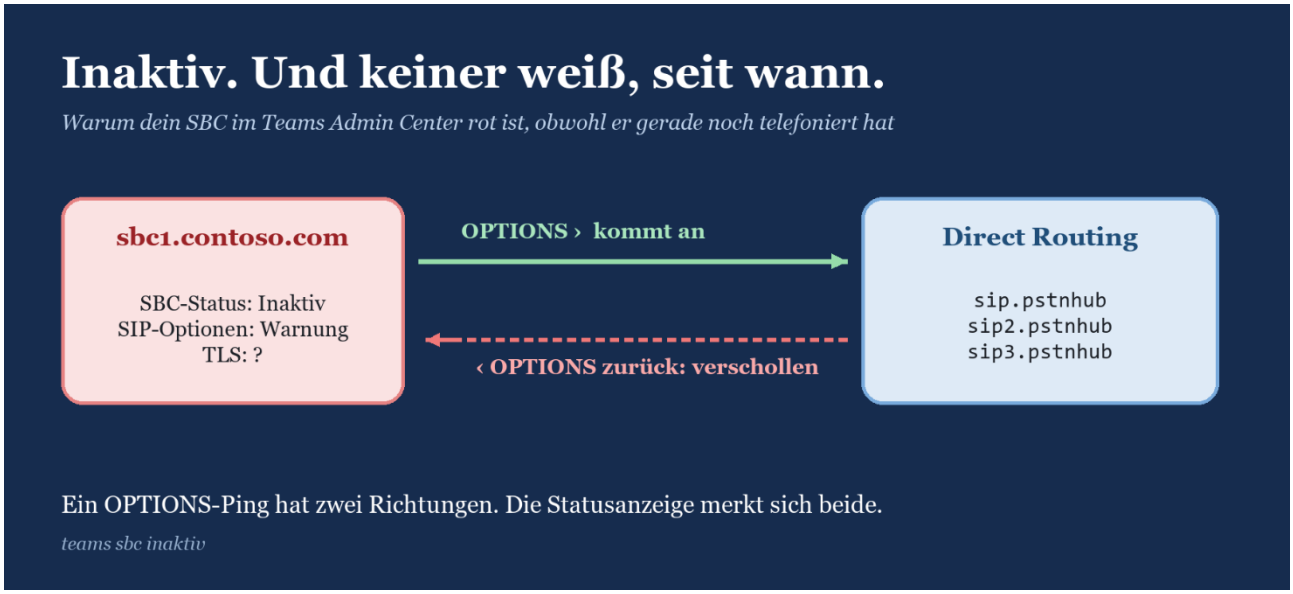
Teams SBC inaktiv: OPTIONS-Ping und Verbindungsstatus prüfen



WISSEN

Alles zur Teams-Telefonie: Direct Routing, SBC, Wählpläne, Routing, Notruf und Betrieb an einem Ort.

› **Teams-Telefonie**

BERATUNG

Dein SBC flackert zwischen Aktiv und Inaktiv, und keiner weiß warum? Wir sehen uns Log, Zertifikat und Firewall gemeinsam mit dir an.

› **Beratung zur Teams-Telefonie**

SCHULUNG

Für Admins, die SIP-Logs, TLS-Handshakes und den Integritätsstatus von Direct Routing selbst lesen wollen.

› **Schulung Teams-Telefonie**

Das Teams Admin Center hat eine sehr eigene Art, schlechte Nachrichten zu überbringen. Kein Pop-up, keine Mail, kein Trommelwirbel. Nur ein kleines Wort in der Zeile deines SBC: Inaktiv. Daneben vielleicht eine gelbe Warnung bei den SIP-Optionen. Und dann die große Frage, die jeder Admin kennt: Ist das jetzt ein Schönheitsfehler, oder telefoniert gerade niemand mehr?

Beides ist möglich, und genau das macht diese Anzeige so tückisch. Microsoft schreibt selbst, dass der Integritätsstatus im Teams Admin Center ausschließlich auf dem Austausch von SIP-OPTIONS zwischen SBC und den SIP-Proxys von Direct Routing beruht und nicht auf dem echten Anrufverkehr. Ein SBC kann also Inaktiv anzeigen und trotzdem Gespräche vermitteln. Er kann aber auch grün aussehen und bei der nächsten Zertifikatsprüfung kippen.

In diesem Beitrag gehst du die Kette einmal sauber durch: OPTIONS-Ping in beide Richtungen, FQDN im Zertifikat, Contact-Header, Firewall-Ports und TLS-Version. Du bekommst eine Tabelle, die jede Statusanzeige mit ihrer Bedeutung und der passenden Prüfung verbindet, lesende PowerShell-Befehle für die Diagnose und konkrete Schritte zur Behebung mit Rollback. Was ein SBC grundsätzlich tut und warum Teams ihn braucht, steht in Teams SBC Grundlagen: der Session Border Controller. Den Gesamtüberblick über das Thema findest du auf der Seite Teams-Telefonie.

FAKTEN · Das Beispiel in diesem Beitrag

Erfundener Tenant Contoso (contoso.com) mit Standorten in Frankfurt, Köln, Berlin, Hamburg und München. Zwei Session Border Controller sbc1.contoso.com und sbc2.contoso.com, beide mit Signalisierungsport 5061 im Teams Admin Center eingetragen. Rufnummern im Muster +49 69 555

0100. Wo eine öffentliche IP-Adresse gebraucht wird, steht eine Dokumentationsadresse aus 203.0.113.0/24.

Verhalten, Ports, Adressbereiche und Statuswerte stammen aus der Microsoft-Dokumentation auf Microsoft Learn, Stand November 2026.

Das Symptom: Inaktiv, Warnung oder beides

Was Anwender sagen

Ein inaktiver SBC fällt Anwendern oft gar nicht sofort auf, und wenn doch, dann in unterschiedlichen Verkleidungen:

- **„Seit heute Morgen kommt bei uns niemand mehr durch."** Eingehende Anrufe enden beim Anrufer in einer Ansage oder im Nichts. Typisch, wenn Microsoft den SBC nicht mehr erreicht.
- **„Rausrufen geht, aber wir sind nicht erreichbar."** Die ausgehende TLS-Verbindung des SBC steht, der Rückweg von Microsoft zum SBC nicht. Das ist das klassische Halbseitenbild.
- **„Manchmal geht es, manchmal nicht, und dann wieder doch."** Der Status springt zwischen Aktiv und Inaktiv, oft weil der SBC feste IP-Adressen statt der Microsoft-FQDNs anspricht.
- **„Mir ist nichts aufgefallen."** Gleichzeitig sagt das Teams Admin Center Inaktiv. Auch das kommt vor und ist kein Grund zur Entwarnung, sondern zur Neugier.

Was Admins sehen

Im Teams Admin Center unter Sprache › Direct Routing liegt das Integritätsdashboard. Oben steht die Zusammenfassung mit der Anzahl der SBCs, der Voice Routes und der SBCs mit Problemen. Als Probleme zählt Microsoft niedrige Netzwerkeffektivität, ablaufende Zertifikate, Inaktivität, fehlende SIP-Optionen und Kapazitätsengpässe. Auf dem Reiter SBCs siehst du je SBC den Status der TLS-Konnektivität und der SIP-Optionen. Öffnest du einen SBC, kommen der Gesamtstatus (Aktiv oder Inaktiv), der Zeitpunkt der letzten TLS-Verbindung und der Zeitpunkt der letzten empfangenen SIP-Optionen hinzu. Je nach Spracheinstellung deines Browsers stehen dort deutsche oder englische Begriffe, also Inaktiv oder Inactive.

Und dann gibt es noch einen Zustand, der gern verwechselt wird: das Gateway, das jemand deaktiviert hat. Das ist kein Gesundheitsstatus, sondern ein Schalter in der Konfiguration (Enabled). Ein deaktiviertes Gateway bekommt keine neuen ausgehenden Anrufe, egal wie fleißig es OPTIONS schickt. Ein inaktives Gateway dagegen ist eingeschaltet, aber Microsoft hört nichts von ihm.

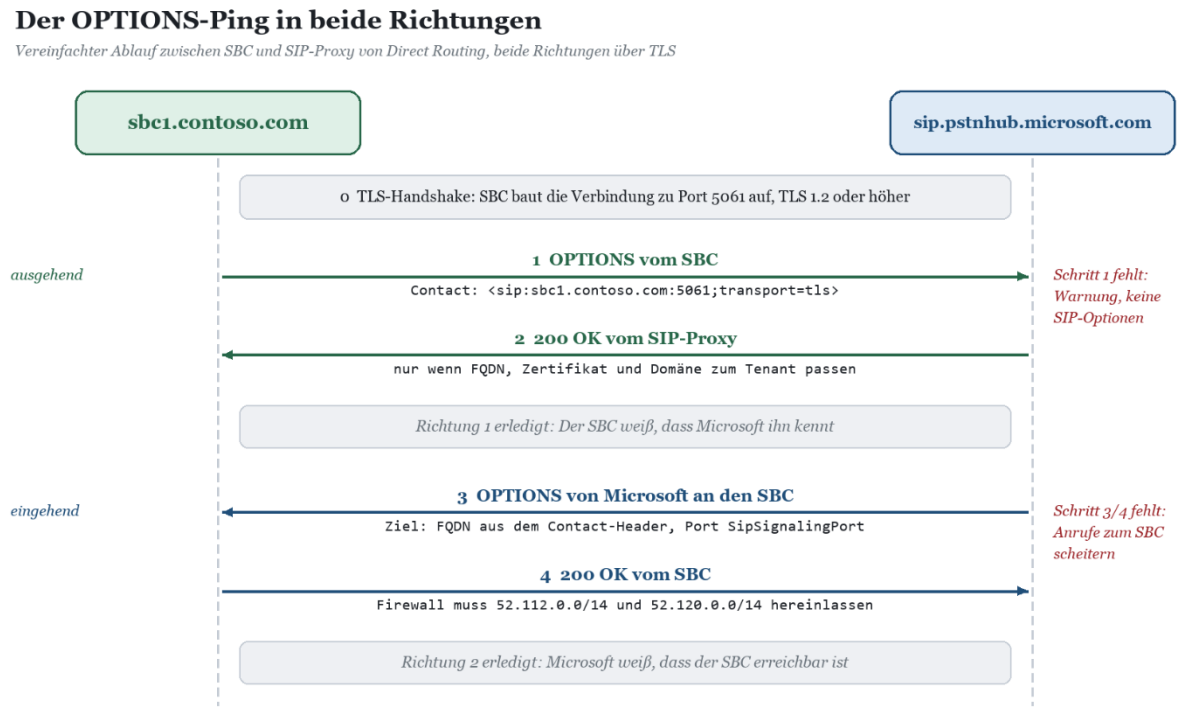
WICHTIG · Status ist nicht gleich Anrufverkehr

Microsoft beschreibt den Fall ausdrücklich: Anrufe funktionieren, aber der SBC wird als Inaktiv oder mit SIP-OPTIONS-Warnung angezeigt. Grund: Die Anzeige beruht allein auf dem OPTIONS-Austausch. Umgekehrt nutzt Direct Routing genau diese OPTIONS-Informationen bei der Auswahl des SBC für einen Anruf. Ein inaktiver SBC ist also auch dann ein Problem, wenn er gerade noch telefoniert, spätestens beim Failover.

Wie der Fehler technisch zustande kommt

Der OPTIONS-Ping in beide Richtungen

Bei einem ausgehenden Anruf läuft die Kette Benutzer › Wählplan › Normalisierung › Voice Routing Policy › PSTN Usage › Voice Route › SBC. Der Status im Admin Center betrifft nur das letzte Glied, aber genau dort entscheidet sich, ob alles davor überhaupt ankommt. Und dieses letzte Glied wird über einen unscheinbaren Mechanismus überwacht: SIP OPTIONS, eine Art Ping auf SIP-Ebene.



Skizze 1: Microsoft wertet für die Gesundheit die OPTIONS des SBC aus. Ein SBC ohne OPTIONS in den letzten drei Minuten wird herabgestuft

Der Ablauf hat zwei Richtungen. Zuerst baut der SBC eine TLS-Verbindung zum SIP-Proxy von Microsoft auf, Zielport 5061, und schickt ein OPTIONS. Microsoft prüft dabei, ob der FQDN, den der SBC im Contact-Header (oder im Record-Route-Header) mitliefert, zu einem Gateway in einem Tenant passt, und antwortet mit 200 OK. In der Gegenrichtung schickt der SIP-Proxy seinerseits OPTIONS an den SBC, adressiert an genau diesen FQDN und an den Port, den du im Gateway als Signalisierungsport hinterlegt hast. Der SBC antwortet ebenfalls mit 200 OK.

Für die Gesundheitsbewertung ist laut Microsoft entscheidend, dass der SBC regelmäßig sendet. Standard bei den meisten SBCs ist ein OPTIONS pro Minute. Direct Routing nimmt dieses Intervall dreimal: Hat der SBC in den letzten drei Minuten vor einem Anruf OPTIONS geschickt, gilt er als gesund. Wenn nicht, wird er in der Route herabgestuft. Er wird dann nicht als Erster versucht, aber noch einmal, bevor ein Anruf endgültig scheitert.

FAKTEN · Die Zahlen aus der Microsoft-Dokumentation

Signalisierung: SIP über TLS. Vom SBC zum SIP-Proxy Zielport 5061, vom SIP-Proxy zum SBC der am SBC konfigurierte Port.

SIP-Proxys: sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com. Sie lösen in die Bereiche 52.112.0.0/14 und 52.120.0.0/14 auf.

Medien ohne Media Bypass: UDP 3478 bis 3481 und 49152 bis 53247 in beide Richtungen.

Gesundheit: OPTIONS in den letzten drei Minuten, sonst Herabstufung. Zertifikatswarnung 30 Tage

vor Ablauf. TLS-Version am SBC: 1.2 oder höher.

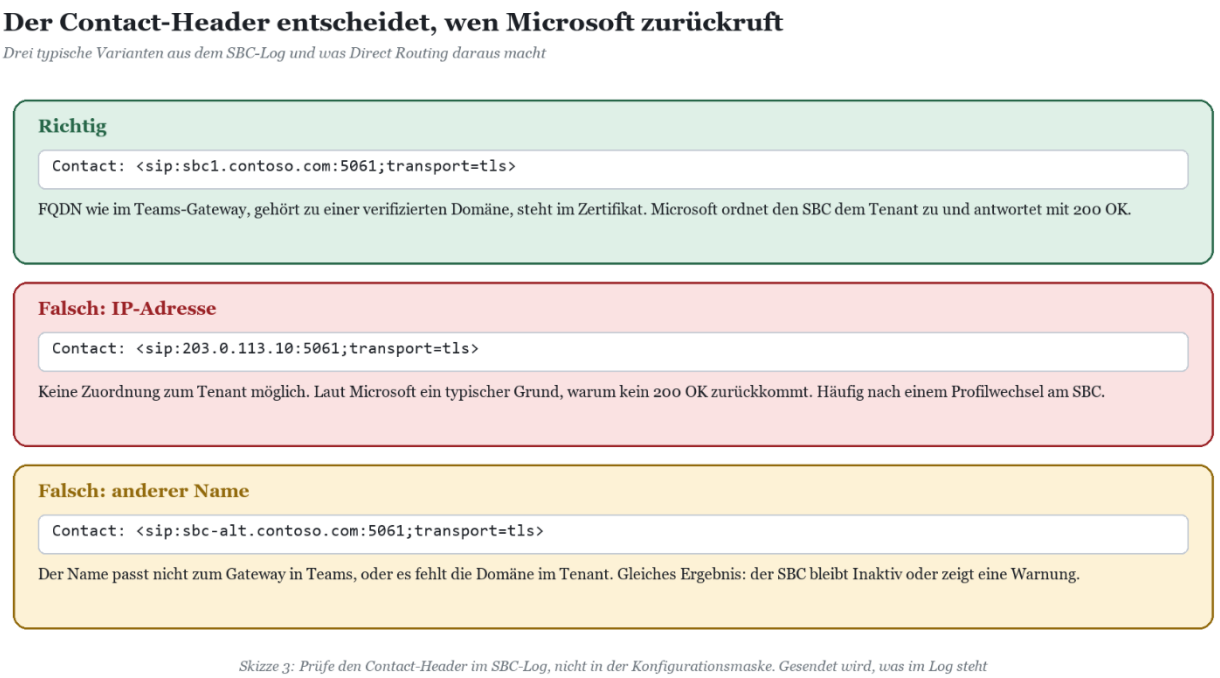
Die fünf Stellen, an denen der Ping verloren geht

Aus dem Ablauf ergeben sich die typischen Ursachen. Sie sind nicht exotisch, sie sind langweilig. Und gerade deshalb übersieht man sie, weil man nach etwas Spannenderem sucht.

1. TLS kommt nicht zustande. Der SBC spricht nur TLS 1.0 oder 1.1, die ausgehende Firewall lässt Port 5061 nicht durch, oder der SBC vertraut dem Zertifikat des SIP-Proxys nicht, weil die passenden Stammzertifikate fehlen. Microsoft nennt TLS 1.2 oder höher als Voraussetzung. Wie du die Root-CAs am SBC auf Stand bringst, steht in SIP 504 nach dem Zertifikatswechsel: Root-CAs am SBC aktualisieren.

2. Microsoft akzeptiert das Zertifikat des SBC nicht. Das Zertifikat ist selbstsigniert, abgelaufen oder widerrufen, stammt nicht von einer CA aus dem Microsoft Trusted Root Program, ihm fehlt der Verwendungszweck Serverauthentifizierung, oder der FQDN steht weder im Common Name noch im Subject Alternative Name. Platzhalterzertifikate sind erlaubt, decken aber nur eine Ebene ab: *.contoso.com passt auf sbc1.contoso.com, nicht auf sbc1.ffm.contoso.com. Eine weitere Falle ist eine unvollständige Kette, bei der das Zwischenzertifikat im TLS-Handshake fehlt.

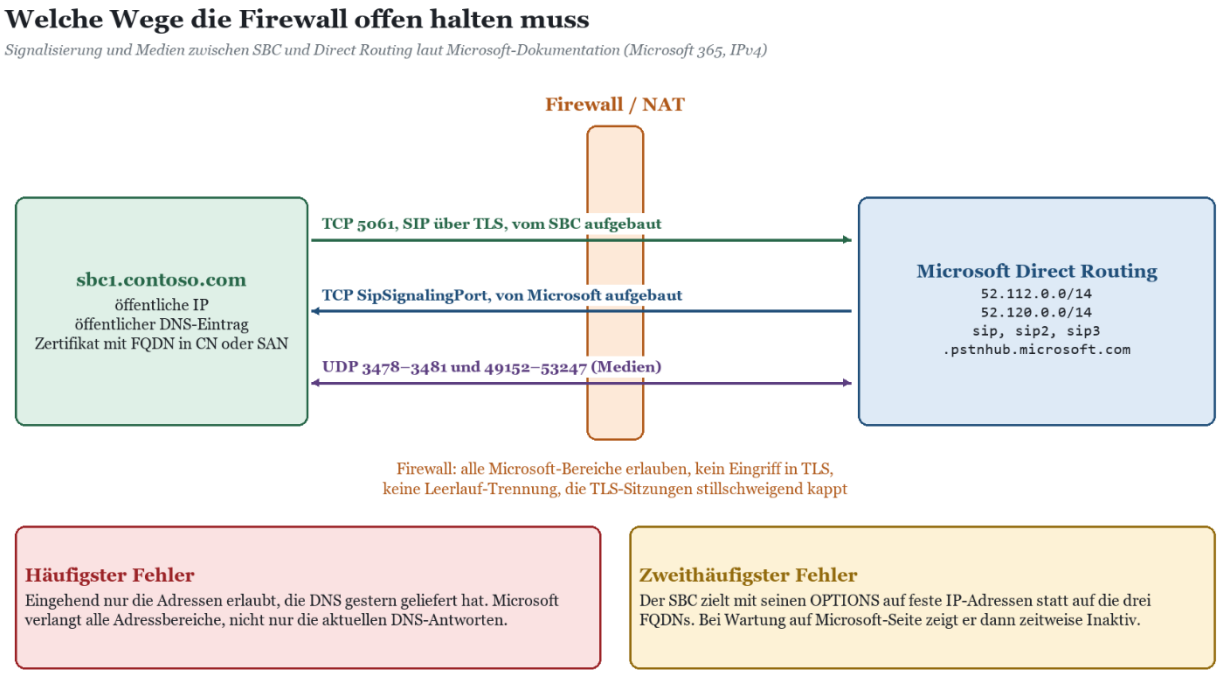
3. Der FQDN passt nicht zum Tenant. Der Contact-Header enthält eine IP-Adresse statt des FQDN, einen anderen Namen als das Gateway in Teams, oder die Domäne ist im Tenant nicht vollständig verifiziert. Microsoft weist außerdem darauf hin, dass eine neue Domäne für einen SBC erst aktiv wird, wenn mindestens ein lizenzierter Benutzer mit dieser Domäne existiert, und dass das bis zu 24 Stunden dauern kann.



Skizze 3: Prüfe den Contact-Header im SBC-Log, nicht in der Konfigurationsmaske. Gesendet wird, was im Log steht

4. Der Rückweg ist zu. Microsofts OPTIONS erreichen den SBC nicht, weil die Firewall eingehend nur einzelne Adressen erlaubt, der öffentliche DNS-Eintrag des SBC fehlt oder auf eine alte Adresse zeigt, oder der Port im Gateway nicht zu dem Port passt, auf dem der SBC lauscht. Microsoft empfiehlt ausdrücklich, alle Adressbereiche zu erlauben, nicht nur die, die DNS gerade liefert.

5. Es geht, aber nicht dauerhaft. Der SBC sendet seine OPTIONS an feste IP-Adressen statt an die drei FQDNs. Zieht Microsoft wegen Wartung um, zielt der SBC ins Leere, und der Status flackert. Ähnlich wirken Firewalls oder Load Balancer, die lange TLS-Sitzungen stillschweigend beenden, und Rate-Limits am SBC, die OPTIONS als lästigen Verkehr drosseln.



Skizze 4: Medienports nur ohne Media Bypass. Mit Media Bypass sprechen Clients direkt mit dem SBC, dafür gelten eigene Bereiche

WARNUNG · SendSipOptions ausschalten ist keine Lösung

Wer die Warnung loswerden will, kommt schnell auf die Idee, im Gateway SendSipOptions auf $false zu setzen. Dann zeigt das Dashboard „Warnung, SIP-Nachrichten sind nicht konfiguriert“, und das Monitoring für diesen SBC ist laut Microsoft weg. Microsoft empfiehlt ausdrücklich, OPTIONS eingeschaltet zu lassen, weil sonst ein SBC mit abgelaufenem Zertifikat oder hängendem SIP-Stack auf Netzebene erreichbar wirkt und erst beim Anruf auffällt.

Statusanzeige, Bedeutung, Prüfung

Die folgende Tabelle ist die Übersetzung des Dashboards in Arbeitsschritte. Die Bedeutungen folgen der Microsoft-Dokumentation zum Integritätsdashboard, die Prüfungen sind die Stellen, an denen du mit der Suche anfängst.

Statusanzeige	Bedeutung	Prüfung
SBC-Status: Aktiv	Der SBC ist gesund und nimmt Verkehr an.	Nichts zu tun. Gelegentlich den Zeitpunkt der letzten SIP-Optionen ansehen.
SBC-Status: Inaktiv	Keine aktuellen Anrufe oder Integritätsprüfungen vom SBC.	Diagnosepfad komplett: TLS, Zertifikat, Contact-Header, Firewall, OPTIONS-Ziel.
SIP-Optionen: Aktiv	Microsoft sieht OPTIONS in regelmäßigem Abstand.	Bei Anrufproblemen trotzdem: Rückweg und Medienports prüfen.
Warnung, keine SIP-Optionen	Gateway angelegt und auf OPTIONS eingestellt, aber Microsoft hat nie OPTIONS von diesem SBC gesehen.	Ausgehend: Firewall 5061, TLS-Version, Zertifikat, FQDN im Contact-Header, Domäne aktiviert.
Warnung, SIP-Nachrichten nicht	Überwachung per OPTIONS ist nicht eingeschaltet.	SendSipOptions im Gateway und OPTIONS-Versand am SBC prüfen.

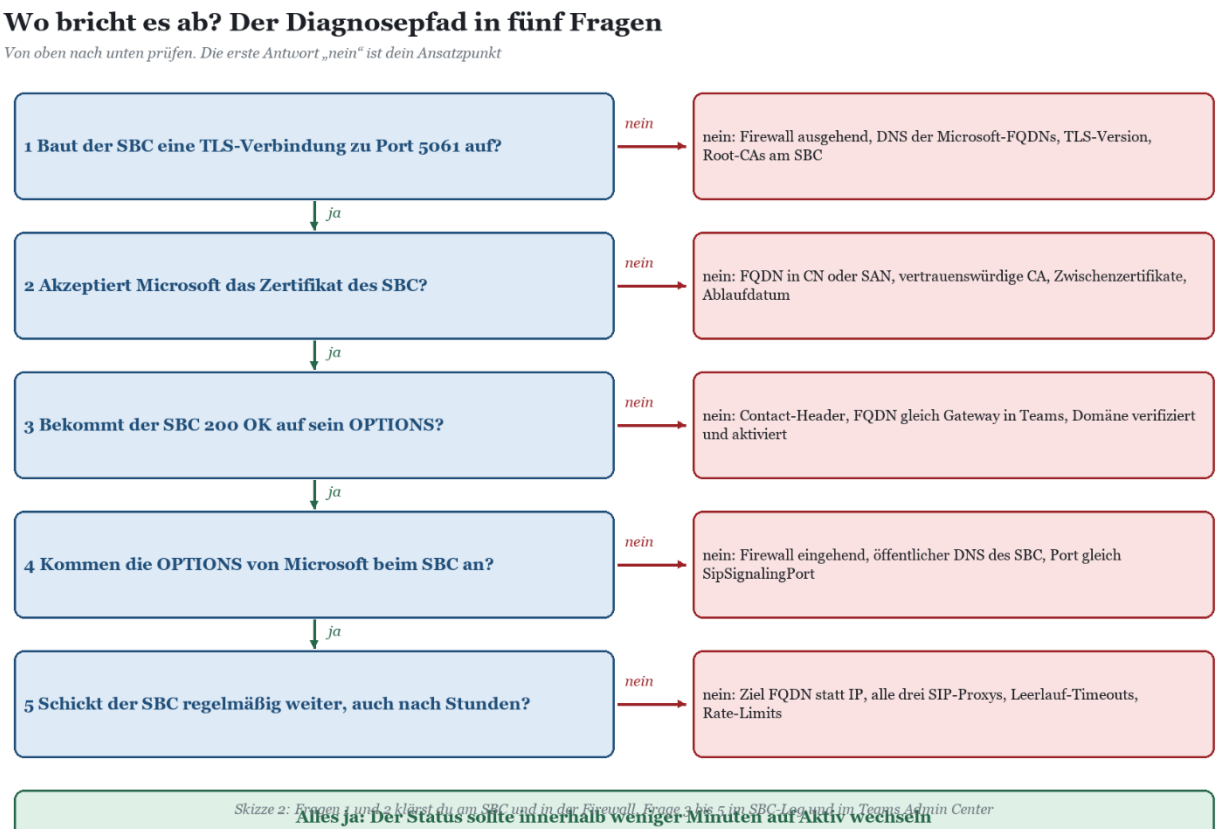
konfiguriert		
TLS-Konnektivität: Warnung zum Zertifikat	Das Zertifikat läuft innerhalb von 30 Tagen ab, ist abgelaufen oder ungültig.	Ablaufdatum, CA, Kette und SAN prüfen, neues Zertifikat einspielen, alte TLS-Sitzungen beenden.
SBC mit Problemen, nie verbunden	Per PowerShell angelegt, aber nie verbunden: Das Dashboard zeigt ihn als nicht gesund.	FQDN, Domäne, DNS und ob der SBC überhaupt schon auf Microsoft zeigt.
Niedrige Netzwerkeffektivität	Anteil zugestellter Anrufe zu niedrig, etwa durch 504 vom SBC.	SIP-Codes je SBC ansehen. Unter 100 Anrufen kann ein niedriger Wert normal sein.
Kapazität gleichzeitiger Anrufe	Auslastung gemessen gegen MaxConcurrentSessions.	Grenzwert gleich tatsächlicher Trunk-Kapazität? Kein Gesundheits-, sondern ein Planungsthema.
Gateway deaktiviert (Enabled = False)	Kein Status, sondern Konfiguration: keine neuen ausgehenden Anrufe über diesen SBC.	Get-CsOnlinePSTNGateway, Eigenschaft Enabled. Oft nach Wartung vergessen.

AUS DER PRAXIS · Ein Logistiker mit fünf Lagerstandorten

Zwei SBCs, beide seit Monaten zuverlässig. Nach einem Firewall-Tausch zeigte sbc2 dauerhaft Inaktiv, telefoniert wurde aber weiter über sbc1. Niemand störte sich daran, bis sbc1 bei einem Stromausfall im Rechenzentrum ausfiel und sbc2 übernehmen sollte. Er übernahm nicht. Ursache: Die neue Firewall ließ eingehend nur die drei Adressen zu, die bei der Migration per DNS aufgelöst worden waren. Die Regel auf die vollständigen Bereiche 52.112.0.0/14 und 52.120.0.0/14 umzustellen, dauerte fünf Minuten. Das Ignorieren der Warnung hatte vorher vier Monate gedauert.

Diagnose Schritt für Schritt

Die Diagnose folgt dem Weg des OPTIONS-Pings. Die Befehle für den Tenant stammen aus dem PowerShell-Modul MicrosoftTeams und lesen nur. Für die Netzprüfungen brauchst du einen Rechner im selben Netzsegment wie der SBC, etwa in der DMZ, denn vom Arbeitsplatz aus prüfst du die falsche Firewall.



Skizze 2: Fragen 1 und 2 klärst du am SBC und in der Firewall, Frage 3 bis 5 im SBC-Log und im Teams Admin Center

Schritt 1: Das Integritätsdashboard lesen

Im Teams Admin Center öffnest du Sprache › Direct Routing und dort den betroffenen SBC. Notiere drei Werte: den Status der SIP-Optionen samt Warntext, den Zeitpunkt „SIP-Optionen zuletzt überprüft“ und den Zeitpunkt der letzten TLS-Verbindung. Ein Klick auf die Warnung zeigt eine detaillierte Beschreibung mit Empfehlung. Lies sie, bevor du rätst.

Die beiden Zeitstempel verraten viel. Liegt die letzte TLS-Verbindung aktuell, die letzten OPTIONS aber Stunden zurück, steht die Leitung, und das Problem sitzt in der SIP-Schicht: Contact-Header, FQDN, Domäne. Liegen beide weit zurück, kommt der SBC gar nicht erst durch: Firewall, DNS, TLS, Zertifikat. Fällt der Zeitpunkt mit einem Zertifikatswechsel, Firewall-Tausch oder Firmware-Update zusammen, hast du den Täter meist schon.

Schritt 2: Das Gateway in Teams prüfen

```
Get-CsOnlinePSTNGateway |
  Select-Object Identity, Fqdn, SipSignalingPort, Enabled, SendSipOptions,
    MaxConcurrentSessions, FailoverTimeSeconds |
  Format-Table -AutoSize
```

Prüfe: Stimmt der FQDN buchstabengenau mit dem Namen überein, den der SBC im Contact-Header schickt und der im Zertifikat steht? Ist SipSignalingPort der Port, auf dem der SBC wirklich lauscht? Steht SendSipOptions auf True? Und ist das Gateway überhaupt Enabled? Ein Tippfehler im FQDN, etwa sbcl statt sbc1, kostet erstaunlich viele Stunden.

Danach die Domäne. Der SBC-FQDN muss zu einer verifizierten Domäne deines Tenants gehören, *.onmicrosoft.com ist nicht zulässig. Im Microsoft 365 Admin Center unter Einstellungen › Domänen siehst du, ob contoso.com oder eine eigene Unterdomäne für die SBCs als eingerichtet geführt wird. Für eine Unterdomäne, die nur für SBCs existiert, brauchst du nach Microsoft-Dokumentation mindestens einen lizenzierten Benutzer mit dieser Domäne, damit sie für Direct Routing aktiv wird.

Schritt 3: DNS und Erreichbarkeit aus Sicht des SBC

Vom Rechner in der DMZ prüfst du, ob die Microsoft-FQDNs auflösen und Port 5061 ausgehend offen ist, und ob dein eigener SBC-FQDN öffentlich auf die richtige Adresse zeigt.

```
# Ausgehend: Microsoft-SIP-Proxys auflösen und Port 5061 testen
"sip.pstnhub.microsoft.com", "sip2.pstnhub.microsoft.com", "sip3.pstnhub.microsoft.com" |
  ForEach-Object { Test-NetConnection -ComputerName $_ -Port 5061 } |
  Select-Object ComputerName, RemoteAddress, TcpTestSucceeded

# Eigener FQDN: Welche öffentliche Adresse liefert DNS?
Resolve-DnsName -Name sbc1.contoso.com -Type A
```

Resolve-DnsName fragt standardmäßig den internen DNS-Server. Bei Split-DNS bekommst du dann die interne Adresse und hältst alles für gut. Frage deshalb zusätzlich einen öffentlichen Resolver, etwa mit dem Parameter -Server, oder prüfe den Eintrag beim DNS-Anbieter. Microsoft verlangt, dass der SBC-FQDN über öffentliches DNS auf eine öffentliche Adresse auflöst.

Den eingehenden Weg kannst du aus dem eigenen Netz nicht testen, denn du bist nicht Microsoft. Hier hilft nur der Blick ins Firewall-Log: Kommen Verbindungen aus 52.112.0.0/14 und 52.120.0.0/14 auf dem Signalisierungsport des SBC an, und werden sie erlaubt oder verworfen?

Schritt 4: Zertifikat und TLS-Version prüfen

Welches Zertifikat der SBC tatsächlich ausliefert und welche TLS-Version er aushandelt, liest du mit wenigen Zeilen PowerShell aus. Das Skript baut nur eine Verbindung auf und liest das Zertifikat, es verändert nichts.

```
$fqdn = "sbc1.contoso.com"; $port = 5061
$tcp  = [System.Net.Sockets.TcpClient]::new($fqdn, $port)
$ssl  = [System.Net.Security.SslStream]::new($tcp.GetStream(), $false, { $true })
$ssl.AuthenticateAsClient($fqdn)
$cert = [System.Security.Cryptography.X509Certificates.X509Certificate2]$ssl.RemoteCertificate
[pscustomobject]@{
  Protokoll = $ssl.SslProtocol
  Subject   = $cert.Subject
  Issuer    = $cert.Issuer
  Ablauf    = $cert.NotAfter
  SAN       = ($cert.Extensions | Where-Object { $_.Oid.Value -eq "2.5.29.17" }).Format($false)
}
$ssl.Dispose(); $tcp.Dispose()
```

Der Validierungs-Callback { $true } sorgt dafür, dass du das Zertifikat auch dann siehst, wenn es ungültig ist. Das ist für die Diagnose gewollt. Achte auf drei Dinge: Steht sbc1.contoso.com im SAN oder als CN? Liegt Ablauf in der Zukunft, und zwar mit mehr als 30 Tagen Abstand? Ist Protokoll mindestens Tls12? Viele SBCs nehmen Verbindungen nur aus den Microsoft-Bereichen an; dann führst du die Prüfung direkt am SBC oder über dessen eigene Diagnosefunktion aus.

TIPP · Die Kette nicht vergessen

Ein gültiges Serverzertifikat reicht nicht, wenn der SBC das Zwischenzertifikat im TLS-Handshake nicht mitschickt. Microsoft beschreibt genau diesen Fall: Die Kette lässt sich nicht validieren, die Verbindung wird zurückgesetzt, und der Status flackert. Im SBC prüfst du, ob Server- und Zwischenzertifikat gemeinsam im TLS-Kontext hinterlegt sind.

Schritt 5: Das SBC-Log lesen

Jetzt kommt die eigentliche Wahrheit. Microsoft schreibt, dass Direct Routing eine detaillierte Beschreibung von Problemen an den SBC zurückschickt, die du im SBC-Log nachlesen kannst. Call Analytics hilft hier nicht, denn ein abgewiesenes OPTIONS ist kein Anruf. Filtere im Log auf die Methode OPTIONS und prüfe:

- **Wohin geht das OPTIONS?** Ziel sollten die FQDNs sip, sip2 und sip3.pstnhub.microsoft.com sein, nicht einzelne IP-Adressen.
- **Was steht im Contact-Header?** Der SBC-FQDN, genau wie im Gateway, mit Port und transport=tls. Keine interne oder öffentliche IP-Adresse.
- **Welche Antwort kommt zurück?** 200 OK ist gut. Eine Fehlerantwort trägt meist einen Hinweistext, der den Grund nennt. Kommt gar nichts, liegt das Problem vor SIP, also bei TLS oder Netz.
- **Kommen OPTIONS von Microsoft an?** Wenn der SBC nur eigene OPTIONS sieht und nie fremde, ist der Rückweg zu: Firewall, NAT, DNS oder falscher Port.
- **Wie regelmäßig?** Lücken von mehr als drei Minuten führen zur Herabstufung. Rate-Limits oder Sitzungs-Timeouts sind dann die Verdächtigen.

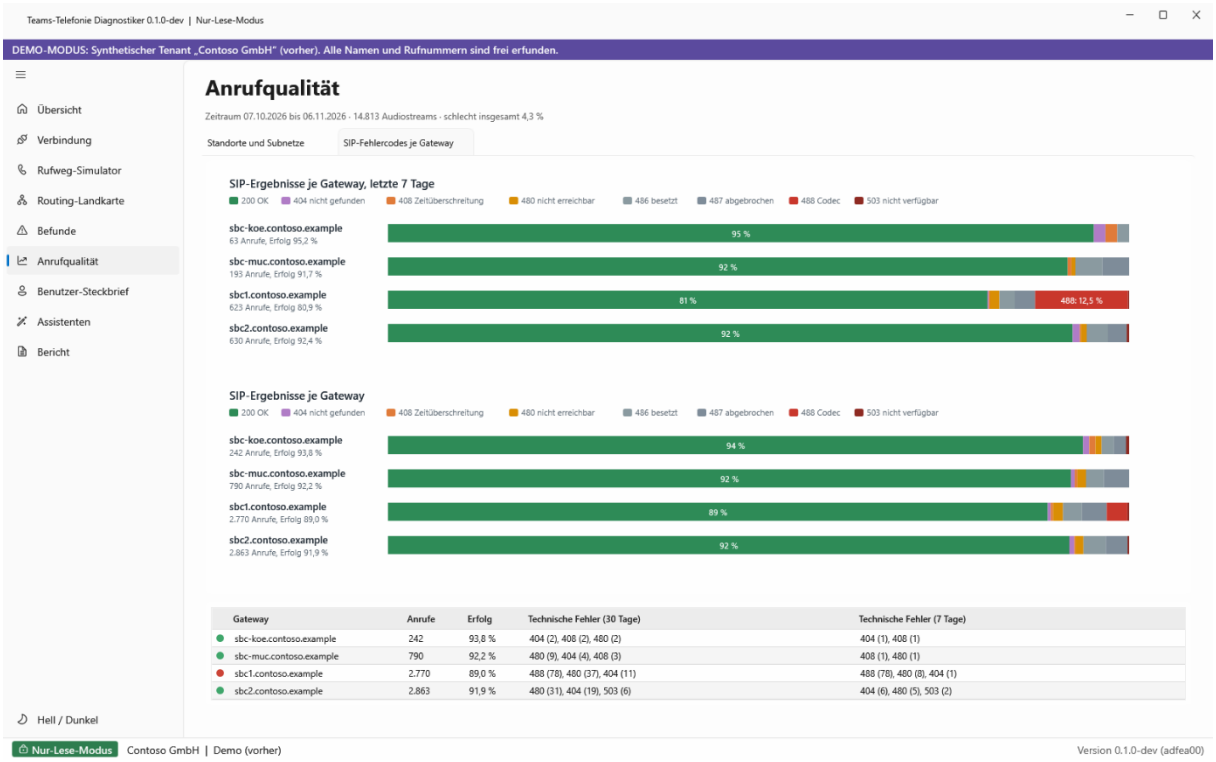
Wenn das OPTIONS-Ping sauber läuft, Anrufe aber mit Fehlercodes scheitern, liegt das Problem weiter vorn oder hinten im Rufweg. Dann helfen SIP-Fehlercodes in Teams Direct Routing verstehen und Teams-Anruf geht nicht raus: den Rufweg Schritt für Schritt prüfen.

WERKZEUG · So findet es der Teams-Telefonie Diagnostiker

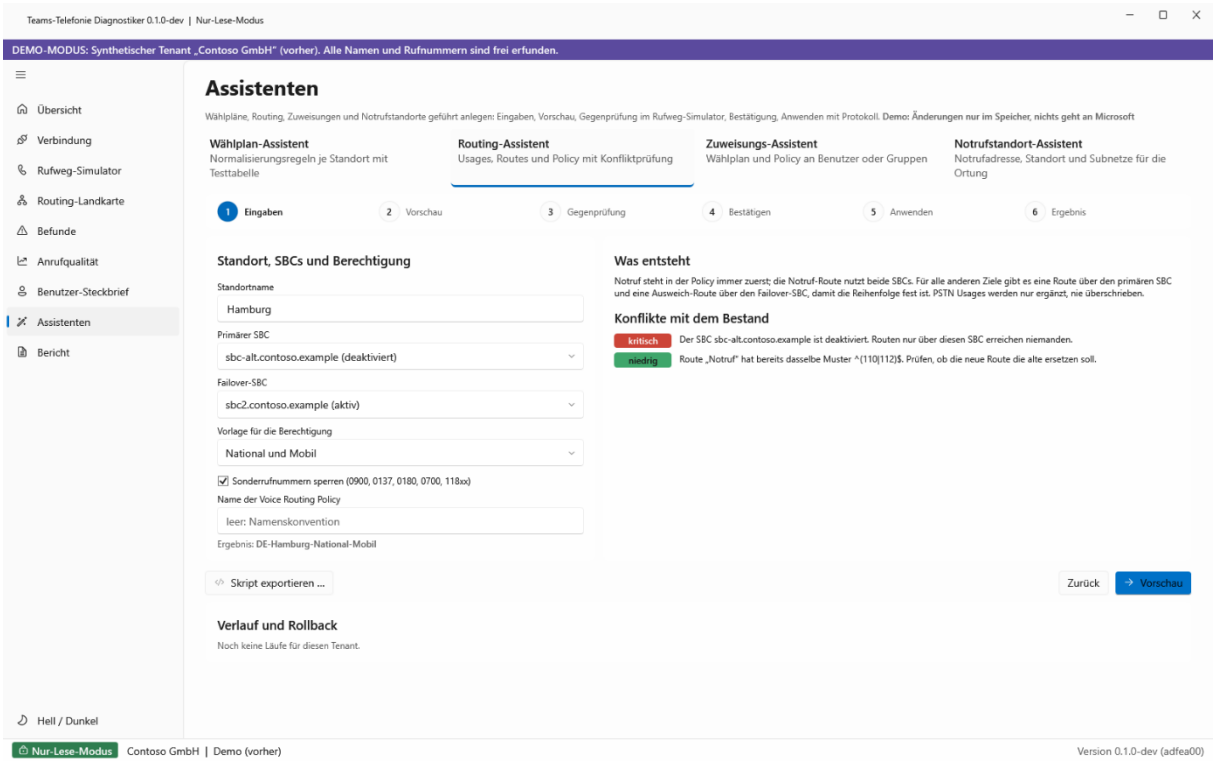
Die Ampel für SBC/Routing fasst die Befunde zu Gateways und Routen zusammen. Die Ansicht SIP-Fehlercodes je Gateway zeigt je SBC den Anteil von 200 OK und den Fehlercodes über die letzten sieben Tage und den Gesamtzeitraum. So siehst du, ob ein SBC, der im Admin Center auffällt, auch im Anrufverkehr gehäuft mit 408, 503 oder 504 antwortet, oder ob nur die Anzeige leidet.

Die Befunde mit Prüffall halten fest, worauf sich eine Meldung stützt. Die Drift-Erkennung meldet, wenn sich Gateways oder Routen seit dem letzten Stand geändert haben, etwa ein umgestellter Port oder ein deaktiviertes Gateway. Der Assistent für Routing weist vor dem Anlegen einer Route auf deaktivierte SBCs hin.

Mehr zum Werkzeug: Teams-Telefonie Diagnostiker. Du kannst es 15 Tage kostenlos testen.



Hier siehst du je Gateway, welche SIP-Ergebnisse auftreten und ob ein SBC auch im Anrufverkehr auffällt (Demo-Daten).



Der Routing-Assistent meldet einen kritischen Konflikt, wenn eine neue Route auf einen deaktivierten SBC zeigen würde (Demo-Daten).

Behebung mit Rollback

Bevor du etwas änderst, sicherst du den Stand der Gateways. Das dauert Sekunden und erspart dir im Ernstfall die Frage, wie es vorher eigentlich war.

```
$stand = Get-Date -Format "yyyyMMdd-HHmm"
Get-CsOnlinePSTNGateway | Export-Clixml ".\gateways-$stand.xml"
```

Am SBC gilt dasselbe: Konfiguration exportieren, bevor du Profile, Zertifikate oder Transportregeln anfasst. Fast jeder SBC kann das, und fast niemand macht es, bis zum ersten Mal, wo es gefehlt hat.

TLS und Zertifikat in Ordnung bringen

1. **TLS-Version anheben.** Am SBC TLS 1.2 oder höher für die Verbindung zu Microsoft erzwingen, ältere Versionen abschalten. Rollback: vorherige Transporteinstellung aus dem Export.
2. **Zertifikat erneuern.** Neue Zertifikatsanforderung (CSR) am SBC erzeugen, FQDN in CN oder SAN, Verwendungszweck Serverauthentifizierung, CA aus dem Microsoft Trusted Root Program. Zwischenzertifikat mit einbinden.
3. **Alte TLS-Sitzungen beenden.** Microsoft weist darauf hin, dass nach einem Zertifikatswechsel die alten TLS-Verbindungen getrennt und neu aufgebaut werden müssen, sonst bleiben die Ablaufwarnungen stehen. Am einfachsten über einen Neustart des SBC-Dienstes im Wartungsfenster.
4. **Stammzertifikate am SBC prüfen.** Der SBC muss dem Zertifikat des SIP-Proxys vertrauen. Fehlen die aktuellen Microsoft-Stammzertifikate, scheitert der Handshake von seiner Seite.

Rollback beim Zertifikat heißt: das alte Zertifikat bleibt bis zur erfolgreichen Umstellung im SBC hinterlegt, und du schaltest nur den TLS-Kontext um. Ist das alte schon abgelaufen, gibt es keinen sinnvollen Rollback, nur einen schnellen Vorwärtsweg.

AUS DER PRAXIS · Aus meinem eigenen Netz

Auf meinem eigenen anynode-SBC habe ich das Zertifikat erneuert, sauber mit neuer Kette, und mich über eine grüne TLS-Prüfung gefreut. Das Teams Admin Center zeigte trotzdem tagelang die Warnung zum Ablauf. Der Grund war genau der, den Microsoft dokumentiert: Die bestehenden TLS-Verbindungen liefen noch mit dem alten Zertifikat. Ein Neustart des Dienstes am späten Abend, und die Warnung war weg. Seitdem steht dieser Schritt in meiner eigenen Checkliste ganz oben.

Contact-Header und FQDN korrigieren

Am SBC legst du im SIP-Profil für die Teams-Seite fest, dass im Contact-Header der FQDN steht, nicht die IP-Adresse. Wie die Einstellung heißt, ist herstellerabhängig; gesucht ist etwas wie „Host-Name im Contact“ oder „FQDN statt IP verwenden“. Danach prüfst du im Log das nächste OPTIONS. Rollback: das vorherige SIP-Profil aus dem Export zurückspielen.

Passt dagegen der Name im Gateway nicht, korrigierst du nicht den SBC, sondern Teams. Den FQDN eines Gateways kannst du nicht umbenennen, du legst ein neues Gateway mit dem richtigen FQDN an, trägst es in die Routen ein und entfernst das alte erst danach. Wie das Anlegen im Detail geht, steht in Teams Direct Routing einrichten.

```
New-CsOnlinePSTNGateway -Fqdn "sbc1.contoso.com" -SipSignalingPort 5061 `
  -SendSipOptions $true -Enabled $true

# Rollback
Remove-CsOnlinePSTNGateway -Identity "sbc1.contoso.com"
```

WARNUNG · Enabled ausdrücklich setzen

New-CsOnlinePSTNGateway legt ein Gateway laut Microsoft deaktiviert an, wenn du Enabled nicht angibst. Ein neues Gateway ohne -Enabled $true kann grün im Dashboard stehen und trotzdem keinen einzigen ausgehenden Anruf bekommen. Und bevor du ein altes Gateway mit Remove-CsOnlinePSTNGateway entfernst, nimmst du es aus allen Voice Routes heraus. Erst die Routen, dann das Gateway.

Firewall und Port richtigstellen

- **Ausgehend:** TCP 5061 vom SBC zu 52.112.0.0/14 und 52.120.0.0/14 erlauben.
- **Eingehend:** TCP auf dem Signalisierungsport des SBC aus 52.112.0.0/14 und 52.120.0.0/14 erlauben, nicht nur aus einzelnen Adressen.
- **Medien:** UDP 3478 bis 3481 und 49152 bis 53247 in beide Richtungen, wenn kein Media Bypass genutzt wird.
- **Port in Teams und am SBC gleich:** Lauscht der SBC auf einem anderen Port als 5061, muss SipSignalingPort im Gateway genau diesen Port tragen.

```
# Vorher notieren
Get-CsOnlinePSTNGateway -Identity "sbc1.contoso.com" | Select-Object SipSignalingPort,
SendSipOptions

# Anpassen
Set-CsOnlinePSTNGateway -Identity "sbc1.contoso.com" -SipSignalingPort 5061 -SendSipOptions
$true

# Rollback mit den notierten Werten, zum Beispiel
Set-CsOnlinePSTNGateway -Identity "sbc1.contoso.com" -SipSignalingPort 5067
```

OPTIONS-Ziel und Dauerbetrieb stabilisieren

Trage am SBC als Ziele für Teams alle drei FQDNs sip, sip2 und sip3.pstnhub.microsoft.com ein, nicht ihre IP-Adressen. Microsoft nennt für Geräte, die DNS-Namen sauber verarbeiten, alternativ sip-all.pstnhub.microsoft.com, das auf alle möglichen Adressen auflöst. Prüfe außerdem, ob eine Firewall oder ein Load Balancer zwischen SBC und Internet lange TLS-Sitzungen nach einem Leerlauf-Timeout kappt, und ob ein Rate-Limit am SBC die OPTIONS von Microsoft bremst. Danach sollte der Status innerhalb weniger Minuten auf Aktiv wechseln. Bei einer frisch aktivierten Domäne kann es laut Microsoft bis zu 24 Stunden dauern.

Änderung	Rollback
TLS-Version am SBC angehoben	Transportprofil aus dem SBC-Export zurückspielen
Zertifikat getauscht	alten TLS-Kontext reaktivieren, solange das alte Zertifikat gültig ist
Contact-Header auf FQDN umgestellt	vorheriges SIP-Profil aus dem Export
Neues Gateway mit korrektem FQDN	aus Routen entfernen, dann Remove-CsOnlinePSTNGateway
SipSignalingPort oder SendSipOptions geändert	Set-CsOnlinePSTNGateway mit den notierten Werten
Firewall-Regel erweitert	vorherige Regel aus dem Firewall-Backup, aber nur mit gutem Grund

Vorbeugung: Damit Inaktiv keine Überraschung mehr ist

- **Zertifikatsablauf im Kalender.** Das Dashboard warnt 30 Tage vorher. Dein Kalender sollte früher warnen, zum Beispiel 60 Tage vorher, mit dem Neustart des SBC-Dienstes als eigenem Punkt.
- **Firewall-Regeln auf Bereiche, nicht auf Adressen.** Jede Regel für Direct Routing nennt 52.112.0.0/14 und 52.120.0.0/14. Einzelne Adressen sind beim nächsten Umzug von Microsoft falsch.
- **Inaktiv ist ein Ticket.** Auch wenn noch telefoniert wird. Ein inaktiver zweiter SBC ist ein Failover, der im Ernstfall nicht übernimmt.
- **Änderungen dokumentieren.** Firewall-Tausch, Firmware-Update, Zertifikatswechsel und Profiländerungen am SBC gehören in dasselbe Änderungsprotokoll wie die Teams-Konfiguration.
- **Gateway-Konfiguration regelmäßig vergleichen.** Ein Export pro Monat und ein Vergleich mit dem Vormonat zeigt geänderte Ports, abgeschaltete OPTIONS oder deaktivierte Gateways, bevor ein Anwender sie meldet.

Warum ein inaktiver zweiter SBC im Ernstfall nichts übernimmt und wie du den Failover gefahrlos testest, steht in SBC-Failover in Teams funktioniert nicht.

Wie du solche Vergleiche systematisch aufsetzt, steht in Konfigurationsdrift in der Teams-Telefonie erkennen. Wer die Verantwortung für Zertifikate, Firewall und SBC zwischen Netzwerk-, Sicherheits- und Telefonieteam sauber verteilen will, findet das Gerüst in Microsoft Teams Telefonie-Governance. Und wenn das Problem schon brennt und intern niemand mehr das SBC-Log lesen mag, hilft die Beratung zur Teams-Telefonie.

WEITERLESEN · Passend dazu

› Teams SBC Grundlagen: der Session Border Controller
› Teams Direct Routing einrichten
› SIP 504 nach dem Zertifikatswechsel: Root-CAs am SBC aktualisieren
› SBC-Failover in Teams funktioniert nicht
› SIP-Fehlercodes in Teams Direct Routing verstehen
› Eingehende Anrufe kommen in Teams nicht an
› Teams-Telefonie Probleme: die zehn häufigsten Ursachen

FAQ

Warum zeigt mein SBC Inaktiv, obwohl Anrufe funktionieren?

Weil der Status im Teams Admin Center laut Microsoft ausschließlich auf dem OPTIONS-Austausch beruht und nicht auf dem Anrufverkehr. Meist fehlen OPTIONS in einer Richtung, etwa wegen eines falschen Contact-Headers oder einer Firewall-Regel. Behebe das trotzdem, denn Direct Routing nutzt die OPTIONS-Informationen bei der Auswahl des SBC.

Wie oft muss der SBC OPTIONS senden?

Üblich ist einmal pro Minute. Microsoft betrachtet einen SBC als gesund, wenn er in den letzten drei Minuten vor einem Anruf OPTIONS geschickt hat. Sonst wird er herabgestuft und erst nach den gesunden SBCs versucht.

Welche TLS-Version braucht der SBC?

TLS 1.2 oder höher. Mit älteren Versionen kann der SBC laut Microsoft keine 200-OK-Antwort auf seine OPTIONS erwarten, oder die TLS-Verbindung wird sofort wieder geschlossen.

Darf ich ein Platzhalterzertifikat verwenden?

Ja, wenn es RFC 2818 entspricht. Es deckt aber nur eine Ebene ab: *.contoso.com passt auf sbc1.contoso.com, nicht auf sbc1.ffm.contoso.com.

Was ist der Unterschied zwischen Inaktiv und deaktiviert?

Inaktiv ist ein Gesundheitsstatus: Microsoft hört keine aktuellen OPTIONS oder Anrufe vom SBC. Deaktiviert ist eine Einstellung im Gateway (Enabled = False): Der SBC bekommt keine neuen ausgehenden Anrufe, egal wie gesund er ist.

Kann ich die Warnung abschalten, indem ich SendSipOptions auf False setze?

Technisch ja, sinnvoll nein. Dann fehlt das Monitoring für diesen SBC, und das Dashboard zeigt stattdessen, dass SIP-Nachrichten nicht konfiguriert sind. Microsoft empfiehlt ausdrücklich, OPTIONS eingeschaltet zu lassen.

Mein Status flackert zwischen Aktiv und Inaktiv. Woran liegt das?

Häufig sendet der SBC seine OPTIONS an feste IP-Adressen statt an die drei Microsoft-FQDNs, oder eine Zwischenzertifikatskette ist unvollständig. Auch Leerlauf-Timeouts in Firewalls und Rate-Limits am SBC kommen in Frage.

Ich habe das Zertifikat erneuert, die Warnung bleibt. Was jetzt?

Die alten TLS-Verbindungen mit dem alten Zertifikat bestehen noch. Microsoft empfiehlt, sie zu trennen, am einfachsten durch einen Neustart des SBC im Wartungsfenster. Danach baut der SBC die Verbindungen mit dem neuen Zertifikat auf.

Gilt das auch für Operator Connect?

Nein. Bei Operator Connect betreibt der Anbieter die SBCs, und Microsoft weist darauf hin, dass diese Hinweise für Direct Routing gelten. Bei Operator Connect wendest du dich an deinen Anbieter.

Fazit: Ein Ping, zwei Richtungen, fünf Verdächtige

Ein SBC, der im Teams Admin Center als Inaktiv oder mit Warnung auftaucht, ist selten ein Rätsel. Er ist ein OPTIONS-Ping, der auf dem Hin- oder Rückweg verloren geht, und die Verdächtigen sind immer dieselben: TLS-Version, Zertifikat samt Kette und FQDN, Contact-Header, Firewall und Port, OPTIONS-Ziel. Mit dem Integritätsdashboard, ein paar lesenden PowerShell-Zeilen und einem ehrlichen Blick ins SBC-Log findest du die Stelle meist in unter einer Stunde.

Der schwarze Humor der Sache: Die gefährlichste Variante ist die, bei der noch alle telefonieren. Sie wartet geduldig auf den Tag, an dem der andere SBC ausfällt, und erklärt dir dann in aller Ruhe, warum Redundanz ohne funktionierenden Ping nur ein zweites Gehäuse im Rack ist. Nimm der Warnung diesen Auftritt und kümmere dich heute darum.