für das Zertifikat ein.

    - Geben Sie in **Bitlänge** die Bitlänge ein (typischerweise wird der Standardwert **2048** verwendet).

    - Stellen Sie sicher, dass das Kontrollkästchen **Privaten Schlüssel des Zertifikats als exportierbar markieren** aktiviert ist.

8. Geben Sie auf der Seite **Organisationsinformationen** den Namen für die Organisation und Organisationseinheit ein (z. B. eine Gruppe oder Abteilung).

9. Geben Sie auf der Seite **Geographische Informationen** die Standortinformationen ein.

10. Auf der Seite **Antragstellername/Alternative Antragstellernamen** werden die Informationen angezeigt, die automatisch vom Assistenten aufgefüllt werden. Wenn zusätzliche alternative Antragstellernamen erforderlich sind, werden diese in den nächsten zwei Schritten angegeben.

11. Aktivieren Sie auf der Seite **SIP-Domäneneinstellung für alternative Antragstellernamen (SANs)** das Kontrollkästchen der Domäne, um der Liste der alternativen Antragstellernamen einen Eintrag „sip.*<SIP-Domäne>*“ hinzuzufügen.

12. Geben Sie auf der Seite **Weitere alternative Antragstellernamen konfigurieren** zusätzliche alternative Antragstellernamen an, die benötigt werden.

13. Überprüfen Sie auf der Seite **Zusammenfassung über Zertifikatsanforderungen** die Zertifikatinformationen, die zum Generieren der Anforderung verwendet werden sollen.

14. Nachdem die Befehle ausgeführt wurden, führen Sie die folgenden Aufgaben aus:

    - Klicken Sie zum Anzeigen des Protokolls auf **Protokoll anzeigen**.
    - Klicken Sie auf **Weiter**, um die Zertifikatsanforderung abzuschließen.

15. Führen Sie auf der Seite **Zertifikatsanforderungsdatei** die folgenden Schritte aus:

    - Klicken Sie auf **Anzeigen**, um die generierte CSR-Datei (Certificate Signing Request, Zertifikatsignieranforderung) anzuzeigen.
    - Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

16. Kopieren Sie die Ausgabedatei an einen Speicherort, von dem aus Sie diese an die öffentliche Zertifizierungsstelle übermitteln können.

So erstellen Sie eine Zertifikatsanforderung für die externe Schnittstelle des Edgeservers zur Unterstützung von Verbindungen mit öffentlichen Instant Messaging-Diensten über AOL

1. Wenn die erforderliche Vorlage für die Zertifizierungsstelle zur Verfügung gestellt wurde, fordern Sie auf dem Edgeserver mithilfe des folgenden Windows PowerShell-Cmdlets das Zertifikat an:

   ```
   Request-CsCertificate –New -Type AccessEdgeExternal  –Output C:\
   <certfilename.txt or certfilename.csr>  –ClientEku $true –
   Template <template name>
   ```

   Der standardmäßige Zertifikatname der in Lync Server 2010 bereitgestellten Vorlage lautet „Web Server“. Geben Sie *<template name>* nur an, wenn eine andere Vorlage als die Standardvorlage verwendet werden muss.

   Hinweis:
   Wenn Ihre Organisation die Verbindung mit öffentlichen Instant Messaging-Diensten über AOL unterstützen möchte, müssen Sie Windows PowerShell anstelle des Zertifikat-Assistenten zum Anfordern des Zertifikats verwenden, das dem externen Edge für den Zugriffs-Edgedienst zugewiesen werden soll. Der Grund dafür ist, dass die Lync Server 2010-Vorlage „Web Server“, die der Zertifikat-Assistent zum Anfordern von Zertifikaten

verwendet, keine EKU-Clientkonfiguration unterstützt. Vor der Verwendung von Windows PowerShell zum Erstellen des Zertifikats muss der Administrator der Zertifizierungsstelle eine neue Vorlage mit Unterstützung für Client-EKU erstellen und bereitstellen.

So übermitteln Sie eine Anforderung an eine öffentliche Zertifizierungsstelle

1. Öffnen Sie die Ausgabedatei.
2. Kopieren Sie den Inhalt der Signieranforderung für das Zertifikat, und fügen Sie ihn ein.
3. Geben Sie nach Aufforderung Folgendes an:
   - **Microsoft** als Serverplattform.
   - **IIS** als Version.
   - **Web Server** als Verwendungstyp.
   - **PKCS7** als Antwortformat.
4. Wenn die öffentliche Zertifizierungsstelle Ihre Informationen überprüft hat, erhalten Sie eine E-Mail mit dem erforderlichen Text für das Zertifikat.
5. Kopieren Sie den Text aus der E-Mail, und speichern Sie ihn in einer Textdatei (TXT-Datei) auf Ihrem lokalen Computer.

So importieren Sie das Zertifikat für die externe Schnittstelle des Edgeservers

1. Melden Sie sich als Mitglied der Administratorgruppe an demselben Edgeserver an, auf dem Sie die Zertifikatsanforderung erstellt haben.
2. Klicken Sie im Bereitstellungs-Assistenten auf der Seite **Edgeserver bereitstellen** neben **Schritt 3: Zertifikate anfordern, installieren oder zuweisen** auf **Erneut ausführen**.
3. Klicken Sie auf der Seite **Verfügbare Zertifikataufgaben** auf **Zertifikat aus einer P7B-, PFX- oder CER-Datei importieren**.
4. Klicken Sie auf der Seite **Zertifikat importieren** auf **Durchsuchen**, um das Zertifikat, das Sie für die externe Schnittstelle des Edgeservers angefordert haben, zu suchen und auszuwählen (oder geben Sie den vollständigen Pfad und Dateinamen ein). Wenn das Zertifikat einen privaten Schlüssel enthält, wählen Sie **Zertifikatdatei enthält den privaten Schlüssel des Zertifikats** aus, und geben Sie das Kennwort für den privaten Schlüssel ein. Klicken Sie auf **Weiter**.

5. Überprüfen Sie die Zusammenfassung auf der Seite **Zertifikatszusammenfassung importieren**, und klicken Sie dann auf **Weiter**.

6. Überprüfen Sie auf der Seite **Befehle werden ausgeführt** die Ergebnisse des Imports, klicken Sie auf **Protokoll anzeigen**, um bei Bedarf weitere Informationen anzuzeigen, und klicken Sie dann auf **Fertig stellen**, um den Zertifikatimport abzuschließen.

7. Wenn Sie einen Edgeserverpool konfigurieren, exportieren Sie das Zertifikat mit seinem privaten Schlüssel wie weiter unten in diesem Thema unter „So exportieren Sie das Zertifikat mit dem privaten Schlüssel für Edgeserver in einem Pool“ beschrieben. Kopieren Sie die exportierte Zertifikatdatei auf die anderen Edgeserver, und importieren Sie sie in den Computerspeicher auf den einzelnen Edgeservern.

So exportieren Sie das Zertifikat mit dem privaten Schlüssel für Edgeserver in einem Pool

1. Melden Sie sich als Mitglied der Administratorgruppe an demselben Edgeserver an, auf dem Sie das Zertifikat importiert haben.

2. Klicken Sie auf **Start** und dann auf **Ausführen**, und geben Sie **MMC** ein.

3. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.

4. Klicken Sie in **Snap-Ins hinzufügen bzw. entfernen** auf **Zertifikate** und anschließend auf **Hinzufügen**.

5. Wählen Sie im Dialogfeld **Zertifikate** die Option **Computerkonto** aus, und klicken Sie auf **Weiter**. Wählen Sie **Lokalen Computer: (Computer, auf dem diese Konsole ausgeführt wird)** im Dialogfeld **Computer auswählen** aus, klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **OK**, um die Konfiguration der MMC-Konsole abzuschließen.

6. Doppelklicken Sie auf **Zertifikate (Lokaler Computer)**, um die Zertifikatspeicher zu erweitern. Doppelklicken Sie auf **Eigene Zertifikate**, und doppelklicken Sie dann auf **Zertifikate**.

   Wichtig:
   Falls im persönlichen Zertifikatspeicher für den lokalen Computer keine Zertifikate vorhanden sind, ist dem importierten Zertifikat kein privater Schlüssel zugeordnet. Überprüfen Sie die Anforderungs- und Importschritte. Falls das Problem weiterhin besteht, wenden Sie sich an den Administrator oder Anbieter Ihrer Zertifizierungsstelle.

7. Klicken Sie im persönlichen Zertifikatspeicher für den lokalen Computer mit der rechten Maustaste auf das Zertifikat, das Sie exportieren. Klicken Sie auf **Alle Aufgaben** und

dann auf **Exportieren**.

8. Klicken Sie im Zertifikatexport-Assistenten auf **Weiter**, wählen Sie **Ja, privaten Schlüssel exportieren** aus, und klicken Sie dann auf **Weiter**.

   Hinweis:
   Falls die Option **Ja, privaten Schlüssel exportieren** nicht verfügbar ist, wurde der private Schlüssel für dieses Zertifikat nicht für den Export markiert. Sie müssen das Zertifikat erneut anfordern und sicherstellen, dass das Zertifikat für den Export markiert ist, um den Export des privaten Schlüssels zu ermöglichen. Erst dann können Sie den Export fortsetzen. Wenden Sie sich an den Administrator oder Anbieter Ihrer Zertifizierungsstelle.

9. Wählen Sie im Dialogfeld „Format der zu exportierenden Datei“ die Option **Privater Informationsaustausch – PKCS #12 (.PFX)** aus, und wählen Sie dann Folgendes aus:

   - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
   - Alle erweiterten Eigenschaften exportieren

     Warnung:
     Wählen Sie beim Exportieren des Zertifikats von einem Edgeserver nicht **Privaten Schlüssel nach erfolgreichem Export löschen** aus. Bei Auswahl dieser Option müssen Sie das Zertifikat und den privaten Schlüssel auf diesem Edgeserver importieren.

10. Klicken Sie auf **Weiter**.
11. Geben Sie ein Kennwort für den privaten Schlüssel ein. Geben Sie das Kennwort zur Bestätigung erneut ein, und klicken Sie dann auf **Weiter**.
12. Geben Sie einen Pfad und einen Dateinamen mit der Dateierweiterung PFX für das exportierte Zertifikat ein. Der Pfad muss entweder für alle anderen Edgeserver im Pool zugänglich sein oder für den Transport mithilfe von Wechselmedien (z. B. USB-Speicherstick) verfügbar sein. Klicken Sie auf **Weiter**.
13. Überprüfen Sie die Zusammenfassung im Dialogfeld **Fertigstellen des Assistenten**, und klicken Sie dann auf **Fertig stellen**.
14. Klicken Sie im Dialogfeld mit dem Hinweis auf den erfolgreichen Export auf **OK**.
15. Importieren Sie die exportierte Zertifikatdatei auf den anderen Edgeservern mithilfe der weiter oben in diesem Thema unter „So importieren Sie das Zertifikat für die externe Schnittstelle des Edgeservers“ beschriebenen Schritte.

So weisen Sie der externen Schnittstelle des Edgeservers das Zertifikat zu

1. Klicken Sie auf jedem Edgeserver im Bereitstellungs-Assistenten neben **Schritt 3: Zertifikate anfordern, installieren oder zuweisen** auf **Erneut ausführen**.
2. Klicken Sie auf der Seite **Verfügbare Zertifikataufgaben** auf **Vorhandenes Zertifikat zuweisen**.
3. Klicken Sie auf der Seite **Zertifikatzuweisung** auf **Externes Edgezertifikat**, und aktivieren Sie das Kontrollkästchen **Erweiterte Zertifikatverwendungen**.
4. Aktivieren Sie auf der Seite **Erweiterte Zertifikatverwendungen** alle Kontrollkästchen, um das Zertifikat allen Verwendungen zuzuweisen.
5. Wählen Sie auf der Seite **Zertifikatspeicher** das öffentliche Zertifikat aus, das Sie für die externe Schnittstelle dieses Edgeservers angefordert und importiert haben.

   Hinweis:
   Wenn das angeforderte und importierte Zertifikat nicht in der Liste aufgeführt wird, stellen Sie sicher, dass der Antragstellername und die alternativen Antragstellernamen des Zertifikats alle Anforderungen für das Zertifikat erfüllen. Wenn Sie das Zertifikat und die Zertifikatkette nicht über die vorstehenden Verfahren, sondern manuell importiert haben, überprüfen Sie zudem, ob sich das Zertifikat im richtigen Zertifikatspeicher befindet (im Zertifikatspeicher des Computers, nicht des Benutzers oder Diensts).
6. Überprüfen Sie auf der Seite **Zusammenfassung der Zertifikatzuweisung** die Einstellungen, und klicken Sie dann auf **Weiter**, um die Zertifikate zuzuweisen.
7. Klicken Sie auf der Seite zum Abschließen des Assistenten auf **Fertig stellen**.
8. Nachdem Sie das Edgezertifikat über diese Schritte zugewiesen haben, öffnen Sie auf jedem Server das Zertifikat-Snap-In, erweitern Sie den Eintrag **Zertifikate (Lokaler Computer)** sowie den Eintrag **Eigene Zertifikate**, und klicken Sie auf **Zertifikate**. Überprüfen Sie dann im Detailbereich, ob das Zertifikat aufgeführt ist.
9. Wenn Ihre Bereitstellung mehrere Edgeserver umfasst, wiederholen Sie dieses Verfahren für jeden Edgeserver.

Einrichten der Zertifikate für den Reverseproxy

Jeder Reverseproxyserver erfordert ein Webserverzertifikat zur Verwendung durch den Überwachungsdienst. Das Webserverzertifikat muss von einer öffentlichen Zertifizierungsstelle ausgestellt werden.

Ausführliche Informationen hierzu und zu anderen Anforderungen an Zertifikate finden Sie unter Zertifikatanforderungen für den externen Benutzerzugriff.

So richten Sie ein Webdienstezertifikat für den Reverseproxy ein

- Der Reverseproxy sollte bereits eingerichtet sein (einschließlich des Webdienstezertifikats). Wenn Sie die erforderlichen Schritte nicht ausgeführt haben, bevor Sie mit der Bereitstellung Ihrer Edgeserver begonnen haben, führen Sie die Schritte in Einrichten von Reverseproxyservern aus, um eine Anforderung zu erstellen, das Webdienstezertifikat zu installieren und anschließend die einzelnen Webveröffentlichungsregeln zu erstellen und für die Verwendung des Zertifikats zu konfigurieren.

Starten der Edgeserver

Nachdem Sie die Einrichtung der Edgeserver und Geräte zum Lastenausgleich abgeschlossen haben, müssen Sie die Dienste auf jedem Edgeserver starten.

So starten Sie die Dienste

1. Klicken Sie auf jedem Edgeserver im Bereitstellungs-Assistenten neben **Schritt 4: Dienste starten** auf **Ausführen**.
2. Überprüfen Sie auf der Seite **Lync Server 2010-Dienste starten** die Liste der Dienste, und klicken Sie dann auf **Weiter**, um die Dienste zu starten.
3. Klicken Sie nach dem Start der Dienste auf **Fertig stellen**, um den Assistenten zu schließen.
4. Klicken Sie unter **Schritt 4: Dienste starten** auf **Dienststatus (optional)**.
5. Überprüfen Sie mithilfe der MMC-Konsole **Dienste** auf dem Server, ob alle Lync Server 2010-Dienste ausgeführt werden.

Einrichten von Reverseproxyservern

Für Microsoft Lync Server 2010-Edgeserverbereitstellungen ist ein HTTPS-Reverseproxy im Umkreisnetzwerk erforderlich, damit externe Clients auf die Lync Server 2010-Webdienste (in Office Communications Server als *Webkomponenten* bezeichnet) auf dem Director und im Home-Pool des Benutzers zugreifen können. Beispielsweise ist für die folgenden Features ein externer Zugriff über einen Reverseproxy erforderlich:

- Herunterladen von Besprechungsinhalten durch externe Benutzer

- Erweitern von Verteilergruppen durch externe Benutzer
- Herunterladen von Dateien aus dem Adressbuchdienst durch Remotebenutzer
- Zugriff auf den Microsoft Lync Web App-Client
- Zugriff auf die Webseite mit Einstellungen für Einwahlkonferenzen
- Zugriff auf den Standortinformationsdienst
- Herstellen einer Verbindung mit dem Geräteupdate-Webdienst und Abrufen von Updates durch externe Geräte

Es wird empfohlen, den HTTP-Reverseproxy zum Veröffentlichen aller Webdienste in sämtlichen Pools zu konfigurieren. Durch das Veröffentlichen von „https:// *ExternalFQDN*/*“ werden alle virtuellen IIS-Verzeichnisse für einen Pool veröffentlicht. Sie benötigen eine Veröffentlichungsregel für jeden Standard Edition-Server, Front-End-Pool oder Director oder Directorpool in Ihrer Organisation.

Darüber hinaus müssen Sie die einfachen URLs veröffentlichen. Wenn die Organisation über einen Director oder einen Directorpool verfügt, überwacht der HTTP-Reverseproxy HTTP/HTTPS-Proxyanforderungen für die einfachen URLs und sendet sie an das virtuelle Verzeichnis der externen Webdienste auf dem Director oder Directorpool. Wenn Sie keinen Director bereitgestellt haben, müssen Sie einen Pool zur Verarbeitung von Anforderungen für einfache URLs festlegen. (Wenn es sich hierbei nicht um den Home-Pool des Benutzers handelt, wird eine Weiterleitung an die Webdienste im Home-Pool des Benutzers durchgeführt.)
Die einfachen URLs können durch eine dedizierte Webveröffentlichungsregel verarbeitet werden, oder Sie können sie den öffentlichen Namen der Webveröffentlichungsregel für den Director hinzufügen.

Sie können Microsoft Forefront Threat Management Gateway 2010 oder Microsoft Internet Security and Acceleration (ISA) Server 2006 SP1 als Reverseproxy verwenden. Anhand der ausführlichen Schritte in diesem Abschnitt wird beschrieben, wie Sie Forefront Threat Management Gateway (TMG) 2010 konfigurieren. Die Schritte zum Konfigurieren von ISA Server 2006 sind fast identisch. Wenn Sie einen anderen Reverseproxy verwenden, finden Sie weitere Informationen in der Dokumentation zu diesem Produkt.

Anhand der Informationen in diesem Abschnitt können Sie einen TMG 2010-Reverseproxy einrichten. Führen Sie hierzu die Verfahren in diesem Abschnitt aus.

- Konfigurieren von Webfarm-FQDNs
- Konfigurieren von Netzwerkadaptern

- Anfordern und Konfigurieren eines Zertifikats für den HTTP-Reverseproxy
- Konfigurieren von Webveröffentlichungsregeln für einen einzelnen internen Pool
- Überprüfen oder Konfigurieren der Authentifizierung und Zertifizierung für virtuelle IIS-Verzeichnisse
- Erstellen von DNS-Einträgen für Reverseproxyserver
- Überprüfen des Zugriffs über den Reverseproxy

Vorbereitung

Richten Sie das verwendete System für Ihren Reverseproxy ein, bevor Sie die Konfiguration des Reverseproxys fortsetzen.

Konfigurieren von Webfarm-FQDNs

Beim Einrichten des Topologie-Generators konnten Sie auf jedem Standard Edition-Server, Front-End-Pool, Director oder Directorpool einen externen voll qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) für Webdienste konfigurieren. Diese Namen werden an die Clients in diesem Pool gesendet, wenn diese sich anmelden, und bei Remoteverbindungen zum Herstellen einer HTTPS-Verbindung zurück zum Reverseproxy verwendet. Wenn Sie diese URLs während der anfänglichen Topologie-Generator-Konfiguration nicht angegeben haben, müssen Sie Lync Server 2010 mithilfe der Verfahren in diesem Thema konfigurieren.

So konfigurieren Sie einen externen Pool-FQDN für Webdienste

1. Starten des Topologie-Generators: Klicken Sie auf **Start**, **Alle Programme**, **Microsoft Lync Server 2010** und anschließend auf **Lync Server-Topologie-Generator**.
2. Klicken Sie im Topologie-Generator in der Konsolenstruktur unter **Standard Edition-Front-End-Server**, **Enterprise Edition-Front-End-Pools** und **Directorpools** mit der rechten Maustaste auf den Namen des Pools, den Sie bearbeiten möchten, und klicken Sie anschließend auf **Eigenschaften bearbeiten**.
3. Fügen Sie im Abschnitt **Webdienste** unter **Externer FQDN für Webdienste** den FQDN hinzu, oder bearbeiten Sie diesen, und klicken Sie anschließend auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf **Lync Server 2010**, und klicken Sie anschließend auf **Veröffentlichen**.
5. Wiederholen Sie diese Schritte für alle Standard Edition-Server, Front-End-Pools sowie Directors oder Directorpools in der Organisation.

Konfigurieren von Netzwerkadaptern

Sie müssen dem externen Netzwerkadapter eine oder mehrere IP-Adressen und dem internen Netzwerkadapter mindestens eine IP-Adresse zuweisen.

Wenn es sich um eine neue Installation handelt, installieren Sie Microsoft Forefront Threat Management Gateway 2010 gemäß den Setupanweisungen des Produkts.

In den folgenden Verfahren verfügt der Server, auf dem Forefront Threat Management Gateway (TMG) 2010 ausgeführt wird, über zwei Netzwerkadapter:

- Einen öffentlichen (externen) Netzwerkadapter, der für Clients angezeigt wird, die eine Verbindung mit Ihrer Website herstellen (normalerweise über das Internet).
- Einen privaten bzw. internen Netzwerkadapter, der für interne Server mit Lync Server 2010 angezeigt wird, die Webdienste hosten.

Wichtig:
Ähnlich wie bei Edgeservern müssen Sie das Standardgateway des externen Netzwerkadapters auf die interne Adresse der externen Firewall festlegen, und Sie müssen beständige statische Routen in der internen Schnittstelle für alle Subnetze mit Servern erstellen, die von den Webveröffentlichungsregeln referenziert werden.

Der Reverseproxy muss den internen Director und die FQDNs des nächsten Hoppools, die in den Webveröffentlichungsregeln verwendet werden, in IP-Adressen auflösen können. Wie bei Edgeservern wird aus Sicherheitsgründen empfohlen, dass Edgeserver nicht auf einen DNS-Server im internen Netzwerk zugreifen. Dies bedeutet, dass Sie DNS-Server entweder im Umkreisnetzwerk bereitstellen müssen oder HOST-Dateieinträge auf dem Reverseproxy benötigen, der die FQDNs in die internen IP-Adressen der Server auflöst.

So konfigurieren Sie die Netzwerkadapter auf dem Reverseproxycomputer

1. Öffnen Sie auf dem Computer unter Windows Server 2008 oder Windows Server 2008 R2, auf dem TMG 2010 ausgeführt wird, das Fenster zum Ändern der Adaptereinstellungen. Klicken Sie dazu auf **Start**, zeigen Sie auf **Systemsteuerung**, klicken Sie auf **Netzwerk- und Freigabecenter**, und klicken Sie dann auf **Adaptereinstellungen ändern**.
2. Klicken Sie mit der rechten Maustaste auf die externe Netzwerkverbindung, die Sie für die externe Schnittstelle verwenden möchten, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Seite **Eigenschaften** auf die Registerkarte **Netzwerk**, klicken Sie in der Liste **Diese Verbindung verwendet folgende Elemente** auf **Internetprotokoll Version 4**

(TCP/IPv4), und klicken Sie dann auf **Eigenschaften**.

4. Konfigurieren Sie auf der Seite **Internetprotokolleigenschaften (TCP/IP)** die IP-Adressen entsprechend dem Netzwerksubnetz, an das der Netzwerkadapter angeschlossen ist.

   Hinweis:
   Wenn der Reverseproxy bereits von anderen Anwendungen genutzt wird, die HTTPS/443 verwenden, (z. B. zum Veröffentlichen von Outlook Web Access) müssen Sie entweder eine weitere IP-Adresse hinzufügen, um die Lync Server 2010-Webdienste ohne Konflikte mit den vorhandenen Regeln und Weblisteners über HTTPS/443 veröffentlichen zu können, oder Sie müssen das vorhandene Zertifikat durch ein Zertifikat ersetzen, das die neuen externen FQDNs dem alternativen Antragstellernamen hinzufügt.

5. Klicken Sie auf **OK** und dann nochmals auf **OK**.

6. Klicken Sie unter **Netzwerkverbindungen** mit der rechten Maustaste auf die interne Netzwerkverbindung, die Sie für die interne Schnittstelle verwenden möchten, und klicken Sie dann auf **Eigenschaften**.

7. Wiederholen Sie die Schritte 3 bis 5, um die interne Netzwerkverbindung zu konfigurieren.

Anfordern und Konfigurieren eines Zertifikats für den HTTP-Reverseproxy

Sie müssen für die Zertifizierungsstelleninfrastruktur, mit der die Serverzertifikate der Server mit Microsoft Lync Server 2010 ausgestellt wurden, das Zertifikat der Stammzertifizierungsstelle auf dem Server installieren, auf dem Microsoft Forefront Threat Management Gateway 2010 ausgeführt wird.

Außerdem müssen Sie ein öffentliches Webserverzertifikat auf Ihrem Reverseproxyserver installieren. Die Liste der alternativen Antragstellernamen dieses Zertifikats sollte die veröffentlichten externen FQDNs für jeden Pool enthalten, in dem Benutzer verwaltet werden, die für den Remotezugriff aktiviert wurden. Außerdem muss das Zertifikat die externen FQDNs aller Director-Server oder Directorpools enthalten, die innerhalb dieser Edgeinfrastruktur verwendet werden. In den alternativen Antragstellernamen müssen außerdem wie in der folgenden Tabelle dargestellt die einfachen URLs für Besprechungen (Meet) und Einwahl (Dialin) enthalten sein.

	Wert	**Beispiel**
Antragstellername	Pool-FQDN	webext.contoso.com

	Wert	Beispiel
Alternativer Antragstellername	Pool-FQDN	webext.contoso.com **Wichtig:** Der Antragstellername muss ebenfalls im alternativen Antragstellernamen vorhanden sein.
Alternativer Antragstellername	Einfache URL für Besprechungen **Hinweis:** Alle einfachen URLs für Besprechungen müssen im alternativen Antragstellernamen enthalten sein. Jede SIP-Domäne muss über mindestens eine aktive einfache URL für Besprechungen verfügen.	meet.contoso.com
Alternativer Antragstellername	Einfache URLs vom Typ „Dialin“	dialin.contoso.com

Hinweis:
Wenn Ihre interne Bereitstellung mehr als einen Standard Edition-Server oder Front-End-Pool umfasst, müssen Sie Webveröffentlichungsregeln für jeden externen FQDN der Webfarm konfigurieren. Außerdem benötigen Sie entweder ein Zertifikat und einen Weblistener für jeden Eintrag, oder Sie müssen ein Zertifikat anfordern, dessen Liste alternativer Antragstellernamen die Namen enthält, die von allen Pools verwendet werden. Diese müssen einem Weblistener zugewiesen und in mehreren Webveröffentlichungsregeln gemeinsam verwendet werden.

Konfigurieren von Webveröffentlichungsregeln für einen einzelnen internen Pool

Microsoft Forefront Threat Management Gateway 2010 verwendet Webveröffentlichungsregeln zum Veröffentlichen von internen Ressourcen (z. B. Besprechungs-URLs) für Benutzer im Internet.

Zusätzlich zu den Webdienste-URLs für die virtuellen Verzeichnisse müssen Sie Veröffentlichungsregeln für einfache URLs erstellen. Für jede einfache URL muss eine einzelne Regel für den Reverseproxy erstellt werden, die auf diese einfache URL zeigt.

Verwenden Sie die folgenden Verfahren, um Webveröffentlichungsregeln zu erstellen.

Hinweis:
Für diese Verfahren wird vorausgesetzt, dass die Standard Edition von Forefront Threat Management Gateway (TMG) 2010 installiert ist.

So erstellen Sie eine Webveröffentlichungsregel auf dem Computer, auf dem TMG 2010 ausgeführt wird

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme** und dann auf **Microsoft Forefront TMG**, und klicken Sie auf **Forefront TMG-Verwaltung**.

2. Erweitern Sie im linken Bereich **ServerName**, klicken Sie mit der rechten Maustaste auf **Firewallrichtlinie**, zeigen Sie auf **Neu**, und klicken Sie dann auf **Website-Veröffentlichungsregel**.

3. Geben Sie auf der Seite **Willkommen** einen Anzeigenamen für die Veröffentlichungsregel ein (z. B. „LyncServerWebDownloadsRule“).

4. Wählen Sie auf der Seite **Regelaktion auswählen** die Option **Zulassen** aus.

5. Wählen Sie auf der Seite **Veröffentlichungstyp** die Option **Einzelne Website oder Lastenausgleich veröffentlichen** aus.

6. Klicken Sie auf der Seite **Sicherheit der Serververbindung** auf **SSL verwenden, um eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm herzustellen**.

7. Geben Sie auf der Seite **Interne Veröffentlichungsdetails** im Feld **Interner Sitename** den FQDN der internen Webfarm ein, auf der Besprechungsinhalte und Adressbuchdateien gehostet werden.

   Hinweis:
   Wenn der interne Server ein Standard Edition-Server ist, entspricht dieser FQDN dem vollqualifizierten Domänennamen des Standard Edition-Servers. Handelt es sich bei Ihrem internen Server um einen Front-End-Pool, entspricht dieser FQDN einer virtuellen IP (VIP) für das Hardwaregerät zum Lastenausgleich, das den Lastenausgleich für die internen Webfarmserver durchführt. Der TMG-Server muss in der Lage sein, den FQDN für die IP-Adresse des internen Webservers aufzulösen. Wenn der TMG-Server den FQDN nicht in eine ordnungsgemäße IP-Adresse auflösen kann, können Sie **Name oder IP-Adresse eines Computers verwenden, um eine Verbindung zum veröffentlichten Server herzustellen** auswählen und dann die IP-Adresse des internen Webservers in das Feld **Computername oder IP-Adresse** eingeben. In diesem Fall müssen Sie

sicherstellen, dass der Port 53 auf dem TMG-Server geöffnet ist und der Server mit einem DNS-Server im Umkreisnetzwerk kommunizieren kann. Für die Namensauflösung können Sie auch Einträge in der Datei lokaler Hosts verwenden.

8. Geben Sie auf der Seite **Interne Veröffentlichungsdetails** im Feld **Pfad (optional)** als Pfad zum Ordner, der veröffentlicht werden soll, **/*** ein.

   Hinweis:
   Sie können im Assistenten zum Veröffentlichen von Websites nur einen Pfad angeben. Weitere Pfade können Sie hinzufügen, indem Sie die Eigenschaften der Regel ändern.

9. Stellen Sie auf der Seite **Details des öffentlichen Namens** sicher, dass unter **Anforderungen annehmen für** die Option **Diesen Domänennamen** ausgewählt ist, und geben Sie den externen FQDN der Webdienste in das Feld **Öffentlicher Name** ein.

10. Klicken Sie auf der Seite **Weblistener auswählen** auf **Neu**, um den Assistenten für neue Weblistenerdefinition zu öffnen.

11. Geben Sie auf der Seite **Willkommen** im Feld **Weblistenername** einen Namen für den Weblistener ein (z. B. „LyncServerWebServers“).

12. Wählen Sie auf der Seite **Sicherheit der Clientverbindung** die Einstellung **Sichere SSL-Verbindungen mit Clients erforderlich** aus.

13. Wählen Sie auf der Seite **Weblistener-IP-Adressen** die Option **Extern** aus, und klicken Sie dann auf **IP-Adressen auswählen**.

14. Wählen Sie auf der Seite zur Auswahl von externen Listener-IP-Adressen die Option **Angegebene IP-Adressen auf dem Forefront TMG-Computer im ausgewählten Netzwerk** aus, wählen Sie die passende IP-Adresse aus, und klicken Sie auf **Hinzufügen**.

15. Klicken Sie auf der Seite **Listener-SSL-Zertifikate** auf **Jeder IP-Adresse ein Zertifikat zuweisen**, wählen Sie die IP-Adresse aus, die dem externen Web-FQDN zugeordnet ist, und klicken Sie dann auf **Zertifikat auswählen**.

16. Wählen Sie auf der Seite **Zertifikat auswählen** das Zertifikat aus, das den in Schritt 9 angegebenen öffentlichen Namen entspricht, und klicken Sie auf **Auswählen**.

17. Wählen Sie auf der Seite **Authentifizierungseinstellungen** die Option **Keine Authentifizierung** aus.

18. Klicken Sie auf der Seite **Einstellungen für einmaliges Anmelden (SSO)** auf **Weiter**.

19. Überprüfen Sie auf der Seite **Fertigstellen des Assistenten** die Einstellungen unter **Weblistener**, und klicken Sie dann auf **Fertig stellen**.

20. Klicken Sie auf der Seite **Authentifizierungsdelegierung** auf **Keine Delegierung, aber direkte Authentifizierung des Clients**.

21. Klicken Sie auf der Seite **Benutzersatz** auf **Weiter**.

22. Überprüfen Sie auf der Seite **Fertigstellen des Assistenten** die Einstellungen für die Webveröffentlichungsregel, und klicken Sie dann auf **Fertig stellen**.

23. Klicken Sie im Detailbereich auf **Übernehmen**, um die Änderungen zu speichern und die Konfiguration zu aktualisieren.

So ändern Sie die Eigenschaften der Webveröffentlichungsregel

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme** und dann auf **Microsoft Forefront TMG**, und klicken Sie auf **Forefront TMG-Verwaltung**.

2. Erweitern Sie im linken Bereich **ServerName**, und klicken Sie dann auf **Firewallrichtlinie**.

3. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Webserververöffentlichungsregel, die Sie im vorhergehenden Verfahren erstellt haben (z. B. „LyncServerExternalRule“), und klicken Sie dann auf **Eigenschaften**.

4. Führen Sie auf der Seite **Eigenschaften** auf der Registerkarte **Von** folgende Schritte aus:

   - Klicken Sie in der Liste **Diese Regel betrifft Datenverkehr von diesen Quellen** auf **Beliebig**, und klicken Sie dann auf **Entfernen**.

   - Klicken Sie auf **Hinzufügen**.

   - Erweitern Sie in **Netzwerkidentitäten hinzufügen** den Eintrag **Netzwerke**, klicken Sie auf **Extern**, dann auf **Hinzufügen** und zuletzt auf **Schließen**.

5. Stellen Sie auf der Registerkarte **An** sicher, dass das Kontrollkästchen **Ursprünglichen Hostheader anstelle des aktuellen Headers weiterleiten** aktiviert ist.

6. Aktivieren Sie auf der Registerkarte **Bridging** das Kontrollkästchen **Anforderung an SSL-Port umleiten**, und geben Sie anschließend Port **4443** an.

7. Fügen Sie auf der Registerkarte **Öffentlicher Name** die einfachen URLs hinzu

(z. B. „meet.contoso.com“ und „dialin.contoso.com“).

8. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, und klicken Sie dann auf **OK**.

9. Klicken Sie im Detailbereich auf **Übernehmen**, um die Änderungen zu speichern und die Konfiguration zu aktualisieren.

Überprüfen oder Konfigurieren der Authentifizierung und Zertifizierung für virtuelle IIS-Verzeichnisse

Führen Sie das folgende Verfahren aus, um die Zertifizierung für die virtuellen IIS-Verzeichnisse (Internet Information Services, Internetinformationsdienste) zu konfigurieren oder um die ordnungsgemäße Konfiguration der Zertifizierung zu überprüfen. Führen Sie das folgende Verfahren auf jedem Server mit IIS in Ihrem internen Lync Server-Pool aus.

Hinweis:
Das folgende Verfahren bezieht sich auf die externe Lync Server-Website in IIS.

So überprüfen oder konfigurieren Sie die Authentifizierung und Zertifizierung für virtuelle IIS-Verzeichnisse

1. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und dann auf **Verwaltung**, und klicken Sie auf **Internetinformationsdienste-Manager**.

2. Erweitern Sie im **Internetinformationsdienste-Manager** die Option **ServerName** und anschließend **Websites**.

3. Klicken Sie mit der rechten Maustaste auf **Lync Server External Web Site** und anschließend auf **Bindungen bearbeiten**.

4. Stellen Sie sicher, dass HTTPS Port 4443 zugeordnet ist, und klicken Sie dann auf **HTTPS**.

5. Wählen Sie den HTTPS-Eintrag aus, klicken Sie auf **Bearbeiten**, und vergewissern Sie sich, dass „Lync Server WebServicesExternalCertificate“ an dieses Protokoll gebunden ist.

Erstellen von DNS-Einträgen für Reverseproxyserver

Erstellen Sie externe DNS-A-Einträge für die öffentliche externe Schnittstelle Ihres ISA Server-Computers, wie unter Konfigurieren von DNS-Einträgen für die Edgeunterstützung beschrieben. Sie benötigen DNS-Einträge für die externen FQDNs der Webdienste in jedem Pool, für den Director (oder Directorpool) und für jede einfache URL.

Überprüfen des Zugriffs über den Reverseproxy

Überprüfen Sie mit dem folgenden Verfahren, ob die Benutzer auf Informationen auf dem Reverseproxy zugreifen können. Möglicherweise müssen Sie die Firewall- und die DNS-Konfiguration (Domain Name System) vollständig abschließen, bevor der Zugriff ordnungsgemäß funktioniert.

So überprüfen Sie den Zugriff über das Internet auf die Website

- Öffnen Sie einen Webbrowser, und geben Sie in der Adressleiste die URLs ein, die von den Clients für den Zugriff auf die Adressbuchdateien und die Website für Konferenzen verwendet werden:
    - Geben Sie für den Adressbuchserver eine URL ähnlich der folgenden ein: **https://Externer FQDN der Webfarm/abs**, wobei *Externer FQDN der Webfarm* für den externen FQDN der Webfarm steht, von der die Dateien des Adressbuchservers gehostet werden. Der Benutzer sollte eine HTTP-Anforderung erhalten, weil als Verzeichnissicherheit für den Ordner des Adressbuchservers standardmäßig die Windows-Authentifizierung konfiguriert ist.
    - Geben Sie für Konferenzen eine URL ähnlich der folgenden ein: **https://Externer FQDN der Webfarm/meet**, wobei *Externer FQDN der Webfarm* für den externen FQDN der Webfarm steht, von der Besprechungsinhalte gehostet werden. Unter dieser URL sollte die Problembehandlungsseite für Konferenzen angezeigt werden.
    - Geben Sie für die Verteilergruppenerweiterung eine URL ähnlich der folgenden ein: **https://Externer FQDN der Webfarm/GroupExpansion/service.svc**. Der Benutzer sollte eine HTTP-Anforderung erhalten, weil als Verzeichnissicherheit für den Erweiterungsdienst von Verteilergruppen standardmäßig die Windows-Authentifizierung konfiguriert ist.
    - Für die Einwahl geben Sie die einfache URL für Einwahlkonferenzen ein. Der Benutzer sollte auf die Seite zur Einwahl geleitet werden.

Konfigurieren der Unterstützung für den externen Benutzerzugriff

Nach der Installation und Konfiguration Ihrer internen Microsoft Lync Server 2010-Bereitstellung können interne Benutzer in Ihrer Organisation mit anderen internen Benutzern zusammenarbeiten, die über SIP-Konten in den Active Directory-Domänendiensten (Active Directory Domain Services, AD DS) verfügen. Die Zusammenarbeit kann den Austausch von Sofortnachrichten und Anwesenheitsinformationen sowie, bei entsprechender Konfiguration, die Teilnahme an Konferenzen (auch als „Besprechungen“ bezeichnet) umfassen. Standardmäßig können sich nur am internen Netzwerk angemeldete Benutzer bei

Lync Server 2010 anmelden. Sie aktivieren und konfigurieren den Zugriff durch externe Benutzer und steuern, ob unterstützte externe Benutzer mit internen Lync Server-Benutzern zusammenarbeiten können. Zu externen Benutzern gehören Remotebenutzer, Partnerbenutzer (einschließlich unterstützter Benutzer öffentlicher Sofortnachrichten-Dienstanbieter [Instant Messaging])
und anonyme Teilnehmer an Konferenzen, je nachdem, wie Sie den Zugriff durch externe Benutzer konfigurieren.

Die Bereitstellung eines Edgeservers oder Edgepools ist der erste Schritt zur Unterstützung externer Benutzer. Ausführliche Informationen zur Bereitstellung von Edgeservern finden Sie unter Bereitstellen von Edgeservern in der Bereitstellungsdokumentation.

Nachdem Sie einen Edgeserver oder einen Edgepool vollständig eingerichtet haben, müssen Sie die zu unterstützenden Typen des externen Benutzerzugriffs aktivieren und die Unterstützung für die externen Benutzer konfigurieren, die in Ihrer Organisation unterstützt werden sollen.
In Lync Server 2010 aktivieren und konfigurieren Sie den externen Benutzerzugriff über die Lync Server-Systemsteuerung und die Lync Server-Verwaltungsshell. Ausführliche Informationen zu diesen Verwaltungstools finden Sie unter „Lync Server-Systemsteuerung“ in der Betriebsdokumentation, unter „Lync Server-Verwaltungsshell“ in der Betriebsdokumentation und unter „Installieren der Lync Sever-Verwaltungstools“ in der Betriebsdokumentation.

Zur Unterstützung des externen Benutzerzugriffs müssen Sie die beiden folgenden Schritte ausführen:

- Aktivieren Sie die Unterstützung für Ihre Organisation. Zum Aktivieren der Unterstützung für den externen Benutzerzugriff in Ihrer Bereitstellung aktivieren Sie jeden Typ des externen Benutzerzugriffs, der unterstützt werden soll. Sie aktivieren und deaktivieren die Unterstützung für den externen Benutzerzugriff in der Lync Server 2010-Systemsteuerung, indem Sie die globalen Einstellungen auf der Seite **Zugriffs-Edgekonfiguration** in der Gruppe **Zugriff durch externe Benutzer** bearbeiten. Durch die Aktivierung der Unterstützung für den externen Benutzerzugriff wird angegeben, dass Ihre Server, auf denen der Lync Server-Zugriffs-Edgedienst ausgeführt wird, die Kommunikation mit externen Benutzern unterstützen. Externe Benutzer können jedoch erst dann mit internen Benutzern kommunizieren, wenn Sie außerdem mindestens eine Richtlinie zur Verwaltung der Verwendung des externen Benutzerzugriffs konfigurieren. Externe Benutzer können nicht mit Benutzern Ihrer Organisation kommunizieren, wenn der externe Benutzerzugriff deaktiviert ist oder wenn keine Richtlinien für dessen Unterstützung konfiguriert wurden.

- Konfigurieren Sie eine oder mehrere Richtlinien für die Unterstützung des externen Benutzerzugriffs, und weisen Sie sie zu. Hierzu können folgende Richtlinien gehören.

- Richtlinien für den Zugriff externer Benutzer, die Sie erstellen und konfigurieren können, um einen oder mehrere Typen des externen Benutzerzugriffs zu steuern, beispielsweise den Zugriff für Remotebenutzer, den Zugriff für Benutzer aus Partnerdomänen und den Zugriff für Benutzer unterstützter öffentlicher Sofortnachrichten-Dienstanbieter. Richtlinien für externe Benutzer werden in der Lync Server 2010-Systemsteuerung über die globale Richtlinie konfiguriert. Optional können Sie auf der Seite **Externe Zugriffsrichtlinie** in der Gruppe **Externer Benutzerzugriff** eine oder mehrere Richtlinien auf Standort- und Benutzerebene konfigurieren. Die globale Richtlinie wird bei der ersten Bereitstellung eines Edgeservers oder eines Edgepools erstellt und kann nicht gelöscht werden.
  Sie erstellen und konfigurieren Richtlinien auf Standort- und Benutzerebene, die Sie zum Einschränken des externen Benutzerzugriffs auf bestimmte Standorte oder Benutzer verwenden möchten. Globale und Standortrichtlinien werden automatisch zugewiesen. Wenn Sie eine Benutzerrichtlinie erstellen und konfigurieren, müssen Sie sie anschließend den jeweiligen Benutzern oder Benutzergruppen zuweisen, für die die Richtlinie gelten soll. Jede Richtlinie für den externen Benutzerzugriff kann eine oder mehrere der folgenden Zugriffsarten unterstützen: Remotebenutzerzugriff, Partnerbenutzerzugriff und Verbindung mit öffentlichen Instant Messaging-Diensten.

- Konferenzrichtlinien, die Sie zur Steuerung von Konferenzen in Ihrer Organisation erstellen und konfigurieren können, einschließlich der Benutzer in Ihrer Organisation, die anonyme Benutzer zu den von ihnen geleiteten Konferenzen einladen können. Nachdem Sie eine Konferenzrichtlinie erstellt und die Unterstützung für anonyme Benutzer in der Richtlinie aktiviert haben, müssen Sie die Richtlinie den jeweiligen Benutzern oder Benutzergruppen zuweisen, die anonyme Benutzer zu ihren Konferenzen einladen müssen.

Sie können auch dann Einstellungen für den Zugriff externer Benutzer konfigurieren, wenn Sie den externen Benutzerzugriff für Ihre Organisation nicht aktiviert haben. Hierzu gehören auch Richtlinien, die Sie zum Steuern des externen Benutzerzugriffs verwenden möchten. Die von Ihnen konfigurierten Richtlinien und anderen Einstellungen treten jedoch erst in Kraft, wenn der externe Benutzerzugriff für Ihre Organisation aktiviert wird. Externe Benutzer können nicht mit Benutzern Ihrer Organisation kommunizieren, wenn der externe Benutzerzugriff deaktiviert ist oder wenn keine Richtlinien für den externen Benutzerzugriff konfiguriert wurden.

Ihre Edgebereitstellung authentifiziert die Typen externer Benutzer und steuert den Zugriff basierend auf der Konfiguration der Edgeunterstützung. Zum Steuern der Kommunikation über die Firewall können Sie eine oder mehrere Richtlinien sowie weitere Einstellungen konfigurieren, durch die definiert wird, wie Benutzer innerhalb und außerhalb der Firewall miteinander

kommunizieren. Hierzu gehören die globale Standardrichtlinie für den externen Benutzerzugriff sowie Richtlinien auf Standort- und Benutzerebene, die Sie zum Aktivieren eines oder mehrerer Typen des externen Benutzerzugriffs für bestimmte Standorte oder Benutzer erstellen und konfigurieren können.

Inhalt dieses Abschnitts

- Aktivieren oder Deaktivieren des externen Benutzerzugriffs für Ihre Organisation
- Konfigurieren der Kommunikation mit externen Benutzern

Aktivieren oder Deaktivieren des externen Benutzerzugriffs für Ihre Organisation

Nach der Bereitstellung eines oder mehrerer Edgeserver müssen Sie die spezifischen Typen des externen Benutzerzugriffs aktivieren, die für Ihre Organisation unterstützt werden sollen. Hierzu gehören folgende Typen des externen Benutzerzugriffs:

- **Zugriff durch Remotebenutzer** Aktivieren Sie diese Option, wenn Benutzer in Ihrer Organisation, die sich außerhalb der Firewall befinden (z. B. Telearbeiter und Benutzer auf Geschäftsreise), sich mit Lync Server 2010 verbinden können sollen.
- **Partnerverbund** Aktivieren Sie diese Option, wenn Sie den Zugriff von Benutzern aus Verbundpartnerdomänen und/oder von Benutzern öffentlicher Sofortnachrichten-Dienstanbieter ermöglichen möchten.
- **Anonymer Benutzerzugriff** Aktivieren Sie diese Option, wenn Sie möchten, dass interne Benutzer anonyme Benutzer zu ihren Konferenzen einladen können.

Hinweis:
Neben dem Aktivieren der Unterstützung für den externen Benutzerzugriff müssen Sie auch Richtlinien konfigurieren, um die Verwendung des externen Benutzerzugriffs in Ihrer Organisation zu steuern, bevor den Benutzern ein beliebiger Typ des externen Benutzerzugriffs zur Verfügung steht. Ausführliche Informationen zum Erstellen, Konfigurieren und Anwenden von Richtlinien für den externen Benutzerzugriff finden Sie unter „Verwalten der Kommunikation mit externen Benutzern“ in der Bereitstellungs- oder Betriebsdokumentation.

Inhalt dieses Abschnitts

- Aktivieren oder Deaktivieren des Zugriffs durch Remotebenutzer für Ihre Organisation
- Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation
- Aktivieren oder Deaktivieren des Zugriffs anonymer Benutzer für Ihre Organisation

Aktivieren oder Deaktivieren des Zugriffs durch Remotebenutzer für Ihre Organisation

Bei Remotebenutzern handelt es sich um Benutzer in Ihrer Organisation, die über eine dauerhafte Active Directory-Identität innerhalb der Organisation verfügen. Wenn sie nicht intern mit dem Organisationsnetzwerk verbunden sind, melden sich Remotebenutzer häufig außerhalb der Firewall über ein VPN (Virtuelles Privates Netzwerk) bei Lync Server an. Remotebenutzer umfassen Mitarbeiter, die zu Hause oder unterwegs arbeiten, sowie andere Remotemitarbeiter, z. B. vertrauenswürdige Lieferanten, denen Anmeldeinformationen für das Unternehmen zur Verfügung gestellt wurden. Wenn Sie den Remotebenutzerzugriff aktivieren, müssen sich unterstützte Remotebenutzer nicht über ein VPN anmelden, um unter Verwendung von Lync Server 2010 mit internen Benutzern zusammenzuarbeiten.

Zur Unterstützung des Remotebenutzerzugriffs muss diese Option aktiviert werden.
Bei Aktivierung wird der Remotebenutzerzugriff für die gesamte Organisation aktiviert.
Wenn Sie den Zugriff durch Remotebenutzer zu einem späteren Zeitpunkt temporär oder dauerhaft unterbinden möchten, können Sie die Option für Ihre Organisation deaktivieren.
Verwenden Sie das Verfahren in diesem Abschnitt, um den Zugriff durch Remotebenutzer für Ihre Organisation zu aktivieren oder zu deaktivieren.

Hinweis:
Durch die Aktivierung des Remotebenutzerzugriffs wird lediglich angegeben, dass Ihre Server, auf denen der Zugriffs-Edgedienst ausgeführt wird, die Kommunikation mit Remotebenutzern unterstützen. Remotebenutzer können jedoch erst dann an Sofortnachrichtenunterhaltungen oder Konferenzen in Ihrer Organisation teilnehmen, wenn Sie außerdem mindestens eine Richtlinie zur Verwaltung der Verwendung des Remotebenutzerzugriffs konfigurieren. Ausführliche Informationen zur Konfiguration von Richtlinien für die Verwendung des Remotebenutzerzugriffs finden Sie unter Verwalten des Remotebenutzerzugriffs in der Bereitstellungs- oder Betriebsdokumentation.

So aktivieren oder deaktivieren Sie den Zugriff durch Remotebenutzer für Ihre Organisation

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.
2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.
3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Zugriffs-Edgekonfiguration**.

4. Klicken Sie auf der Seite **Zugriffs-Edgekonfiguration** auf **Global**, klicken Sie auf **Bearbeiten**, und klicken Sie dann auf **Details anzeigen**.

5. Führen Sie im Abschnitt **Zugriffs-Edgekonfiguration bearbeiten** einen der folgenden Schritte aus:

    - Aktivieren Sie das Kontrollkästchen **Zugriff durch Remotebenutzer aktivieren**, um den Zugriff durch Remotebenutzer für Ihre Organisation zuzulassen.

    - Deaktivieren Sie das Kontrollkästchen **Zugriff durch Remotebenutzer aktivieren**, um den Zugriff durch Remotebenutzer für Ihre Organisation zu deaktivieren.

6. Klicken Sie auf **Commit ausführen**.

Sie müssen außerdem mindestens eine Richtlinie für den externen Zugriff konfigurieren, damit Remotebenutzer sich an Ihren Servern mit Lync Server 2010 anmelden können. Ausführliche Informationen finden Sie unter Verwalten des Remotebenutzerzugriffs in der Bereitstellungs- oder Betriebsdokumentation.

Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation

Die Unterstützung für einen Partnerverbund ist erforderlich, um Benutzern mit einem Konto in einer vertrauenswürdigen Kunden- oder Partnerorganisation – Partnerdomänen und Benutzer eines unterstützten öffentlichen Sofortnachrichtenanbieters (Instant Messaging) eingeschlossen – die Zusammenarbeit mit Benutzern in Ihrer Organisation zu ermöglichen. Wenn Sie eine Vertrauensstellung mit solchen externen Domänen eingerichtet haben, können Sie Benutzer in diesen Domänen für den Zugriff auf Ihre Bereitstellung und für die Teilnahme an der Lync Server-Kommunikation autorisieren. Diese Vertrauensstellung wird als Partnerverbund bezeichnet, und es besteht weder ein Zusammenhang mit noch eine Abhängigkeit von einer Active Directory-Vertrauensstellung.

Zur Unterstützung des Benutzerzugriffs auf Partnerdomänen müssen Sie den Partnerverbund aktivieren. Wenn Sie den Partnerverbund für Ihre Organisation aktivieren, müssen Sie auch angeben, ob die folgenden Optionen implementiert werden sollen:

- Partnerdomänenerkennung aktivieren. Wenn Sie diese Option aktivieren, verwendet Lync Server 2010 DNS-Einträge (Domain Name System), um Domänen zu suchen, die nicht in der Liste der zulässigen Domänen aufgeführt sind. Darüber hinaus wird der eingehende Datenverkehr von ermittelten Verbundpartnern automatisch ausgewertet und je nach Vertrauensebene, Umfang des Datenverkehrs und den Administratoreinstellungen eingeschränkt oder blockiert. Wenn Sie diese Option nicht aktivieren, wird der Partnerbenutzerzugriff nur für Benutzer in Domänen aktiviert, die Sie der Liste der

zulässigen Domänen hinzugefügt haben. Unabhängig von der Aktivierung dieser Option können Sie festlegen, ob einzelne Domänen blockiert oder zugelassen werden, und Sie können den Zugriff auf bestimmte Server in der Partnerdomäne einschränken, auf denen der Zugriffs-Edgedienst ausgeführt wird. Ausführliche Informationen zum Steuern des Zugriffs durch Partnerdomänen finden Sie unter Steuern des Zugriffs durch einzelne Partnerdomänen.

- Senden Sie einen Archivierungshaftungsausschluss an Verbundpartner, um sie darüber zu informieren, dass die Kommunikation aufgezeichnet wird. Wenn Sie die Archivierung der externen Kommunikation mit Verbundpartnerdomänen unterstützen, sollten Sie die Benachrichtigung über den Archivierungshaftungsausschluss aktivieren, um die Partner über die Archivierung ihrer Nachrichten in Kenntnis zu setzen.

Wenn Sie den Zugriff durch Benutzer von Partnerdomänen zu einem späteren Zeitpunkt temporär oder dauerhaft unterbinden möchten, können Sie den Partnerverbund für Ihre Organisation deaktivieren. Verwenden Sie das Verfahren in diesem Abschnitt, um den Partnerbenutzerzugriff für Ihre Organisation zu aktivieren oder zu deaktivieren, und um die geeigneten Partnerverbundoptionen festzulegen, die für Ihre Organisation unterstützt werden sollen.

Hinweis:
Durch die Aktivierung des Partnerverbunds für Ihre Organisation legen Sie lediglich fest, dass Ihre Server, auf denen der Zugriffs-Edgedienst ausgeführt wird, eine Kommunikation mit Benutzern von Partnerdomänen unterstützen (öffentliche Sofortnachrichtenanbieter eingeschlossen). Benutzer in Partnerdomänen können nicht an Sofortnachrichtensitzungen oder Konferenzen in Ihrer Organisation teilnehmen. Dies ist erst möglich, wenn Sie zusätzlich mindestens eine Richtlinie zur Unterstützung des Partnerbenutzerzugriffs konfigurieren. Benutzer öffentlicher Sofortnachrichten-Dienstanbieter können nicht an Sofortnachrichtensitzungen oder Konferenzen in Ihrer Organisation teilnehmen. Dies ist erst möglich, wenn Sie zusätzlich mindestens eine Richtlinie zur Unterstützung von Verbindungen mit öffentlichen Instant Messaging-Diensten konfigurieren. Ausführliche Informationen zum Konfigurieren von Richtlinien für die Kommunikation mit Benutzern von Partnerdomänen in anderen Organisationen finden Sie unter Verwalten des Zugriffs durch Verbundpartnerbenutzer in der Bereitstellungs- oder Betriebsdokumentation. Wenn Sie außerdem die Kommunikation mit Benutzern von Sofortnachrichten-Dienstanbietern unterstützen möchten, müssen Sie entsprechende Richtlinien konfigurieren. Zusätzlich müssen Sie die Unterstützung für einzelne Dienstanbieter konfigurieren, die Sie unterstützen möchten. Ausführliche Informationen finden Sie unter Verwalten der Unterstützung für Sofortnachrichtenanbieter in der Bereitstellungs- oder Betriebsdokumentation.

So aktivieren oder deaktivieren Sie den Partnerbenutzerzugriff für Ihre Organisation

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Zugriffs-Edgekonfiguration**.

4. Klicken Sie auf der Seite **Zugriffs-Edgekonfiguration** auf **Global**, klicken Sie auf **Bearbeiten**, und klicken Sie dann auf **Details anzeigen**.

5. Führen Sie im Abschnitt **Zugriffs-Edgekonfiguration bearbeiten** einen der folgenden Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Kommunikation mit Partnerbenutzern aktivieren**, um den Partnerbenutzerzugriff für Ihre Organisation zu aktivieren.

   - Deaktivieren Sie das Kontrollkästchen **Kommunikation mit Partnerbenutzern aktivieren**, um den Partnerbenutzerzugriff für Ihre Organisation zu deaktivieren.

6. Führen Sie nach Aktivierung des Kontrollkästchens **Kommunikation mit Partnerbenutzern aktivieren** einen der folgenden Schritte aus:

   a. Aktivieren Sie das Kontrollkästchen **Partnerdomänenerkennung aktivieren**, um die automatische Erkennung von Partnerdomänen zu unterstützen.

   b. Wenn Ihre Organisation die Archivierung der externen Kommunikation unterstützt, aktivieren Sie das Kontrollkästchen **Archivierungshaftungsausschluss an Verbundpartner senden**.

7. Klicken Sie auf **Commit ausführen**.

Sie müssen außerdem mindestens eine Richtlinie für den externen Zugriff konfigurieren, damit Partnerbenutzer mit Benutzern in Ihrer Lync Server 2010-Bereitstellung zusammenarbeiten können. Ausführliche Informationen finden Sie unter Verwalten des Zugriffs durch Verbundpartnerbenutzer in der Bereitstellungs- oder Betriebsdokumentation. Informationen zur Steuerung des Zugriffs für bestimmte Partnerdomänen finden Sie unter

Steuern des Zugriffs durch einzelne Partnerdomänen in der Bereitstellungs- oder Betriebsdokumentation.

Aktivieren oder Deaktivieren des Zugriffs anonymer Benutzer für Ihre Organisation

Anonyme Benutzer sind Benutzer, die nicht über ein Benutzerkonto in den Active Directory-Domänendiensten (Active Directory Domain Services, AD DS) Ihrer Organisation oder in einer unterstützten Partnerdomäne verfügen und zur Remoteteilnahme an einer lokalen Konferenz eingeladen werden können. Wenn Sie die anonyme Teilnahme an Besprechungen zulassen, können anonyme Benutzer (also Benutzer, deren Identität nur durch den Besprechungs- oder Konferenzschlüssel bestätigt wird) an Besprechungen teilnehmen. Um die anonyme Teilnahme zuzulassen, müssen Sie diese Option für Ihre Organisation aktivieren.

Wenn Sie den Zugriff durch anonyme Benutzer zu einem späteren Zeitpunkt temporär oder dauerhaft unterbinden möchten, können Sie die Option für Ihre Organisation deaktivieren. Verwenden Sie das Verfahren in diesem Abschnitt, um den Zugriff durch anonyme Benutzer für Ihre Organisation zu aktivieren oder zu deaktivieren.

Hinweis:
Beim Aktivieren des Zugriffs durch anonyme Benutzer für Ihre Organisation wird lediglich angegeben, dass Ihre Server, auf denen der Zugriffs-Edgedienst ausgeführt wird, den Zugriff durch anonyme Benutzer unterstützen. Anonyme Benutzer können erst an Besprechungen in Ihrer Organisation teilnehmen, wenn Sie zusätzlich mindestens eine Konferenzrichtlinie konfigurieren und auf einen oder mehrere Benutzer oder Benutzergruppen anwenden. Nur Benutzer, denen eine Konferenzrichtlinie zur Unterstützung anonymer Benutzer zugeordnet ist, können anonyme Benutzer zu Besprechungen einladen. Ausführliche Informationen zur Konfiguration von Konferenzrichtlinien für die Unterstützung anonymer Benutzer finden Sie unter Konfigurieren von Konferenzrichtlinien zur Unterstützung anonymer Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

So aktivieren oder deaktivieren Sie den Zugriff durch anonyme Benutzer für Ihre Organisation

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden

zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Zugriffs-Edgekonfiguration**.

4. Klicken Sie auf der Seite **Zugriffs-Edgekonfiguration** auf **Global**, klicken Sie auf **Bearbeiten**, und klicken Sie dann auf **Details anzeigen**.

5. Führen Sie im Abschnitt **Zugriffs-Edgekonfiguration bearbeiten** einen der folgenden Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Kommunikation mit anonymen Benutzern aktivieren**, um den Zugriff durch anonyme Benutzer für Ihre Organisation zu aktivieren.

   - Deaktivieren Sie das Kontrollkästchen **Kommunikation mit anonymen Benutzern aktivieren**, um den Zugriff durch anonyme Benutzer für Ihre Organisation zu deaktivieren.

6. Klicken Sie auf **Commit ausführen**.

Sie müssen außerdem mindestens eine Konferenzrichtlinie zur Unterstützung anonymer Benutzer konfigurieren und zuweisen, um anonymen Benutzern die Teilnahme an Konferenzen zu ermöglichen, die von Benutzern in Ihrer Lync Server 2010-Bereitstellung gehostet werden. Ausführliche Informationen finden Sie unter Konfigurieren von Konferenzrichtlinien zur Unterstützung anonymer Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

Konfigurieren der Kommunikation mit externen Benutzern

Standardmäßig werden keine Richtlinien zur Unterstützung des Zugriffs durch externe Benutzer konfiguriert, einschließlich des Zugriffs durch Remotebenutzer und durch Partnerbenutzer, auch dann nicht, wenn Sie die Unterstützung für den Zugriff durch externe Benutzer bereits für Ihre Organisation aktiviert haben. Zur Steuerung des Zugriffs durch externe Benutzer müssen Sie eine oder mehrere Richtlinien konfigurieren und den für jede Richtlinie unterstützten Typ des externen Benutzerzugriffs angeben. Hierzu gehören die folgenden Richtlinien für den externen Zugriff:

- **Globale Richtlinie** Die globale Richtlinie wird bei der Bereitstellung der Edgeserver erstellt. Standardmäßig sind in der globalen Richtlinie keine Optionen für den externen Benutzerzugriff aktiviert. Zur Unterstützung des Zugriffs durch externe Benutzer auf globaler Ebene konfigurieren Sie die globale Richtlinie so, dass mindestens ein Typ des externen Benutzerzugriffs unterstützt wird. Die globale Richtlinie gilt für alle Benutzer in Ihrer

Organisation, wird jedoch durch Standort- und Benutzerrichtlinien außer Kraft gesetzt. Wenn Sie die globale Richtlinie löschen, wird diese nicht entfernt. Stattdessen wird sie auf die Standardeinstellung zurückgesetzt.

- **Standortrichtlinie** Sie können eine oder mehrere Standortrichtlinien erstellen und konfigurieren, um die Unterstützung für den Zugriff durch externe Benutzer auf bestimmte Standorte einzuschränken. Die Konfiguration in der Standortrichtlinie setzt die globale Richtlinie außer Kraft, jedoch nur für den durch die Standortrichtlinie abgedeckten Standort. Wenn Sie beispielsweise den Remotebenutzerzugriff in der globalen Richtlinie aktivieren, können Sie eine Standortrichtlinie festlegen, die den Remotebenutzerzugriff für einen bestimmten Standort deaktiviert. Standardmäßig wird eine Standortrichtlinie auf alle Benutzer des jeweiligen Standorts angewendet, Sie können jedoch einem Benutzer eine Benutzerrichtlinie zuweisen, um die Standortrichtlinieneinstellung außer Kraft zu setzen.

- **Benutzerrichtlinie** Sie können eine oder mehrere Benutzerrichtlinien erstellen und konfigurieren, um die Unterstützung für den Zugriff durch Remotebenutzer auf bestimmte Benutzer einzuschränken. Die Konfiguration in der Benutzerrichtlinie setzt die Richtlinien auf globaler und Standortebene außer Kraft. Dies gilt jedoch nur für die Benutzer, denen die Benutzerrichtlinie zugewiesen wird. Wenn Sie beispielsweise den Zugriff durch Remotebenutzer in der globalen und in der Standortrichtlinie aktivieren, können Sie eine Benutzerrichtlinie festlegen, die den Zugriff durch Remotebenutzer deaktiviert. Anschließend können Sie diese Benutzerrichtlinie bestimmten Benutzern zuweisen. Wenn Sie eine Benutzerrichtlinie erstellen, müssen Sie sie auf einen oder mehrere Benutzer anwenden, damit sie wirksam wird.

Sie müssen eine Konferenzrichtlinie konfigurieren und Benutzern zuweisen, um die Teilnahme anonymer Benutzer an Konferenzen zu unterstützen. Indem Sie Benutzern oder Benutzergruppen eine Konferenzrichtlinie zuweisen, in der die anonyme Teilnahme aktiviert wird, ermöglichen Sie diesen Benutzern das Einladen anonymer Benutzer zu von ihnen organisierten Konferenzen.

Neben Richtlinien für den externen Benutzerzugriff und Konferenzrichtlinien erfordern einige Optionen für den externen Benutzerzugriff die Konfiguration weiterer Optionen. Hierzu gehören auch der Zugriff durch Partnerbenutzer und der Zugriff durch öffentliche Benutzer. Dies umfasst Folgendes:

- Die Angabe zulässiger und blockierter Domänen für Verbundpartner, einschließlich aller spezifischen Server, auf denen der Zugriffs-Edgedienst ausgeführt wird, den Sie zulassen oder blockieren möchten.

- Die Angabe der spezifischen Dienstanbieter, die von Ihrer Organisation unterstützt werden, einschließlich des Namens des Servers, auf dem der Zugriffs-Edgedienst ausgeführt wird, sowie die für den Anbieter unterstützte Überprüfungsstufe.

Inhalt dieses Abschnitts

- Verwalten des Remotebenutzerzugriffs
- Verwalten des Zugriffs durch Verbundpartnerbenutzer
- Verwalten der Unterstützung für Sofortnachrichtenanbieter
- Konfigurieren von Konferenzrichtlinien zur Unterstützung anonymer Benutzer
- Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer

Verwalten des Remotebenutzerzugriffs

Sie konfigurieren eine oder mehrere Richtlinien für den Zugriff externer Benutzer und steuern, ob Remotebenutzer mit internen Lync Server-Benutzern zusammenarbeiten können. Zum Steuern des Zugriffs durch Remotebenutzer können Sie Richtlinien auf globaler, Standort- und Benutzerebene konfigurieren. Standortrichtlinien setzen die globale Richtlinie außer Kraft, und Benutzerrichtlinien setzen Standort- und globale Richtlinien außer Kraft. Ausführliche Informationen zu den konfigurierbaren Richtlinientypen finden Sie unter „Verwalten der Kommunikation mit externen Benutzern“ in der Bereitstellungs- oder Planungsdokumentation.

Hinweis:
Sie können auch dann Richtlinien zur Steuerung des Zugriffs durch Remotebenutzer konfigurieren, wenn Sie den Zugriff durch Remotebenutzer für Ihre Organisation nicht aktiviert haben. Die von Ihnen konfigurierten Richtlinien treten jedoch erst in Kraft, wenn der Zugriff durch Remotebenutzer für Ihre Organisation aktiviert wird. Ausführliche Informationen zum Aktivieren des Remotebenutzerzugriffs finden Sie unter Aktivieren oder Deaktivieren des Zugriffs durch Remotebenutzer für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation. Wenn Sie eine Benutzerrichtlinie zur Steuerung des Zugriffs durch Remotebenutzer angeben, gilt die Richtlinie zudem nur für Benutzer, die für Lync Server 2010 aktiviert und für die Verwendung der Richtlinie konfiguriert wurden. Ausführliche Informationen zum Angeben von Benutzern, die sich von Remotestandorten aus bei Lync Server 2010 anmelden können, finden Sie unter Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

Führen Sie die folgenden Schritte aus, um die einzelnen Richtlinien für den externen Zugriff zu konfigurieren, die zur Steuerung des Remotebenutzerzugriffs verwendet werden sollen.

Hinweis:
In diesem Verfahren wird lediglich beschrieben, wie Sie eine Richtlinie zum Aktivieren der Kommunikation mit Remotebenutzern konfigurieren. Sämtliche Richtlinien, die Sie für die Unterstützung des Remotebenutzerzugriffs konfigurieren, können jedoch ebenfalls zur Unterstützung des Zugriffs durch Partnerbenutzer und öffentliche Benutzer

verwendet werden. Ausführliche Informationen zur Konfiguration von Richtlinien für die Unterstützung von Partnerbenutzern finden Sie unter Konfigurieren von Richtlinien zur Steuerung des Partnerbenutzerzugriffs. Ausführliche Informationen zur Konfiguration von Richtlinien für die Unterstützung von öffentlichen Benutzern finden Sie unter Konfigurieren von Richtlinien zur Steuerung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern.

So konfigurieren Sie eine Richtlinie für den externen Zugriff für die Unterstützung des Zugriffs durch Remotebenutzer

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Externe Zugriffsrichtlinie**.

4. Führen Sie auf der Seite **Externe Zugriffsrichtlinie** einen der folgenden Schritte aus:

    - Um die globale Richtlinie für die Unterstützung des Zugriffs durch Remotebenutzer zu konfigurieren, klicken Sie auf die globale Richtlinie, dann auf **Bearbeiten** und schließlich auf **Details anzeigen**.

    - Klicken Sie zum Erstellen einer neuen Standortrichtlinie auf **Neu** und anschließend auf **Standortrichtlinie**. Klicken Sie im Dialogfeld **Standort auswählen** in der Liste auf den entsprechenden Standort, und klicken Sie dann auf **OK**.

    - Klicken Sie zum Erstellen einer neuen Benutzerrichtlinie auf **Neu** und anschließend auf **Benutzerrichtlinie**. Erstellen Sie unter **Neue externe Zugriffsrichtlinie** einen eindeutigen Namen im Feld **Name**, der auf den Zweck der Benutzerrichtlinie hinweist (z. B. **EnableRemoteUsers** für eine Benutzerrichtlinie, welche die Kommunikation für Remotebenutzer ermöglicht).

    - Klicken Sie zum Ändern einer vorhandenen Richtlinie in der Tabelle auf die entsprechende Richtlinie, klicken Sie auf **Bearbeiten** und anschließend auf **Details anzeigen**.

5. (Optional) Wenn Sie eine Beschreibung hinzufügen oder bearbeiten möchten, geben Sie die Informationen zur Richtlinie unter **Beschreibung** an.

6. Führen Sie einen der folgenden Schritte aus:

    - Aktivieren Sie das Kontrollkästchen **Kommunikation mit Remotebenutzern aktivieren**, um den Zugriff durch Remotebenutzer für die Richtlinie zu aktivieren.

    - Deaktivieren Sie das Kontrollkästchen **Kommunikation mit Remotebenutzern aktivieren**, um den Zugriff durch Remotebenutzer für die Richtlinie zu deaktivieren.

7. Klicken Sie auf **Commit ausführen**.

Um den Zugriff durch Remotebenutzer zu ermöglichen, müssen Sie auch die Unterstützung für den Remotebenutzerzugriff in Ihrer Organisation aktivieren. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Zugriffs durch Remotebenutzer für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation.

Handelt es sich um eine Benutzerrichtlinie, müssen Sie die Richtlinie auch auf Benutzer anwenden, für die Sie eine Remoteverbindung zulassen möchten. Ausführliche Informationen finden Sie unter Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

Verwalten des Zugriffs durch Verbundpartnerbenutzer

Sie müssen die beiden folgenden Aufgaben ausführen, um die Unterstützung von Benutzern in Partnerdomänen zu konfigurieren:

- Konfigurieren Sie eine oder mehrere Richtlinien für den externen Benutzerzugriff, um Benutzer in Partnerdomänen zu unterstützen.

- Geben Sie spezifische Partnerdomänen an, die Sie zulassen oder blockieren möchten.

Wenn Sie die Unterstützung für den Partnerverbund aktiviert haben, müssen Sie zusätzlich angeben, ob die automatische Erkennung von Partnerdomänen zugelassen wird. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungsdokumentation.

Inhalt dieses Abschnitts

- Konfigurieren von Richtlinien zur Steuerung des Partnerbenutzerzugriffs

- Steuern des Zugriffs durch einzelne Partnerdomänen

Konfigurieren von Richtlinien zur Steuerung des Partnerbenutzerzugriffs

Wenn Sie Richtlinien zur Unterstützung von Verbundpartnern konfigurieren, gelten die Richtlinien für Benutzer von Partnerdomänen, jedoch nicht für Benutzer von Sofortnachrichten-Dienstanbietern (z. B. Windows Live), solange Sie nicht auch die Unterstützung für Benutzer von Dienstanbietern in dieser Richtlinie aktivieren. Sie können eine oder mehrere Richtlinien für den Zugriff externer Benutzer konfigurieren und steuern, ob Benutzer von Partnerdomänen mit internen Lync Server-Benutzern zusammenarbeiten können. Zum Steuern des Zugriffs durch Partnerbenutzer können Sie Richtlinien auf globaler, Standort- und Benutzerebene konfigurieren. Standortrichtlinien setzen die globale Richtlinie außer Kraft, und Benutzerrichtlinien setzen Standort- und globale Richtlinien außer Kraft. Ausführliche Informationen zu den konfigurierbaren Richtlinientypen finden Sie unter „Verwalten der Kommunikation mit externen Benutzern“ in der Bereitstellungs- oder Planungsdokumentation.

Hinweis:
Sie können auch dann Richtlinien zur Steuerung des Zugriffs durch Partnerbenutzer konfigurieren, wenn Sie den Partnerverbund für Ihre Organisation nicht aktiviert haben. Die von Ihnen konfigurierten Richtlinien treten jedoch erst dann in Kraft, wenn der Partnerverbund für Ihre Organisation aktiviert ist. Ausführliche Informationen zum Aktivieren des Partnerverbunds finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation. Wenn Sie eine Benutzerrichtlinie zur Steuerung des Zugriffs durch Partnerbenutzer angeben, gilt die Richtlinie zudem nur für Benutzer, die für Lync Server 2010 aktiviert und für die Verwendung der Richtlinie konfiguriert wurden. Ausführliche Informationen zum Angeben von Partnerbenutzern, die sich bei Lync Server 2010 anmelden können, finden Sie unter Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

So konfigurieren Sie eine Richtlinie zur Unterstützung des Zugriffs durch Benutzer von Partnerdomänen

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.
2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.
3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Externe Zugriffsrichtlinie**.

4. Führen Sie auf der Seite **Externe Zugriffsrichtlinie** einen der folgenden Schritte aus:

    - Um die globale Richtlinie für die Unterstützung des Zugriffs durch Partnerbenutzer zu konfigurieren, klicken Sie auf die globale Richtlinie, dann auf **Bearbeiten** und schließlich auf **Details anzeigen**.

    - Klicken Sie zum Erstellen einer neuen Standortrichtlinie auf **Neu** und anschließend auf **Standortrichtlinie**. Klicken Sie im Dialogfeld **Standort auswählen** in der Liste auf den entsprechenden Standort, und klicken Sie dann auf **OK**.

    - Klicken Sie zum Erstellen einer neuen Benutzerrichtlinie auf **Neu** und anschließend auf **Benutzerrichtlinie**. Erstellen Sie unter **Neue externe Zugriffsrichtlinie** einen eindeutigen Namen im Feld **Name**, der auf den Zweck der Benutzerrichtlinie hinweist (z. B. **EnableFederatedUsers** für eine Benutzerrichtlinie, welche die Kommunikation für Benutzer aus Partnerdomänen ermöglicht).

    - Klicken Sie zum Ändern einer vorhandenen Richtlinie in der Tabelle auf die entsprechende Richtlinie, klicken Sie auf **Bearbeiten** und anschließend auf **Details anzeigen**.

5. (Optional) Wenn Sie eine Beschreibung hinzufügen oder bearbeiten möchten, geben Sie die Informationen zur Richtlinie unter **Beschreibung** an.

6. Führen Sie einen der folgenden Schritte aus:

    - Aktivieren Sie das Kontrollkästchen **Kommunikation mit Partnerbenutzern aktivieren**, um den Zugriff durch Partnerbenutzer für die Richtlinie zu aktivieren.

    - Deaktivieren Sie das Kontrollkästchen **Kommunikation mit Partnerbenutzern aktivieren**, um den Zugriff durch Partnerbenutzer für die Richtlinie zu deaktivieren.

7. Klicken Sie auf **Commit ausführen**.

Um den Zugriff durch Partnerbenutzer zu ermöglichen, müssen Sie auch die Unterstützung für den Partnerverbund in Ihrer Organisation aktivieren. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation.

Handelt es sich um eine Benutzerrichtlinie, müssen Sie die Richtlinie auch auf Benutzer anwenden, die mit Partnerbenutzern zusammenarbeiten sollen. Ausführliche Informationen finden Sie unter Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

Steuern des Zugriffs durch einzelne Partnerdomänen

Wenn Sie die Unterstützung für Verbundpartner konfiguriert haben, können Sie verwalten, welche speziellen Domänen mit Ihrer Organisation eine Partnerschaft eingehen können, indem Sie einen oder beide der folgenden Schritte ausführen:

- Konfigurieren Sie eine oder mehrere spezifische externe Domänen als zulässige Partnerdomänen. Fügen Sie hierzu jede Domäne der Liste zulässiger Domänen hinzu. Selbst wenn die Erkennung von Verbundpartnern für Ihre Organisation aktiviert ist, führen Sie diesen Schritt aus, wenn es sich bei der Domäne um einen Verbundpartner handelt, der mit mehr als 1.000 Ihrer Benutzer kommunizieren oder mehr als 20 Nachrichten pro Sekunde senden muss. Ist die Erkennung von Verbundpartnern für Ihre Organisation nicht aktiviert, können nur Benutzer aus externen Domänen am Instant Messaging und an Konferenzen mit Benutzern Ihrer Organisation teilnehmen, die Sie der Liste zulässiger Domänen hinzugefügt haben. Wenn Sie den Zugriff einer Partnerdomäne auf einen bestimmten Server beschränken möchten, auf dem der Zugriffs-Edgedienst des Verbundpartners ausgeführt wird, können Sie für jede Domäne in der Liste zulässiger Domänen den Domänennamen des Servers angeben, auf dem der Zugriffs-Edgedienst ausgeführt wird.

- Blockieren Sie eine oder mehrere externe Domänen am Herstellen einer Verbindung mit Ihrer Organisation. Fügen Sie hierzu die Domäne der Liste blockierter Domänen hinzu.

Hinweis:
Dieses Verfahren beschreibt, wie Sie die Unterstützung für bestimmte Domänen konfigurieren. Zur Implementierung der Unterstützung für Partnerbenutzer gehört jedoch auch, dass Sie die Unterstützung für Partnerbenutzer für Ihre Organisation aktivieren sowie Richtlinien konfigurieren und anwenden, um zu steuern, welche Benutzer mit Partnerbenutzern zusammenarbeiten können. Ausführliche Informationen zum Aktivieren der Unterstützung für Partnerbenutzer finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation. Ausführliche Informationen zum Konfigurieren von Richtlinien zur Steuerung des Partnerverbunds finden Sie unter Konfigurieren von Richtlinien zur Steuerung des Partnerbenutzerzugriffs in der Bereitstellungs- oder Betriebsdokumentation.

So fügen Sie eine externe Domäne der Liste zulässiger Domänen hinzu

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync

Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Partnerdomänen**.

4. Klicken Sie auf der Seite **Partnerdomänen** auf **Neu** und anschließend auf **Zulässige Domäne**.

5. Führen Sie unter **Neue Partnerdomänen** die folgenden Schritte aus:

    - Geben Sie unter **Domänenname (oder FQDN)** den Namen der Verbundpartnerdomäne ein.

        Hinweis:

Dieser Name muss eindeutig sein und darf noch nicht als zulässige Domäne für diesen Server vorliegen, auf dem der Zugriffs-Edgedienst ausgeführt wird. Der Name darf höchstens 256 Zeichen lang sein.

Bei der Suche nach dem Namen der Verbundpartnerdomäne wird ein Suffixabgleich durchgeführt. Wenn Sie beispielsweise **contoso.com** eingeben, wird als Suchergebnis auch die Domäne **it.contoso.com** zurückgegeben.

Eine Verbundpartnerdomäne kann nicht gleichzeitig blockiert und zugelassen werden. Lync Server 2010 verhindert dies automatisch, sodass Sie Ihre Listen nicht synchronisieren müssen.

- Wenn Sie den Zugriff für diese Partnerdomäne auf Benutzer eines bestimmten Servers beschränken möchten, auf dem der Zugriffs-Edgedienst ausgeführt wird, geben Sie unter **Zugriffs-Edgedienst (FQDN)** den FQDN des Servers der Partnerdomäne ein, auf dem der Zugriffs-Edgedienst ausgeführt wird.

- Wenn Sie zusätzliche Informationen bereitstellen möchten, geben Sie unter **Kommentar** Informationen ein, die Sie anderen Systemadministratoren über diese Konfiguration mitteilen möchten.

6. Klicken Sie auf **Commit ausführen**.

7. Wiederholen Sie die Schritte 4 bis 6 für jede Verbundpartnerdomäne, die Sie zulassen möchten.

Um den Zugriff durch Partnerbenutzer zu ermöglichen, müssen Sie auch die Unterstützung für den Partnerbenutzerzugriff in Ihrer Organisation aktivieren. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation.

Zusätzlich müssen Sie die Richtlinie konfigurieren und auf Benutzer anwenden, die mit Partnerbenutzern zusammenarbeiten sollen. Ausführliche Informationen finden Sie unter Konfigurieren von Richtlinien zur Steuerung des Partnerbenutzerzugriffs in der Bereitstellungs- oder Betriebsdokumentation.

So fügen Sie eine externe Domäne der Liste blockierter Domänen hinzu

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer**.

4. Klicken Sie auf **Partnerdomänen**, dann auf **Neu** und anschließend auf **Blockierte Domäne**.

5. Führen Sie unter **Neue Partnerdomänen** die folgenden Schritte aus:

    - Geben Sie unter **Domänenname (oder FQDN)** den Namen der Verbundpartnerdomäne ein, die Sie blockieren möchten.

        Hinweis:
Der Name darf höchstens 256 Zeichen lang sein.

Bei der Suche nach dem Namen der Verbundpartnerdomäne wird ein Suffixabgleich durchgeführt. Wenn Sie beispielsweise **contoso.com** eingeben, wird als Suchergebnis auch die Domäne **it.contoso.com** zurückgegeben.

Eine Verbundpartnerdomäne kann nicht gleichzeitig blockiert und zugelassen werden. Lync Server 2010 verhindert dies automatisch, sodass Sie Ihre Listen nicht synchronisieren müssen.

    - (Optional) Geben Sie unter **Kommentar** Informationen ein, die Sie anderen Systemadministratoren über diese Konfiguration mitteilen möchten.

6. Klicken Sie auf **Commit ausführen**.

7. Wiederholen Sie die Schritte 4 bis 6 für jeden Verbundpartner, den Sie blockieren möchten.

Verwalten der Unterstützung für Sofortnachrichtenanbieter

Sie müssen die folgenden Schritte ausführen, um die Unterstützung für Benutzer zu aktivieren, die öffentliche Sofortnachrichtenanbieter (Instant Messaging) nutzen:

- Konfigurieren Sie eine oder mehrere Richtlinien für den externen Benutzerzugriff, um die Verwendung öffentlicher Sofortnachrichtendienste zu unterstützen.
- Geben Sie an, welche öffentlichen Sofortnachrichtenanbieter Sie unterstützen möchten.

Verwenden Sie zur Ausführung dieser Aufgaben die Verfahren in diesem Abschnitt.

Inhalt dieses Abschnitts

- Konfigurieren von Richtlinien zur Steuerung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern
- Angeben der unterstützten Sofortnachrichten-Dienstanbieter

Konfigurieren von Richtlinien zur Steuerung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern

Über Verbindungen mit öffentlichen Instant Messaging-Diensten können Benutzer in Ihrer Organisation per Sofortnachricht mit Benutzern von Sofortnachrichtendiensten kommunizieren, die von öffentlichen Sofortnachrichten-Dienstanbietern bereitgestellt werden, z. B. vom Windows Live-Internetdienstnetzwerk, von Yahoo! und von AOL. Sie konfigurieren eine oder mehrere Richtlinien für den Zugriff externer Benutzer und steuern, ob öffentliche Benutzer mit internen Lync Server-Benutzern zusammenarbeiten können. Zum Steuern des Zugriffs durch öffentliche Benutzer können Sie Richtlinien auf globaler, Standort- und Benutzerebene konfigurieren. Standortrichtlinien setzen die globale Richtlinie außer Kraft, und Benutzerrichtlinien setzen Standort- und globale Richtlinien außer Kraft. Ausführliche Informationen zu den konfigurierbaren Richtlinientypen finden Sie unter „Verwalten der Kommunikation mit externen Benutzern“ in der Bereitstellungs- oder Planungsdokumentation.

Im Fall von Sofortnachrichten-Einladungen hängt die Antwort von der Clientsoftware ab. Die Anforderung wird akzeptiert, sofern externe Absender nicht ausdrücklich durch eine vom Benutzer konfigurierte Regel (also Einstellungen in der Liste **Zulassen** und **Blockieren** des Benutzers) blockiert werden. Darüber hinaus können Sofortnachrichten-Einladungen blockiert werden, wenn ein Benutzer festlegt, dass alle Sofortnachrichten von Benutzern, die nicht in der Liste **Zulassen** enthalten sind, blockiert werden.

Hinweis:
Sie können auch dann Richtlinien zur Steuerung des Zugriffs durch öffentliche Benutzer konfigurieren, wenn Sie den Partnerverbund für Ihre Organisation nicht aktiviert haben. Die von Ihnen konfigurierten Richtlinien treten jedoch erst dann in Kraft, wenn der

Partnerverbund für Ihre Organisation aktiviert ist. Ausführliche Informationen zum Aktivieren des Partnerverbunds finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation. Wenn Sie eine Benutzerrichtlinie zur Steuerung des Zugriffs durch öffentliche Benutzer angeben, gilt die Richtlinie zudem nur für Benutzer, die für Lync Server 2010 aktiviert und für die Verwendung der Richtlinie konfiguriert wurden. Ausführliche Informationen zum Angeben öffentlicher Benutzer, die sich bei Lync Server 2010 anmelden können, finden Sie unter Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

Gehen Sie folgendermaßen vor, um eine Richtlinie zur Unterstützung des Zugriffs durch Benutzer eines oder mehrerer öffentlicher Sofortnachrichtenanbieter zu konfigurieren.

So konfigurieren Sie eine Richtlinie für den externen Zugriff für die Unterstützung des Zugriffs durch öffentliche Benutzer

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Externe Zugriffsrichtlinie**.

4. Führen Sie auf der Seite **Externe Zugriffsrichtlinie** einen der folgenden Schritte aus:

   - Um die globale Richtlinie für die Unterstützung des Zugriffs durch öffentliche Benutzer zu konfigurieren, klicken Sie auf die globale Richtlinie, dann auf **Bearbeiten** und schließlich auf **Details anzeigen**.

   - Klicken Sie zum Erstellen einer neuen Standortrichtlinie auf **Neu** und anschließend auf **Standortrichtlinie**. Klicken Sie im Dialogfeld **Standort auswählen** in der Liste auf den entsprechenden Standort, und klicken Sie dann auf **OK**.

   - Klicken Sie zum Erstellen einer neuen Benutzerrichtlinie auf **Neu** und anschließend auf **Benutzerrichtlinie**. Erstellen Sie unter **Neue externe Zugriffsrichtlinie** einen eindeutigen Namen im Feld **Name**, der auf den Zweck der Benutzerrichtlinie hinweist (z. B. **EnablePublicUsers** für eine Benutzerrichtlinie, welche die

Kommunikation für öffentliche Benutzer ermöglicht).

- Klicken Sie zum Ändern einer vorhandenen Richtlinie in der Tabelle auf die entsprechende Richtlinie, klicken Sie auf **Bearbeiten** und anschließend auf **Details anzeigen**.

5. (Optional) Wenn Sie eine Beschreibung hinzufügen oder bearbeiten möchten, geben Sie die Informationen zur Richtlinie unter **Beschreibung** an.
6. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen **Kommunikation mit öffentlichen Benutzern aktivieren**, um den Zugriff durch öffentliche Benutzer für die Richtlinie zu aktivieren.
   - Deaktivieren Sie das Kontrollkästchen **Kommunikation mit öffentlichen Benutzern aktivieren**, um den Zugriff durch öffentliche Benutzer für die Richtlinie zu deaktivieren.
7. Klicken Sie auf **Commit ausführen**.

Um den Zugriff durch öffentliche Benutzer zu ermöglichen, müssen Sie auch die Unterstützung für den Partnerverbund in Ihrer Organisation aktivieren. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation.

Handelt es sich um eine Benutzerrichtlinie, müssen Sie die Richtlinie auch auf öffentliche Benutzer anwenden, die mit öffentlichen Benutzern zusammenarbeiten sollen. Ausführliche Informationen finden Sie unter Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

Angeben der unterstützten Sofortnachrichten-Dienstanbieter

Benutzer öffentlicher Instant Messaging-Dienste, einschließlich der folgenden: Windows Live, AOL und Yahoo! sowie XMPP-Anbieter und -Server (Extensible Messaging and Presence Protocol), z. B. Google Talk oder Jabber, über ein XMPP-Gateway. Ein öffentlicher Instant Messaging-Dienstanbieter ist ein bestimmter Typ von Verbundpartner. Die Unterstützung für Benutzer öffentlicher Instant Messaging-Dienste stellt bestimmte Anforderungen, die sich von den Anforderungen für Benutzer anderer Verbundpartner unterscheiden. Kunden ohne Volumenlizenz für Lync Server 2010 benötigen eine separate Lizenz, wenn sie Verbindungen mit öffentlichen Instant Messaging-Diensten wie Windows Live, AOL und Yahoo! konfigurieren. Ausführliche Informationen finden Sie im Abschnitt „Changes in Office Communications Server Public IM Federation“ unter http://go.microsoft.com/fwlink/?linkid=197275&clcid=0x407 und im Abschnitt „Microsoft Lync: Pricing and Licensing“ unter http://go.microsoft.com/fwlink/?LinkId=202848&clcid=0x407.

Hinweis:
Für die Verwendung von XMPP müssen Sie das XMPP-Gateway installieren.
Das XMPP-Gateway steht unter der folgenden Adresse im Microsoft Download Center zum Download bereit: http://go.microsoft.com/fwlink/?LinkId=204552&clcid=0x407. Nach der Installation des XMPP-Gateways müssen Sie den Hotfix installieren, der unter der folgenden Adresse heruntergeladen werden kann:
http://go.microsoft.com/fwlink/?LinkId=204561&clcid=0x407.

Sie können einen Sofortnachrichten-Dienstanbieter hinzufügen oder entfernen und andere Einstellungen für die einzelnen Sofortnachrichten-Dienstanbieter ändern (z. B. den Sofortnachrichten-Dienstanbieter vorübergehend blockieren). Für jeden Sofortnachrichten-Dienstanbieter können Sie folgende Einstellungen festlegen:

- Ob der Sofortnachrichten-Dienstanbieter gehostet wird oder öffentlich ist. Gehostete Sofortnachrichten-Dienstanbieter sind in Ihrer Organisation intern und werden als gehostete Dienste ausgeführt. Einige Organisationen ermöglichen externen Benutzern das Herstellen eines Partnerverbunds mit internen Servern als Hostinganbieter, ähnlich der Herstellung eines Partnerverbunds mit einem öffentlichen Anbieter wie MSN.

- Ob ein Verbund des Sofortnachrichten-Dienstanbieters mit Ihrer Organisation zulässig ist.

- Die Netzwerkadresse für den Zugriffsedge des Sofortnachrichten-Dienstanbieters, den Sie über den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Servers angeben, auf dem der Zugriffs-Edgedienst ausgeführt wird.

- Für eingehende Kommunikation stehen folgende Filteroptionen zur Verfügung:

    - **Kommunikation nur mit Benutzern zulassen, die von diesem Anbieter bestätigt wurden** Dies ist die Standardeinstellung. Sie bedeutet, dass Sie den Überprüfungsstufen des Sofortnachrichten-Dienstanbieters vertrauen und eingehende Nachrichten entsprechend behandelt werden. Als unbestätigt markierte Anforderungen werden entsprechend der Beschreibung für die Option **Kommunikation nur mit Benutzern zulassen, die in den Kontaktlisten der Empfänger enthalten sind** behandelt.
      Als bestätigt markierte Anforderungen werden entsprechend der Beschreibung für die Option **Gesamte Kommunikation mit diesem Anbieter zulassen** behandelt.

    - **Kommunikation nur mit Benutzern zulassen, die in den Kontaktlisten der Empfänger enthalten sind** Diese Einstellung bedeutet, dass Sie den Überprüfungsstufen des Sofortnachrichten-Dienstanbieters nicht vertrauen. Wenn Sie diese Option wählen, kennzeichnet der Server, auf dem der Zugriffs-Edgedienst ausgeführt wird, alle eingehenden Anwesenheitsabonnementanforderungen als nicht überprüft. Wenn der Absender bereits auf der Zulassungsliste des Empfängers enthalten ist,

wird die Anforderung vom internen Server beantwortet. Andernfalls wird die Anforderung abgelehnt. Dementsprechend werden auch Anforderungen für eine Sofortnachrichtensitzung, die als nicht überprüft gekennzeichnet sind, vom Client zurückgewiesen.

- **Gesamte Kommunikation mit diesem Anbieter zulassen** Diese Einstellung bedeutet, dass Sie alle Nachrichten akzeptieren, unabhängig davon, ob sie überprüft wurden. Wenn Sie diese Option wählen, kennzeichnet der Server, auf dem der Zugriffs-Edgedienst ausgeführt wird, alle Nachrichten als überprüft. Der Pool oder Server des Empfängers benachrichtigt den Client, und alle Nachrichten werden entsprechend den Clienteinstellungen verarbeitet. Bei Anwesenheitsabonnementanforderungen wird anhand der Clienteinstellungen bestimmt, wie eine Nachricht verarbeitet wird.

Windows Live, AOL und Yahoo! sind standardmäßig in dieser Liste verfügbar, jedoch nicht aktiviert. Für einen öffentlichen Sofortnachrichten-Dienstanbieter müssen für Verbindungen mit öffentlichen Instant Messaging-Diensten möglicherweise zusätzliche Dienstlizenzen gekauft und die Verbindungen bereitgestellt werden. Ausführliche Informationen finden Sie in den Lync Server 2010-Lizenzierungsinformationen unter http://go.microsoft.com/fwlink/?LinkId=202848&clcid=0x407. Preis- und Lizenzierungsinformationen für Verbindungen mit öffentlichen Instant Messaging-Diensten stehen über Microsoft-Volumenlizenzprogramme zur Verfügung. Ausführliche Informationen finden Sie auf der Seite des Volume Licensing Service Center unter http://go.microsoft.com/fwlink/?LinkId=144874&clcid=0x407. Ausführliche Informationen zu den speziellen Anforderungen für öffentliche Sofortnachrichten-Dienstanbieter finden Sie in „Office Communications Server Public IM Connectivity Provisioning Guide“ unter http://go.microsoft.com/fwlink/?LinkId=155970&clcid=0x407.

Hinweis:
Sie können auch dann die Unterstützung für öffentliche Sofortnachrichtenanbieter konfigurieren, wenn Sie den Partnerverbund für Ihre Organisation nicht aktiviert haben. Die von Ihnen konfigurierte Anbieterunterstützung tritt jedoch erst dann in Kraft, wenn der Partnerverbund für Ihre Organisation aktiviert ist. Ausführliche Informationen zum Aktivieren des Partnerverbunds finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation. Zusätzlich erfordert die Unterstützung für Sofortnachrichten-Dienstanbieter die Konfiguration von Richtlinien zur Unterstützung des Benutzerzugriffs. Ausführliche Informationen zur Konfiguration von Richtlinien zur Unterstützung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern finden Sie unter Konfigurieren von Richtlinien zur Steuerung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern.

Gehen Sie folgendermaßen vor, um die Unterstützung von Sofortnachrichtenanbietern für einen oder mehrere gehostete oder öffentliche Sofortnachrichten-Dienstanbieter zu konfigurieren.

So konfigurieren Sie die Unterstützung für einen Sofortnachrichten-Dienstanbieter

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer** und dann auf **Anbieter**. Führen Sie anschließend einen der folgenden Schritte aus:

   - Klicken Sie zum Erstellen eines neuen Anbieters auf **Neu** und anschließend auf **Öffentlich** bzw. **Gehostet**.

     Hinweis:
     Wählen Sie **Gehostet** aus, wenn Ihr Sofortnachrichten-Dienstanbieter in Ihrer Organisation intern ist und als gehostete Dienste ausgeführt wird.
     Einige Organisationen ermöglichen externen Benutzern das Herstellen eines Partnerverbunds mit internen Servern als Hostinganbieter, ähnlich der Herstellung eines Partnerverbunds mit einem öffentlichen Anbieter wie MSN.

   - Erstellen Sie unter **Anbietername** einen eindeutigen Namen.

   - Geben Sie unter **Zugriffsedge (oder FQDN)** den Namen jedes einzelnen Servers ein, auf dem der Zugriffs-Edgedienst ausgeführt wird.

4. Führen Sie einen der folgenden Schritte aus:

   - Zum Aktivieren dieses Anbieters aktivieren Sie das Kontrollkästchen **Kommunikation mit diesem Anbieter aktivieren**, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf **Kommunikation nur mit Benutzern zulassen, die von diesem Anbieter bestätigt wurden**.

   - Aktivieren Sie das Kontrollkästchen **Kommunikation nur mit Benutzern zulassen,**

die in den Kontaktlisten der Empfänger enthalten sind.

- Aktivieren Sie das Kontrollkästchen **Gesamte Kommunikation mit diesem Anbieter zulassen**.
- Um die Kommunikation mit diesem Anbieter zu verhindern, deaktivieren Sie das Kontrollkästchen **Kommunikation mit diesem Anbieter aktivieren**.

5. Klicken Sie zum Ändern eines vorhandenen Anbieters in der Tabelle auf den entsprechenden Anbieter, klicken Sie auf **Bearbeiten** und anschließend auf **Details anzeigen**. Führen Sie anschließend einen der folgenden Schritte aus:

   - Zum Aktivieren dieses Anbieters aktivieren Sie das Kontrollkästchen **Kommunikation mit diesem Anbieter aktivieren**, und führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Kommunikation nur mit Benutzern zulassen, die von diesem Anbieter bestätigt wurden**.
   - Aktivieren Sie das Kontrollkästchen **Kommunikation nur mit Benutzern zulassen, die in den Kontaktlisten der Empfänger enthalten sind**.
   - Aktivieren Sie das Kontrollkästchen **Gesamte Kommunikation mit diesem Anbieter zulassen**.
   - Um die Kommunikation mit diesem Anbieter zu verhindern, deaktivieren Sie das Kontrollkästchen **Kommunikation mit diesem Anbieter aktivieren**.

6. Klicken Sie auf **Commit ausführen**.

Um den Zugriff durch öffentliche Benutzer zu ermöglichen, müssen Sie auch die Unterstützung für den Partnerverbund in Ihrer Organisation aktivieren. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Partnerverbunds für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation.

Die Unterstützung für Sofortnachrichten-Dienstanbieter erfordert außerdem die Konfiguration von Richtlinien zur Unterstützung des Benutzerzugriffs. Ausführliche Informationen zur Konfiguration von Richtlinien zur Unterstützung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern finden Sie unter Konfigurieren von Richtlinien zur Steuerung des Zugriffs durch Benutzer von Sofortnachrichten-Dienstanbietern.

Konfigurieren von Konferenzrichtlinien zur Unterstützung anonymer Benutzer

Wenn Sie die anonyme Teilnahme an Besprechungen zulassen, können anonyme Benutzer (also Benutzer, deren Identität nur durch den Besprechungs- oder Konferenzschlüssel bestätigt wird) an Besprechungen teilnehmen. Standardmäßig werden alle Benutzer daran gehindert, anonyme Benutzer zur Teilnahme an einer Besprechung einzuladen. Sie steuern, wer anonyme Benutzer einladen kann, indem Sie eine Konferenzrichtlinie für die Unterstützung anonymer Benutzer konfigurieren und diese Konferenzrichtlinie auf bestimmte Benutzer anwenden.

Verwenden Sie das Verfahren in diesem Abschnitt, um eine globale Richtlinie für die Unterstützung anonymer Benutzer in Konferenzen zu konfigurieren. Ausführliche Informationen zur Erstellung und Anwendung einer Konferenzrichtlinie für die Unterstützung der Teilnahme anonymer Benutzer an Konferenzen finden Sie unter „Erstellen oder Ändern der Konferenzeinstellungen für einen Standort oder eine Benutzergruppe“ und Anwenden von Konferenzrichtlinien zur Unterstützung anonymer Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

- Auf globaler Ebene können Sie festlegen, ob der Zugriff anonymer Benutzer auf Konferenzen aktiviert werden soll.
- Auf Ebene der Benutzerkonten können Sie steuern, ob ein Benutzer anonyme Benutzer einladen kann, indem Sie festlegen, welche Konferenzrichtlinien auf die einzelnen Benutzer angewendet werden.

So konfigurieren Sie Richtlinien zum Zulassen der anonymen Teilnahme an Besprechungen

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.
2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.
3. Klicken Sie in der linken Navigationsleiste auf **Zugriff durch externe Benutzer**.
4. Klicken Sie auf der Seite **Zugriffs-Edgekonfiguration** auf die globale Richtlinie, klicken Sie auf **Bearbeiten** und dann auf **Details anzeigen**.
5. Aktivieren Sie unter **Zugriffs-Edgekonfiguration bearbeiten** das Kontrollkästchen **Anonyme Benutzer dürfen auf Konferenzen zugreifen**.
6. Klicken Sie auf **Commit ausführen**.
7. Klicken Sie in der linken Navigationsleiste auf **Konferenzen**, und führen Sie einen der

folgenden Schritte aus:

a. Klicken Sie zum Erstellen einer neuen Standortrichtlinie auf **Neu** und anschließend auf **Standortrichtlinie**. Klicken Sie im Dialogfeld **Standort auswählen** in der Liste auf den entsprechenden Standort, und klicken Sie dann auf **OK**.

b. Klicken Sie zum Konfigurieren einer vorhandenen Richtlinie in der Tabelle auf die entsprechende Richtlinie, klicken Sie auf **Bearbeiten** und anschließend auf **Details anzeigen**.

8. Aktivieren Sie im Dialogfeld **Konferenzrichtlinien** das Kontrollkästchen **Teilnehmer dürfen anonyme Benutzer einladen**.

9. Klicken Sie auf **Commit ausführen**.

Damit Benutzer anonyme Benutzer zu Konferenzen einladen können, müssen Sie auch die Unterstützung für anonyme Benutzer in Ihrer Organisation aktivieren. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Zugriffs anonymer Benutzer für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation.

Zusätzlich müssen Sie die Richtlinie auf Benutzer anwenden, die anonyme Benutzer einladen sollen. Ausführliche Informationen finden Sie unter Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer in der Bereitstellungs- oder Betriebsdokumentation.

Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer

Wenn Sie zur Unterstützung anonymer Benutzer Benutzerrichtlinien für den externen Benutzerzugriff oder Konferenzrichtlinien konfigurieren, müssen Sie die Richtlinien den Benutzern oder Benutzergruppen zuweisen, damit diese Unterstützung den Benutzern zur Verfügung steht.

Inhalt dieses Abschnitts

- Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer
- Anwenden von Konferenzrichtlinien zur Unterstützung anonymer Benutzer

Anwenden von Richtlinien für den externen Benutzerzugriff auf Benutzer

Wurde ein Benutzer für Lync Server 2010 aktiviert, können Sie den Partnerverbund, den Zugriff durch Remotebenutzer und Verbindungen mit öffentlichen Instant Messaging-Diensten in der Lync Server-Systemsteuerung konfigurieren, indem Sie bestimmten Benutzern oder Benutzergruppen die entsprechenden Richtlinien zuweisen. Wenn Sie beispielsweise eine Richtlinie für die Unterstützung des Remotebenutzerzugriffs erstellt haben, müssen Sie diese auf

mindestens einen Benutzer oder eine Benutzergruppe anwenden, damit der Benutzer oder die Benutzergruppe von einem Remotestandort aus eine Verbindung mit Lync Server 2010 herstellen und mit internen Benutzern zusammenarbeiten kann.

Hinweis:
Um den Zugriff durch externe Benutzer zu unterstützen, müssen Sie die Unterstützung für jeden Typ des externen Benutzerzugriffs aktivieren, der unterstützt werden soll, sowie die entsprechenden Richtlinien und andere Optionen zur Verwendungssteuerung konfigurieren. Ausführliche Informationen hierzu finden Sie unter Konfigurieren der Unterstützung für den externen Benutzerzugriff in der Bereitstellungsdokumentation oder unter „Verwalten externer Verbindungen“ in der Betriebsdokumentation.

Verwenden Sie das Verfahren in diesem Thema, um eine zuvor erstellte Richtlinie für den externen Benutzerzugriff auf ein oder mehrere Benutzerkonten oder Benutzergruppen anzuwenden.

So wenden Sie eine Richtlinie für den externen Benutzerzugriff auf ein Benutzerkonto an

1. Melden Sie sich mit einem Benutzerkonto, dem die Rolle „CsUserAdministrator“ oder „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Benutzer**, und suchen Sie anschließend nach dem Benutzerkonto, das Sie konfigurieren möchten.

4. Klicken Sie in der Tabelle mit den Suchergebnissen auf das Benutzerkonto, klicken Sie auf **Bearbeiten** und dann auf **Details anzeigen**.

5. Wählen Sie in **Lync Server-Benutzer bearbeiten** unter **Externe Zugriffsrichtlinie** die Benutzerrichtlinie aus, die Sie anwenden möchten.

   Hinweis:
   Mit den Einstellungen **<Automatisch>** werden die Standardeinstellungen der Serverinstallation angewendet. Diese Einstellungen werden vom Server automatisch übernommen.

Anwenden von Konferenzrichtlinien zur Unterstützung anonymer Benutzer

Standardmäßig werden alle Benutzer daran gehindert, anonyme Benutzer zur Teilnahme an einer Besprechung einzuladen. Sie steuern, wer anonyme Benutzer einladen kann, indem Sie eine Konferenzrichtlinie für die Unterstützung anonymer Benutzer konfigurieren und diese Konferenzrichtlinie auf bestimmte Benutzer anwenden. Ausführliche Informationen zur Konfiguration von Konferenzrichtlinien für die Unterstützung anonymer Benutzer finden Sie unter Konfigurieren von Konferenzrichtlinien zur Unterstützung anonymer Benutzer in der Bereitstellungsdokumentation oder unter „Verwalten externer Verbindungen“ in der Betriebsdokumentation.

Verwenden Sie das Verfahren in diesem Abschnitt, um eine bereits erstellte Konferenzrichtlinie auf einen oder mehrere Benutzer oder Benutzergruppen anzuwenden.

Hinweis:
Neben der Konfiguration und Anwendung einer Richtlinie müssen Sie außerdem die Unterstützung für anonyme Benutzer für Ihre Organisation aktivieren, um Benutzern das Einladen anonymer Benutzer zu ermöglichen. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Zugriffs anonymer Benutzer für Ihre Organisation.

So konfigurieren Sie eine Benutzerrichtlinie für die anonyme Teilnahme an Besprechungen

1. Melden Sie sich mit einem Benutzerkonto, das Mitglied der Gruppe „RTCUniversalServerAdmins“ ist (oder über gleichwertige Benutzerrechte verfügt) oder dem die Rolle „CsAdministrator“ zugewiesen ist, an einem beliebigen Computer in Ihrer internen Bereitstellung an.

2. Öffnen Sie ein Browserfenster, und geben Sie die Admin-URL ein, um die Lync Server-Systemsteuerung zu öffnen. Informationen zu den verschiedenen Methoden zum Starten der Lync Server-Systemsteuerung finden Sie unter „Open Lync Server Administrative Tools“.

3. Klicken Sie in der linken Navigationsleiste auf **Konferenzen**, und führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie zum Erstellen einer neuen Benutzerrichtlinie auf **Neu** und anschließend auf **Benutzerrichtlinie**. Erstellen Sie einen eindeutigen Namen im Feld **Name**, der auf den Zweck der Benutzerrichtlinie hinweist (z. B. **EnableAnonymous** für eine Benutzerrichtlinie, welche die Kommunikation mit anonymen Benutzern aktiviert).

   b. Klicken Sie zum Konfigurieren einer vorhandenen Benutzerrichtlinie in der Tabelle auf die entsprechende Richtlinie, klicken Sie auf **Bearbeiten** und anschließend auf **Details anzeigen**.

4. Aktivieren Sie im Dialogfeld **Konferenzrichtlinien** das Kontrollkästchen **Teilnehmer dürfen anonyme Benutzer einladen**.

5. Klicken Sie auf **Commit ausführen**.

6. Klicken Sie in der linken Navigationsleiste auf **Benutzer**, und suchen Sie anschließend nach dem Benutzerkonto, das Sie konfigurieren möchten.

7. Klicken Sie in der Tabelle mit den Suchergebnissen auf das Benutzerkonto, klicken Sie auf **Bearbeiten** und dann auf **Details anzeigen**.

8. Wählen Sie in **Lync Server-Benutzer bearbeiten** unter **Konferenzrichtlinie** die Benutzerrichtlinie mit der Konfiguration für den anonymen Benutzerzugriff aus, die Sie auf diesen Benutzer anwenden möchten.

   Hinweis:
   Mit den Einstellungen **<Automatisch>** werden die Standardeinstellungen der Serverinstallation angewendet und automatisch vom Server zugewiesen.

Damit Benutzer anonyme Benutzer zu Konferenzen einladen können, müssen Sie auch die Unterstützung für anonyme Benutzer in Ihrer Organisation aktivieren. Ausführliche Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren des Zugriffs anonymer Benutzer für Ihre Organisation in der Bereitstellungs- oder Betriebsdokumentation.

Überprüfen der Edgebereitstellung

Nachdem Sie die Installation und Konfiguration ihrer Edgekomponenten abgeschlossen haben, müssen Sie die Konfiguration und Konnektivität der Server überprüfen und die Konnektivität für alle unterstützten externen Benutzertypen überprüfen.

Inhalt dieses Abschnitts

- Überprüfen der Konnektivität zwischen internen Servern und Edgeservern
- Überprüfen der Konnektivität für externe Benutzer

Überprüfen der Konnektivität zwischen internen Servern und Edgeservern

In Microsoft Office Communications Server 2007 R2 stand ein separater Überprüfungs-Assistent zum Prüfen der Konnektivität zwischen Edgeservern und internen Servern zur Verfügung.
In Microsoft Lync Server 2010 wird die Konnektivität automatisch überprüft, wenn Sie Ihre Edgeserver installieren.

Sie können die Replikation von Konfigurationsinformationen auf den Edgeserver überprüfen, indem Sie das Windows PowerShell-Cmdlet **Get-CsManagementStoreReplicationStatus** auf dem internen Computer ausführen, auf dem Sie den zentralen Verwaltungsspeicher bereitgestellt haben (oder auf einem beliebigen Computer in der Domäne, auf dem die Lync Server 2010-Hauptkomponenten (OcsCore.msi) installiert sind). Anfänglich wird anstelle des Status „True“ möglicherweise der Status „False“ für die Replikation angezeigt. Führen Sie in diesem Fall das **Invoke-CsManagementStoreReplication**-Cmdlet aus, und warten Sie den Abschluss der Replikation ab. Führen Sie anschließend erneut das **Get-CsManagementStoreReplicationStatus**-Cmdlet aus.

Sie können die Konnektivität für externe Benutzer separat überprüfen, einschließlich Verwendung der Remoteverbindungsanalyse von Office Communications Server zum Überprüfen der Remotebenutzerkonnektivität. Ausführliche Informationen finden Sie unter Überprüfen der Konnektivität für externe Benutzer.

Überprüfen der Konnektivität für externe Benutzer

Zum Überprüfen der Konnektivität für externe Benutzer müssen Sie sicherstellen, dass die Benutzer eine Verbindung mit dem Server und mit dem Port für den Zugriffs-Edgedienst herstellen können.

Testen der Konnektivität externer Benutzer und des externen Zugriffs

Tests für den Zugriff durch externe Benutzer sollten sämtliche Typen von externen Benutzern umfassen, die von Ihrer Organisation unterstützt werden. Dazu können die folgenden Typen zählen:

- Benutzer aus mindestens einer Partnerdomäne sowie Testen von Sofortnachrichten-, Anwesenheits-, A/V-Funktionen und Desktopfreigabe.
- Benutzer öffentlicher Sofortnachrichten-Dienstanbieter, die von Ihrer Organisation unterstützt werden
  (und für welche die Bereitstellung abgeschlossen wurde).
- Anonyme Benutzer.
- Benutzer innerhalb Ihrer Organisation, die sich remote bei Lync anmelden, jedoch kein VPN verwenden.

Mithilfe dieser Tests wird ermittelt, ob Ihr Edgeserver folgende Aufgaben ausführt:

- Überwachen der erforderlichen Ports durch Verwendung eines Telnet-Clients außerhalb Ihres Netzwerks.
  - Beispiel: telnet ae.contoso.com 443

    - Ausführen des vorstehenden Tests für Ports, die Sie abhängig von Ihrer Bereitstellung auf dem Edgeserver oder Edgeserverpool verwenden.

- Ausführen einer präzisen externen DNS-Auflösung.

    - Senden Sie von außerhalb Ihres Netzwerks ein Pingsignal an jeden externen FQDN Ihres Edgeservers oder Edgeserverpools. Selbst wenn das Pingen nicht erfolgreich ist, werden die IP-Adressen angezeigt, die Sie mit den von Ihnen zugewiesenen Adressen vergleichen können.