



# Citrix SD-WAN WANOP 10.2

**Machine translated content**

## **Disclaimer**

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

## Contents

<b>Über Citrix SD-WAN WANOP</b>	<b>7</b>
<b>Erste Schritte mit Citrix SD-WAN WANOP</b>	<b>17</b>
<b>Wählen Sie eine Appliance basierend auf der Kapazität</b>	<b>19</b>
<b>Auswählen des Bereitstellungsmodus basierend auf der Datenzentrumtopologie</b>	<b>21</b>
<b>Standorte mit einem WAN-Router</b>	<b>23</b>
<b>Standorte mit mehreren WAN-Routern</b>	<b>25</b>
<b>Appliance-Fehler in verschiedenen Bereitstellungsmodi behandelt</b>	<b>28</b>
<b>Unterstützter Modus und Feature-Matrix</b>	<b>29</b>
<b>Konfigurieren des Citrix SD-WAN WANOP-Plug-Ins mit Access Gateway VPNs</b>	<b>30</b>
<b>Bereitstellen von SD-WAN WANOP VPX unter Microsoft Azure</b>	<b>32</b>
<b>SD-WAN WANOP-Upgradeverfahren</b>	<b>38</b>
<b>Erstkonfiguration</b>	<b>41</b>
<b>Voraussetzungen</b>	<b>41</b>
<b>Bereitstellungsarbeitsblatt</b>	<b>42</b>
<b>Konfigurieren der Appliance</b>	<b>46</b>
<b>Zuweisen einer Management-IP-Adresse über den Ethernet-Port</b>	<b>47</b>
<b>Zuweisen einer Management-IP-Adresse über den seriellen Port</b>	<b>48</b>
<b>Provisioning der Appliance</b>	<b>50</b>
<b>Bereitstellungsmodi</b>	<b>54</b>
<b>Anpassen der Ethernet-Ports</b>	<b>56</b>
<b>Port-Parameter</b>	<b>57</b>
<b>Beschleunigte Brücken (APA und aPb)</b>	<b>58</b>
<b>Motherboard-Anschlüsse</b>	<b>60</b>

<b>VLAN-Unterstützung</b>	<b>61</b>
<b>Anpassen der Ethernet-Ports</b>	<b>61</b>
<b>Ethernet-Bypass und Link-Down-Propagierung</b>	<b>62</b>
<b>Beschleunigen einer gesamten Site</b>	<b>63</b>
<b>Teilstandbeschleunigung</b>	<b>63</b>
<b>WCCP-Modus</b>	<b>64</b>
<b>WCCP-Modus (nicht gruppiert)</b>	<b>68</b>
<b>WCCP-Clustering</b>	<b>76</b>
<b>Virtueller Inlinemodus</b>	<b>83</b>
<b>Konfigurieren der Paketweiterleitung auf der Appliance</b>	<b>84</b>
<b>Router-Konfiguration</b>	<b>85</b>
<b>Virtual Inline für Multiple-WAN-Umgebungen</b>	<b>89</b>
<b>Virtueller Inlinemodus und hohe Verfügbarkeit</b>	<b>89</b>
<b>Überwachung und Fehlerbehebung</b>	<b>89</b>
<b>Gruppenmodus</b>	<b>90</b>
<b>Verwendung des Gruppenmodus</b>	<b>91</b>
<b>Funktionsweise des Gruppenmodus</b>	<b>91</b>
<b>Gruppenmodus aktivieren</b>	<b>92</b>
<b>Weiterleitungsregeln</b>	<b>94</b>
<b>Überwachung und Fehlerbehebung Gruppenmodus</b>	<b>96</b>
<b>Anpassen der Ethernet-Ports</b>	<b>96</b>
<b>Funktionsweise des Hochverfügbarkeitsmodus</b>	<b>97</b>
<b>Verkabelungsanforderungen</b>	<b>99</b>
<b>Sonstige Anforderungen</b>	<b>99</b>

<b>Management-Zugriff auf das Hochverfügbarkeitspaar</b>	<b>100</b>
<b>Konfigurieren des Hochverfügbarkeitspaars</b>	<b>100</b>
<b>Aktualisieren von Software auf einem Hochverfügbarkeitspaar</b>	<b>101</b>
<b>Speichern/Wiederherstellen von Parametern eines Hochverfügbarkeitspaares</b>	<b>102</b>
<b>Problembehandlung bei Hochverfügbarkeitspaaren</b>	<b>103</b>
<b>Zwei-Box-Modus</b>	<b>103</b>
<b>FAQ</b>	<b>108</b>
<b>Beschleunigung</b>	<b>109</b>
<b>CIFS und MAPI</b>	<b>109</b>
<b>Komprimierung</b>	<b>112</b>
<b>RPC über HTTPS</b>	<b>114</b>
<b>SCPS</b>	<b>116</b>
<b>Sicheres Peering</b>	<b>116</b>
<b>SSL-Beschleunigung</b>	<b>118</b>
<b>Citrix SD-WAN WANOP-Plug-In</b>	<b>118</b>
<b>Traffic Shaping</b>	<b>124</b>
<b>Upgrade-Prozess (OS)</b>	<b>126</b>
<b>Video-Caching</b>	<b>133</b>
<b>Office 365-Beschleunigung</b>	<b>138</b>
<b>Komprimierung</b>	<b>141</b>
<b>HTTP-Beschleunigung</b>	<b>148</b>
<b>Funktionsweise von HTML5</b>	<b>150</b>
<b>IPv6 (Internet Protocol Version 6) Beschleunigung</b>	<b>152</b>
<b>Verknüpfungsdefinitionen</b>	<b>158</b>



<b>Verwalten von Verknüpfungsdefinitionen in Traffic Shaping</b>	<b>160</b>
<b>Konfigurieren von Verknüpfungsdefinitionen</b>	<b>161</b>
<b>Verwalten und Überwachen mit Citrix Application Delivery Management</b>	<b>167</b>
<b>Citrix Cloud Connector</b>	<b>168</b>
<b>Konfigurieren des Cloud-Connector-Tunnels</b>	<b>172</b>
<b>Konfigurieren des Cloud-Connector-Tunnels zwischen zwei Rechenzentren</b>	<b>175</b>
<b>Konfigurieren des Cloud-Connector-Tunnels zwischen einem Rechenzentrum und AWS/Azure</b>	<b>181</b>
<b>Office 365-Beschleunigung</b>	<b>186</b>
<b>SCPS Unterstützung</b>	<b>199</b>
<b>Sichere Verkehrsbeschleunigung</b>	<b>200</b>
<b>Sicheres Peering</b>	<b>200</b>
<b>CIFS, SMB2 und MAPI</b>	<b>205</b>
<b>Konfigurieren der Citrix SD-WAN WANOP-Appliance zur Optimierung des sicheren Windows-Datenverkehrs</b>	<b>208</b>
<b>Konfigurieren der CIFS- und SMB2/SMB3-Beschleunigung</b>	<b>225</b>
<b>MAPI-Beschleunigung konfigurieren</b>	<b>233</b>
<b>SSL-Komprimierung</b>	<b>235</b>
<b>Funktionsweise der SSL-Komprimierung</b>	<b>236</b>
<b>Konfigurieren der SSL-Komprimierung</b>	<b>239</b>
<b>SSL-Komprimierung mit Citrix SD-WAN WANOP-Plug-in</b>	<b>247</b>
<b>RPC über HTTP</b>	<b>248</b>
<b>TCP-Durchflusskontrollbeschleunigung</b>	<b>251</b>
<b>Verlustfreie und transparente Durchflussregelung</b>	<b>252</b>
<b>Geschwindigkeitsoptimierung</b>	<b>253</b>

<b>Automatische Erkennung und automatische Konfiguration</b>	<b>255</b>
<b>TCP-Strömungssteuerungsmodi</b>	<b>257</b>
<b>Überlegungen zu Firewalls</b>	<b>258</b>
<b>Verkehrsklassifizierung</b>	<b>260</b>
<b>Anwendungsklassifizierer</b>	<b>260</b>
<b>Serviceklassen</b>	<b>262</b>
<b>Traffic Shaping</b>	<b>268</b>
<b>Gewichtete Fair Queuing</b>	<b>270</b>
<b>Traffic Shaping-Richtlinien</b>	<b>271</b>
<b>Video-Caching</b>	<b>275</b>
<b>Video-Caching-Szenarien</b>	<b>278</b>
<b>Konfigurieren der Videozwischenspeicherung</b>	<b>280</b>
<b>Video Vorbevölkerung</b>	<b>285</b>
<b>Überprüfen der Videozwischenspeicherung</b>	<b>293</b>
<b>Verwalten von Videozwischenspeicherquellen</b>	<b>296</b>
<b>WAN-Einsicht</b>	<b>298</b>
<b>Asymmetrisches Routing</b>	<b>302</b>
<b>Citrix SD-WAN WANOP-Client-Plug-in</b>	<b>304</b>
<b>Hardware- und Softwareanforderungen</b>	<b>306</b>
<b>Funktionsweise des WANOP-Plug-ins</b>	<b>307</b>
<b>Bereitstellen von Appliances für die Verwendung mit Plug-Ins</b>	<b>315</b>
<b>Anpassen der MSI-Datei des Plug-Ins</b>	<b>319</b>
<b>Bereitstellen von Plug-Ins unter Windows</b>	<b>321</b>
<b>Citrix SD-WAN WANOP-Plug-in-GUI</b>	<b>327</b>

<b>Aktualisieren des Citrix SD-WAN WANOP-Plug-ins</b>	<b>331</b>
<b>Citrix Virtual Apps and Desktops Beschleunigung</b>	<b>332</b>
<b>Konfigurieren von Virtual Apps-Beschleunigung</b>	<b>333</b>
<b>Optimieren von Citrix Receiver für HTML5</b>	<b>334</b>
<b>Bereitstellungsmodi</b>	<b>337</b>
<b>Adaptive Interoperabilität des Verkehrs</b>	<b>344</b>
<b>Citrix Hypervisor 6.5-Upgrade</b>	<b>345</b>
<b>Wartung</b>	<b>346</b>
<b>Diagnose</b>	<b>350</b>
<b>Problembehandlung</b>	<b>357</b>
<b>CIFS und MAPI</b>	<b>357</b>
<b>Citrix SD-WAN WANOP-Plug-In</b>	<b>361</b>
<b>RPC über HTTPS</b>	<b>362</b>
<b>Video-Caching</b>	<b>363</b>
<b>Citrix Virtual Apps and Desktops Beschleunigung</b>	<b>364</b>

## Über Citrix SD-WAN WANOP

April 19, 2021

Citrix SD-WAN WANOP-Appliances optimieren Ihre WAN-Verbindungen und geben Ihren Benutzern maximale Reaktionsfähigkeit und Durchsatz in jeder Entfernung. Eine Citrix SD-WAN WANOP-Appliance ist einfach bereitzustellen, da sie transparent funktioniert. Eine 20-minütige Installation beschleunigt Ihren WAN-Datenverkehr, ohne dass eine andere Konfiguration erforderlich ist. Sie müssen Ihre Anwendungen, Server, Clients oder Netzwerkinfrastruktur nicht ändern. Sie können sie jedoch nach der Citrix SD-WAN WANOP-Installation ändern, ohne dass die Verkehrsbeschleunigung beeinträchtigt wird. Eine Citrix SD-WAN WANOP-Appliance muss nur dann neu konfiguriert werden, wenn sich Ihre WAN-Verbindungen ändern.

Citrix SD-WAN WANOP-Appliances unterstützen eine breite Palette von Optimierungen, darunter:

- Multi-Session-Komprimierung mit Kompressionsverhältnissen von bis zu 10.000:1.
- Protokollbeschleunigung für Windows-Netzwerkdateisysteme (CIFS), Virtual Apps (ICA und CGP, einschließlich des neuen *ICA-Standards für Multisitzungen*), Microsoft Outlook (MAPI) und SSL.
- Traffic Shaping, um sicherzustellen, dass hoher und interaktiver Datenverkehr Vorrang vor niedriger Priorität oder Massenverkehr hat.
- Erweiterte TCP-Protokollbeschleunigung, die Verzögerungen bei überlasteten Verbindungen oder Verbindungen mit hoher Latenz reduziert.
- Videozwischenspeicherung.

### Wie funktioniert Citrix SD-WAN WANOP?

Citrix SD-WAN WANOP-Produkte arbeiten paarweise an jedem Ende einer Verbindung, um den Datenverkehr über die Verbindung zu beschleunigen. Die vom Sender durchgeführten Transformationen werden vom Empfänger umgekehrt.

Eine Appliance (oder virtuelle Appliance) kann jedoch viele Links verarbeiten, sodass Sie nicht jeder Verbindung ein Paar widmen müssen.

Ein Unternehmen verfügt in der Regel über eine Citrix SD-WAN WANOP-Appliance pro Standort (größere Appliances an größeren Standorten, kleinere an kleineren Standorten), obwohl ein Unternehmen mit zahlreichen Zweigstellen möglicherweise mehrere Appliances in seinem zentralen Rechenzentrum hat.

Ein Link von einer Site mit einer Citrix SD-WAN WANOP-Appliance zu einem Standort, der keine Citrix SD-WAN WANOP-Appliance hat, funktioniert normal, aber ihr Datenverkehr wird nicht beschleunigt.

Die Citrix SD-WAN WANOP-Funktionen umfassen eine robuste Komprimierung für lebhaftere Leistung über relativ langsame Verbindungen und eine verlustfreie Flusskontrolle zur Bewältigung von Überlastungen. TCP-Optimierungen überwinden die Hauptbeschränkungen problematischer Verbindungen, und die Anwendungsoptimierung beseitigt die Einschränkungen von Anwendungen, die für Hochgeschwindigkeitsnetzwerke entwickelt wurden. Eine automatische Erkennungsfunktion macht die Bereitstellung schnell und einfach.

## **Merkmale und Vorteile von Citrix SD-WAN WANOP**

Jede Zeit, die Mitarbeiter damit verbringen, auf ihre Computer zu warten, geht Zeit verloren, was zu einem Verlust der Produktivität führt. Wenn Benutzer remote arbeiten oder externe Ressourcen verwenden, hängt ihre Produktivität von der Reaktionsfähigkeit ihrer Netzwerkverbindungen ab. Die Sicherung der Reaktionsfähigkeit ihrer Verbindungen erfordert eine erweiterte Netzwerkbeschleunigung.

Die Citrix SD-WAN WANOP-Produktlinie schützt Ihre Produktivität, indem sie eine zuverlässige WAN- und Internet-Link-Leistung durch eine Reihe von mehreren, ineinandergreifenden Optimierungen bietet, die jeweils die anderen verstärken. Um maximale Produktivität in Ihrem gesamten Unternehmen zu bieten, gibt es Citrix SD-WAN WANOP-Produkte für jeden Bedarf, vom größten Rechenzentrum über die kleinste Niederlassung bis hin zum einzelnen Laptop.

Citrix SD-WAN WANOP bietet robuste Benutzerfreundlichkeit auch bei unterdimensionierten oder verminderten Links.

### **Merkmale auf einen Blick:**

Weitere Informationen finden Sie in der [Tabelle](#)

### **Merkmale und Vorteile:**

Im Folgenden sind einige der wichtigsten Vorteile unserer Citrix SD-WAN WANOP Produktlinie aufgeführt.

Die **Komprimierung überwindet niedrige Verbindungsgeschwindigkeiten**. Das offensichtlichste Problem bei Wide-Area-Netzwerkverbindungen (WAN) und Internetverbindungen ist ihre geringe Bandbreite im Vergleich zu lokalen Netzwerken (LANs). Ein WAN mit 1 Mbit/s hat nur 1% des Durchsatzes eines 100 Mbit/s LAN. Wie überwinden Sie niedrige Verbindungsbandbreite? Mit Kompression. Ein Komprimierungsverhältnis von 100:1 ermöglicht eine 1-Mbit/s-Verbindung, Daten so schnell wie 100 Mbit/s zu übertragen. Dieser Beschleunigungsfaktor wird erreicht, wenn die folgenden Kriterien erfüllt sind:

- Der Komprimierungsalgorithmus muss hohe Komprimierungsverhältnisse liefern können.
- Der Komprimierungsalgorithmus muss sehr schnell sein (viel schneller als die Verbindungsbandbreite und idealerweise so schnell wie das LAN).

- Die LAN-Segmente der Verbindung müssen über eine vom WAN-Segment unabhängige Flusssteuerung verfügen, da die verschiedenen Segmente Daten mit unterschiedlichen Raten verarbeiten.
- Mehrere Kompressionsmotoren müssen verwendet werden, um die unterschiedlichen Bedürfnisse der verschiedenen Arten von Verkehr zu bewältigen. Interaktiver Datenverkehr erfordert relativ geringe Bandbreite, ist aber sehr empfindlich gegenüber Verzögerungen, während Massenübertragungen sehr empfindlich auf Bandbreite reagieren, aber nicht empfindlich gegenüber Verzögerungen sind.

**TCP-Protokollbeschleunigung überwindet Staus.** Jeder Versuch, Traffic schneller als die Verbindungsgeschwindigkeit zu senden, führt zu einer Überlastung, was zu vielen Problemen führt, die durch hohe Paketverluste und hohe Warteschlangenlatenz verursacht werden.

**Verlustlose Durchflussregelung.** Das TCP/IP-Protokoll verfügt über keine Flusssteuerung, um Absender direkt zu verlangsamen, und das Fehlen dieses notwendigen Kontrollmechanismus macht Paketverluste und übermäßige Warteschlangenverzögerungen normal, selbst bei geschäftskritischen Verbindungen. (Wenn überhaupt, wird dieses Problem im Laufe der Zeit schlimmer, wie Papiere über das Phänomen der **bufferbloat** bestätigen.)

Eine Citrix SD-WAN WANOP-Appliance löst dieses Problem, indem sie die Flusssteuerung bereitstellt, die im TCP/IP-Protokoll ausgelassen wurde. Im Gegensatz zu gewöhnlichen Quality of Service (QoS)-Lösungen, die Paketverluste einfach neu zuweisen, bietet Citrix SD-WAN WANOP eine verlustfreie Flusskontrolle, die die Geschwindigkeit steuert, mit der die Endpunkt-Sender Daten übertragen können, anstatt es Absendern zu ermöglichen, Daten mit jeder Geschwindigkeit zu übertragen, die sie mögen, und Pakete beim Senden zu viel. Jeder Sender überträgt nur so viele Daten, wie Citrix SD-WAN WANOP es ihm ermöglicht, ein Paket zu senden, ohne jemals ein Paket fallen zu lassen, und diese Daten werden genau der richtigen Rate auf den Link gestellt, um die Verbindung voll zu halten, ohne zu überlaufen. Durch die Eliminierung überschüssiger Daten ist Citrix SD-WAN WANOP nicht gezwungen, diese zu verwerfen. Ohne Citrix SD-WAN WANOP müssen die verfallenen Pakete erneut gesendet werden, was zu unnötigen Verzögerungen führt. Die verlustfreie Flusssteuerung eliminiert auch Verzögerungen, die durch übermäßige Pufferung verursacht werden. Die verlustfreie Durchflusssteuerung ist der Schlüssel zu maximaler Reaktionsfähigkeit auf einer besetzten Verbindung, wodurch eine Verbindung, die einst mit einer Auslastung von 40% überlastet war, bei einer Auslastung von 95% produktiv und reaktionsschnell bleibt.

**Beseitigung distanzbasierter Ungerechtigkeit.** Verbindungen mit hoher Latenz oder Paketverlusten sind bei voller Bandbreite schwer zu verwenden, insbesondere bei normalen TCP-Varianten wie TCP Reno. Die Folgen sind übermäßige Verzögerungen und Schwierigkeiten beim Abrufen der Bandbreite, für die Sie bezahlen. Je länger die Verbindungsentfernung ist, desto schlimmer wird das Problem.

Die TCP-Protokollbeschleunigung von Citrix SD-WAN WANOP minimiert diese Effekte und ermöglicht

es, dass interkontinentale und sogar Satellitenverbindungen mit voller Geschwindigkeit ausgeführt werden.

**Traffic Shaping verwaltet die Bandbreite automatisch.** Auf der Ausgabeseite stellt ein fair-queuing-ähnlicher Algorithmus sicher, dass jede Verbindung unabhängig und angesichts ihres fairen Anteils an der Verbindungsbandbreite in die Warteschlange gestellt wird. Traffic-Forming-Richtlinien ermöglichen es, verschiedenen Diensten eine höhere oder niedrigere Priorität zu erhalten. Anwendungsoptimierungen überwinden Designbeschränkungen

Anwendungen und Protokolle, die für den Einsatz in lokalen Netzwerken entwickelt wurden, sind wegen schlechter Leistung in Wide-Area Netzwerken berüchtigt, da die Designer die Auswirkungen langer Lichtgeschwindigkeitsverzögerungen auf ihre Protokolle nicht berücksichtigt haben. Beispielsweise kann ein einfacher Windows-Dateisystem-Vorgang (CIFS) bis zu 50 Roundtrips dauern, wenn Nachrichten über das Netzwerk hin- und hergeleitet werden. In einem Weitbereichsnetzwerk mit 100 ms Roundtrip Zeit verursachen 50 Hin- und Rückfahrten eine Verzögerung von fünf Sekunden.

Obwohl die Lichtgeschwindigkeit eine grundlegende Einschränkung darstellt, können Anwendungsoptimierungen dieselben Vorgänge in einer kleineren Anzahl von Roundtrips ausführen, normalerweise durch spekulative Operationen. Wenn die ursprüngliche Anwendung jeweils einen Befehl ausgeben und darauf warten würde, dass er abgeschlossen ist, bevor der nächste Befehl ausgegeben wird, ist es oft vollkommen sicher, eine Reihe von Befehlen ohne Wartezeiten auszugeben. Darüber hinaus können die Datenübertragungen durch eine Kombination aus Pre-Fetching-, Read-Ahead- und Write-Behind beschleunigt werden. Durch das Verpacken möglichst vieler Operationen in einer einzigen Hin- und Rückfahrt kann die Leistung um das Zehnfache oder mehr gesteigert werden.

Citrix SD-WAN WANOP-Optimierungen sind besonders effektiv für CIFS/SMB (das Windows-Dateisystem), MAPI (das Outlook/Exchange-Protokoll) und HTTP.

**Mehrere Optimierungen verbessern die Leistung von Virtual Apps/Virtual Desktops (Citrix HDX).**

Da Citrix SD-WAN WANOP-Appliances Citrix Produkte sind, sind sie besonders effektiv bei der Beschleunigung von Citrix Protocol wie Citrix Virtual Apps and Desktops. Jeder Aspekt der Citrix SD-WAN WANOP-Beschleunigung kommt mit diesen Protokollen ins Spiel, um die Remote-Benutzererfahrung so produktiv wie möglich zu gestalten.

Citrix SD-WAN WANOP-Appliances verhandeln Sitzungsoptionen mit Citrix Virtual Apps and Desktops Servern. Dadurch kann die Citrix SD-WAN WANOP-Appliance die folgenden Verbesserungen anwenden:

- Es ersetzt die native Komprimierung des Servers durch leistungstärkere Citrix SD-WAN WANOP-Komprimierung.
- Sie basiert auf der Traffic Shaping-Priorität der Verbindung auf den Priority Bits, die in jeder Citrix Virtual Apps and Desktops-Verbindung eingebettet sind. Dadurch kann die Priorität der Verbindung je nach Art des Datenverkehrs variieren. Interaktive Aufgaben sind beispielsweise Aufgaben mit hoher Priorität, und Druckaufträge sind Aufgaben mit geringer Priorität.

- Es erstellt und meldet Statistiken basierend auf den verwendeten Virtual Apps- oder Virtual Desktops-Anwendungen.
- Es behält die End-to-End-Verschlüsselung der ursprünglichen Verbindung bei.

**Automatische Erkennung für minimale Konfiguration.** Da die Lösung doppelendig ist und erfordert, dass ein Citrix SD-WAN WANOP-Produkt an beiden Enden der Verbindung vorhanden sein muss, scheint die Bereitstellung die Remote-Standorte zu belasten, insbesondere solche ohne dedizierte IT-Mitarbeiter. Citrix SD-WAN WANOP ist jedoch sehr einfach zu installieren und zu warten. Eine typische Installation dauert etwa zwanzig Minuten. Die einzigen erforderlichen Parameter sind die üblichen Netzwerkparameter (wie IP-Adresse und Subnetzmaske), die Adresse eines Citrix Lizenzservers und die Sende- und Empfangsgeschwindigkeit der Verbindung.

Das Erfordern nur ein minimales Konfigurationsniveau ist aufgrund der automatischen Erkennung möglich, durch die ein Citrix SD-WAN WANOP bestimmt, welche Verbindungen ohne manuelle Konfiguration beschleunigt werden können (und welche nicht). Ein Citrix SD-WAN WANOP am anderen Ende der Verbindung wird automatisch erkannt und die Verbindung wird dann beschleunigt. Sie können Ihrem Netzwerk Act-hoc-Geräte von Citrix SD-WAN WANOP hinzufügen. Sie müssen nicht einmal die vorhandenen Geräte über die Ankunft eines neuen informieren. Sie entdecken es für sich selbst.

Ein Citrix SD-WAN WANOP verwendet TCP-Header-Optionen, um seine Anwesenheit zu melden und Beschleunigungsparameter mit dem Remote-Citrix SD-WAN WANOP auszuhandeln, da TCP-Header-Optionen Teil des TCP-Standards sind. Diese Methode funktioniert sehr gut, außer in Fällen, in denen Firewalls so programmiert sind, dass sie alle bis auf die häufigsten ablehnen -Optionen. Solche Firewalls existieren, sie können jedoch so konfiguriert werden, dass die von Citrix SD-WAN WANOP verwendeten Optionen durchlaufen werden.

Citrix SD-WAN WANOP-Operationen sind sowohl für den Sender als auch für den Empfänger transparent. Die anderen Geräte in Ihrem Netzwerk wissen nicht, dass Citrix SD-WAN WANOP existiert. Sie arbeiten weiterhin wie vor der Citrix SD-WAN WANOP Installation. Diese Transparenz macht es auch überflüssig, spezielle Software auf Ihren Servern oder Clients zu installieren, um von der Citrix SD-WAN WANOP-Beschleunigung zu profitieren. Alles funktioniert transparent.

#### **Funktionen der Produktlinie:**

Jedes Produkt der Citrix SD-WAN WANOP Produktlinie bietet grundlegende Beschleunigungsfunktionen von Citrix SD-WAN. Die meisten Modelle verfügen auch über zusätzliche Funktionen, wie zum Beispiel:

- Video-Caching
- Mehrere beschleunigte Brücken mit Ethernet-Bypass Funktion
- Überwachung und Verwaltung über GUI, CLI, SNMP, AppFlow und Citrix ADM.

Verschiedene Citrix SD-WAN WANOP-Produkte haben unterschiedliche Fähigkeiten. Produkte, die höhere WAN-Bandbreiten unterstützen, unterstützen auch mehr Benutzer und verfügen in der Regel



über mehr Ressourcen: mehr Energie-CPU, mehr Speicher, größere Festplatten und schnellere Brücken.

Die Fähigkeiten von Produkten, die auf Ihrer eigenen Hardware ausgeführt werden, wie das Citrix SD-WAN WANOP Plug-in und Citrix SD-WAN WANOP VPX, hängen von der Geschwindigkeit der Hardware und der Menge der Systemressourcen ab, die Sie der Beschleunigung widmen.

Aktuelle Spezifikationen finden Sie in Citrix [SD-WAN Produktdatenblatt](#).

## **Citrix SD-WAN WANOP-Architektur**

Citrix SD-WAN WANOP-Appliances beschleunigen den Datenverkehr über Ihre WAN-Verbindungen. Um ein WAN zu beschleunigen, benötigen Sie mindestens zwei Citrix SD-WAN WANOP-Appliances, eine für jeden Standort, den Sie beschleunigen möchten.

Die absenderseitige Citrix SD-WAN WANOP-Appliance wendet eine Reihe von Optimierungen und Transformationen auf Ihren Datenverkehr an, wie Komprimierung und Verschlüsselung. Viele Vorgänge erfordern, dass die empfangsseitige Citrix SD-WAN WANOP eine inverse Operation wie Dekomprimierung oder Entschlüsselung ausführt, um den Datenverkehr in seinen ursprünglichen Zustand zurückzusetzen.

Daher erfordern die meisten Optimierungen, dass der Datenverkehr zwei Citrix SD-WAN WANOP-Appliances durchläuft. Einige Optimierungen sind einseitig und werden von der lokalen Appliance durchgeführt, die alleine agiert. Diese Optimierungen umfassen Traffic Shaping und Video-Caching.

Citrix SD-WAN WANOP-Appliances sind weitgehend transparent für das Netzwerk. Die Appliance selbst scheint eine Brücke zu sein, kein Router, Gateway oder Proxy. Diese Unsichtbarkeit ermöglicht es, die Appliance ohne Konfiguration anderer Hardware zu installieren. Die Appliance-Optimierungen sind ebenfalls transparent und werden nur von der Partner-Appliance am anderen Ende der Verbindung erkannt.

Citrix SD-WAN WANOP-Appliances können beliebig dem Netzwerk hinzugefügt werden, da ihre Funktionen zur automatischen Erkennung und zur automatischen Verhandlung sicherstellen, dass eine neue Appliance im Netzwerk sofort von anderen Appliances erkannt wird und die Beschleunigung sofort beginnt.

Obwohl das obige Diagramm ein Netzwerk mit nur zwei Appliances zeigt, kann eine einzelne Citrix SD-WAN WANOP-Appliance mit einer beliebigen Anzahl von Partnerstandorten kommunizieren. Punkt-zu-Punkt-, Hub-and-Speichen- und Netznetzwerke werden unterstützt.

Neben eigenständigen Appliances umfassen Citrix SD-WAN WANOP-Beschleunigungsprodukte virtuelle Maschinen (die Citrix SD-WAN WANOP VPX-Serie) und einen installierbaren Beschleunigungsdienst für Windows-Systeme (das Citrix SD-WAN WANOP Plug-in).

## Was Beschleunigung bedeutet

In der Citrix SD-WAN WANOP-Terminologie ist „Beschleunigung“ die Verkürzung der Transaktionszeit, wodurch die Wartezeit der Benutzer reduziert wird. Da die Wartezeit der Benutzer einen direkten Produktivitätsverlust darstellt, ist der Hauptvorteil der Beschleunigung eine erhöhte Produktivität.

Im Netzwerkverkehr reicht eine Transaktion von sehr klein —ein einzelnes Byte von Daten in einer Telnet- oder SSH-Terminalsitzung— bis zu sehr groß, wie bei FTP-Übertragungen, die oft ein Gigabyte überschreiten. Ein praktischer Accelerator muss die gesamte Bandbreite der Transaktionsgrößen beschleunigen, vom interaktiven Traffic bis zum Massentransfer, wodurch die beste Leistung und Benutzererfahrung auf der ganzen Linie erzielt werden. Die Citrix SD-WAN WANOP-Technologie erreicht dies auf vielfältige Weise.

## Wie Beschleunigung funktioniert: Die Pipeline

Um zu sehen, wie die Citrix SD-WAN WANOP-Appliance funktioniert, werfen Sie einen Blick auf das Diagramm der Traffic-Flow-Pipeline. Wie Sie sehen können, gibt es zwei Rohrleitungen:

1. Die sendende Pipeline, die die Daten beschleunigt, die aus dem lokalen LAN in das WAN gelangen.
2. Die empfangende Pipeline, die die Daten beschleunigt, die das WAN verlassen und das lokale LAN eingeben.



## Pipeline senden

Um die Appliance zu verstehen, sollten Sie die Sendepipeline einzeln in Betracht ziehen.

1. Eingabepuffer. Pakete aus dem LAN werden von der Appliance empfangen. Da Nicht-TCP/IP-Datenverkehr nur durch den Traffic Shaper optimiert wird, werden Nicht-TCP-Pakete direkt

an den Traffic Shaper umgeleitet. Der TCP/IP-Datenverkehr (von nun an TCP-Datenverkehr genannt) durchläuft den Rest der Pipeline.

2. Video-Cache. Wenn der TCP-Datenverkehr mit den Einstellungen für den Videocache übereinstimmt, wird die Anforderung an die Videocache-Einheit übergeben.
3. LAN-seitige automatische Erkennung. Abgesehen von der Traffic Shaping müssen für die senderseitigen Optimierungen sowohl eine Remote-Appliance als auch die lokale Appliance vorhanden sein. Alle Verbindungen, die keine Remote-Appliance durchlaufen, werden zum Traffic Shaper umgeleitet. Diese Aktion wird von der LAN-seitigen Auto-Erkennungslogik ausgeführt. Der eigentliche Test für eine Remote-Appliance wird durch die WAN-seitige automatische Erkennungseinheit durchgeführt.
4. LAN-seitige Flusssteuern. Citrix SD-WAN WANOP fungiert als transparenter TCP-Proxy, der Pakete vom Endpunkt-Absender im Auftrag des Endpunkt-Empfängers empfängt und bestätigt. Dadurch kann die Appliance sehr schnell große Datenmengen vom lokalen Absender bei voller LAN-Geschwindigkeit akzeptieren, unabhängig davon, wie langsam der Datenverkehr über das WAN verläuft. (Normaler TCP verwendet eine End-to-End-Geschwindigkeitsregelung, die nicht agil genug ist, um maximale Leistung zu ermöglichen.) Darüber hinaus ist die Citrix SD-WAN WANOP-Flow-Steuerung verlustfrei, was bedeutet, dass der lokale Sender nie ein verfallene Paket sieht, was die Zuverlässigkeit und Effizienz erhöht.
5. Anwendungs-Engines. Citrix SD-WAN WANOP führt spezifische Optimierungen für mehrere Protokolle durch, darunter:
  - Citrix Virtual Apps and Desktops, wobei die Protokolle ICA und CGP verwendet werden.
  - Windows-Dateisystem (CIFS, einschließlich der SMB1- und SMB2-Versionen)
  - Outlook/Exchange (MAPI)

Diese Optimierungen reduzieren die Transaktionszeit. Dies geschieht durch Umschreiben, Kombinieren und Neuordnen von Befehlen, mithilfe von Read-Ahead- und Write-Behind, mithilfe von Kenntnissen des Protokolls für erweiterte Traffic Shaping und Komprimierungshinweise.

6. Kompressionsmotor. Durch die Komprimierung werden die Transaktionen verkürzt, wodurch die Zeit für die Übertragung der Daten über den Link verkürzt wird. Der Citrix SD-WAN WANOP-Kompressor verwendet mehrere Komprimierungsalgorithmen, einige sehr effizient für kleine Transaktionen, einige für Massentransaktionen optimiert und andere für mittlere Transaktionen. Kompressionsverhältnisse von 10.000:1 werden vom Citrix SD-WAN WANOP Kompressor leicht erreicht. Der Kompressor ist sehr schnell, so dass hohe Kompressionsverhältnisse bei vollen WAN-Geschwindigkeiten aufrechterhalten werden können. Mit der Citrix SD-WAN WANOP-Verarbeitung kann eine Datei, die im Verhältnis von 100:1 komprimiert wird, einfach über eine 1-Mbit/s-Verbindung mit einem Gesamtdurchsatz von 100 Mbit/s gesendet werden.

7. Sicherheits-Engine. Einige Citrix SD-WAN WANOP-Funktionen erfordern, dass die beiden Appliances eine sichere Peer-Beziehung untereinander und mit dem Ursprungsserver eingehen. Das Sicherheitsmodul authentifiziert diese Peer-Beziehung und verschlüsselt die beschleunigten Datenverbindungen zwischen ihnen. Eine sichere Peerbeziehung ermöglicht die Verwendung der SSL-Komprimierung und der Beschleunigung verschlüsselter Virtual Apps/Virtual Desktops-/ICA/CGP-, Windows Filesystem- (CIFS) und Outlook/Exchange (MAPI)-Datenverkehrs.
8. WAN-seitige Durchflussregelung und automatische Erkennung. Bei der WAN-Verbindung treten Verkehrsverlangsamungen auf, und wenn die Verbindung überlastet ist, gehen Pakete verloren und müssen erneut übertragen werden. Das erneute Übertragen von Paketen führt immer zu einer erheblichen Verzögerung, die manchmal länger als eine Sekunde dauert. Die WAN-seitige Durchflussregelung verwendet fortschrittliche Weiterübertragungselemente und ein fortschrittliches TCP/IP-Protokoll für maximale Leistung sowohl bei sauberen als auch bei unruhigen Verbindungen. Die automatische Erkennungseinheit identifiziert das Vorhandensein einer Citrix SD-WAN WANOP-Einheit des Partners auf Verbindungsbasis, wodurch verhindert wird, dass Optimierungen dort eingesetzt werden, wo sie nicht erwünscht sind, und dass neue Appliances von den vorhandenen Geräte erkannt werden, sobald sie dem Netzwerk hinzugefügt werden. Die automatische Erkennung verwendet Optionen im TCP-Header-Feld. Dies ist normalerweise transparent, kann aber von einigen Firewalls blockiert werden, die neu konfiguriert werden müssen.
9. Anwendungsklassifikator. Diese Unit untersucht den gesamten Datenverkehr, der durch Citrix SD-WAN WANOP fließt, und identifiziert, zu welcher Anwendung oder einem Protokoll sie gehört. Diese Informationen werden in der Berichterstellung und vom Traffic Shaper verwendet.
10. Traffic Shaper. Um Überlastung, übermäßige Warteschlangen und andere Quellen vermeidbarer Verzögerungen zu vermeiden, fügt der Traffic Shaper Datenverkehr in das WAN mit etwas weniger als die Datenrate des WAN ein, um sicherzustellen, dass das WAN nie überlaufen wird. Ein gewichteter Fair Queuing-Algorithmus wird verwendet, um sicherzustellen, dass der gesamte Datenverkehr seinen fairen Anteil an der Verbindungsbandbreite erhält. Traffic-Forming-Richtlinien ermöglichen es verschiedenen Datenverkehrstypen, unterschiedliche Gewichtungen zu empfangen, so dass ein Datenverkehr mehr Bandbreite erhält als andere.

## **Empfangspipeline**

Die Pipeline in der Empfangsrichtung ähnelt der Senderichtung, außer dass sie anstelle der Verschlüsselung entschlüsselt, und statt zu komprimieren, dekomprimiert. Beachten Sie außerdem, dass auch ein Traffic Shaper in Empfangsrichtung vorhanden ist, der Traffic Shaping-Richtlinien auf eingehenden WAN-Datenverkehr anwendet, sodass beide Richtungen geregelt werden.

## **Automatische Erkennung und Transformation auf Paketebene**

Der Algorithmus zur automatischen Erkennung fügt TCP-Header-Optionen ein, um das Vorhandensein einer Citrix SD-WAN WANOP-Appliance anzukündigen und die Verhandlung zu erleichtern. Diese Optionen liegen im Bereich von 24-31. Die folgenden Transformationen auf Paketebene werden verwendet:

- Im ersten Paket der Verbindung (das SYN-Paket) fügt die sendende Appliance Header-Optionen an, die sich selbst als Citrix SD-WAN WANOP-Appliance identifizieren, und deklariert auch andere Funktionen wie die Komprimierung. Dies wird als getaggttes SYN-Paket bezeichnet.
- Nach Erhalt eines gekennzeichneten SYN-Pakets fügt die empfangende Appliance Header-Optionen an das SYN-ACK-Paket an, identifiziert sich wiederum und kündigt seine Fähigkeiten an.
- Sobald die sendende Appliance das getaggte SYN-ACK-Paket erhält, kann die Verbindung entsprechend den Funktionen beschleunigt werden, die von beiden Appliances gemeinsam genutzt werden. Beispielsweise wird die Verbindung komprimiert, wenn beide Appliances Unterstützung für die Komprimierung deklariert haben.
- Die TCP-Anfangssequenznummern (iSNS) in beiden Richtungen werden durch Hinzufügen von 2.000.000.000 zu den ursprünglichen Werten geändert. Dies ist eine Vorsichtsmaßnahme, die verhindert, dass die Verbindung fortgesetzt wird, wenn eine Appliance ausfällt oder eine Routingänderung vorliegt, die verhindert, dass der gesamte Datenverkehr in der Verbindung angezeigt wird. Sobald eine Verbindung beschleunigt wird, muss sie während ihrer gesamten Lebensdauer beschleunigt bleiben.
- Der MSS-Wert wird in der Regel auf 1380 Byte reduziert, um sicherzustellen, dass jedes Paket Platz für die eingefügten Citrix SD-WAN WANOP TCP-Header-Optionen hat.
- Die IP-Adressen und Portnummern der Verbindung bleiben unverändert.

## **Voranmeldung**

Die SYN- und SYN-ACK-Pakete fließen von Ende zu Ende:

- Das SYN-Paket fließt vom Endpunktclient, über die clientseitige Appliance, über das WAN, über die serverseitige Appliance und schließlich zum Server.
- Das SYN-ACK-Paket fließt vom Server, über die serverseitige Appliance, über das WAN, über die clientseitige Appliance und schließlich zum Client.

Dasselbe gilt für die endgültigen Pakete der Verbindung, der FIN, FIN-ACK und RST-Pakete.

Andere Pakete werden jedoch vorab bestätigt. Wenn beispielsweise die serverseitige Appliance ein Paket vom Server empfängt, bestätigt sie es sofort über das LAN und puffert es für eine eventuelle

Übertragung über das WAN. Dadurch können die Puffer der serverseitigen Appliance sehr schnell gefüllt werden, sodass sie immer viele Daten für die Komprimierung und andere Optimierungen verwenden kann. (Dies unterscheidet sich sehr von dem normalen TCP-Vorgang, bei dem alle Bestätigungen von der gegenüberliegenden Seite des WAN kommen, was die Bestätigung sehr langsam macht und jedes Segment der Verbindung zwingt, sich nicht schneller als das langsamste Segment zu bewegen, was die Effektivität der Beschleunigung erheblich reduziert.)

## Verschieben des Datenverkehrs in und aus der Appliance

Citrix SD-WAN WANOP-Appliances verfügen über eine Reihe von „Weiterleitungsmodi“. Ein Weiterleitungsmodus ist eine Methode, um Datenverkehr in und aus der Appliance zu holen. Am gebräuchlichsten ist der Inlinemodus, bei dem der Citrix SD-WAN WANOP ein Bridge-Gerät zu sein scheint. Pakete, die an einem Bridge-Port eingegeben werden, scheinen den anderen zu verlassen. Natürlich transformiert Citrix SD-WAN WANOP Daten auf verschiedene Arten, so dass das Paket, das den zweiten Port verlässt, in vielen Fällen nicht mit dem Paket identisch ist, das in den ersten Port gelangt ist, aber so erscheint es dem Rest des Netzwerks.

Wenn der Inlinemodus nicht praktisch ist, stehen mehrere andere Methoden zur Verfügung, insbesondere der WCCP-Modus. Dies sind einarmige Modi, die ein einziges Schnittstellenkabel verwenden.

### Tipp

Sie können Ihre Citrix SD-WAN WANOP-Appliances mit Citrix ADM verwalten und überwachen, weitere Informationen finden Sie unter [Verwalten von Citrix SD-WAN Instances mit Citrix ADM](#)

## Erste Schritte mit Citrix SD-WAN WANOP

April 19, 2021

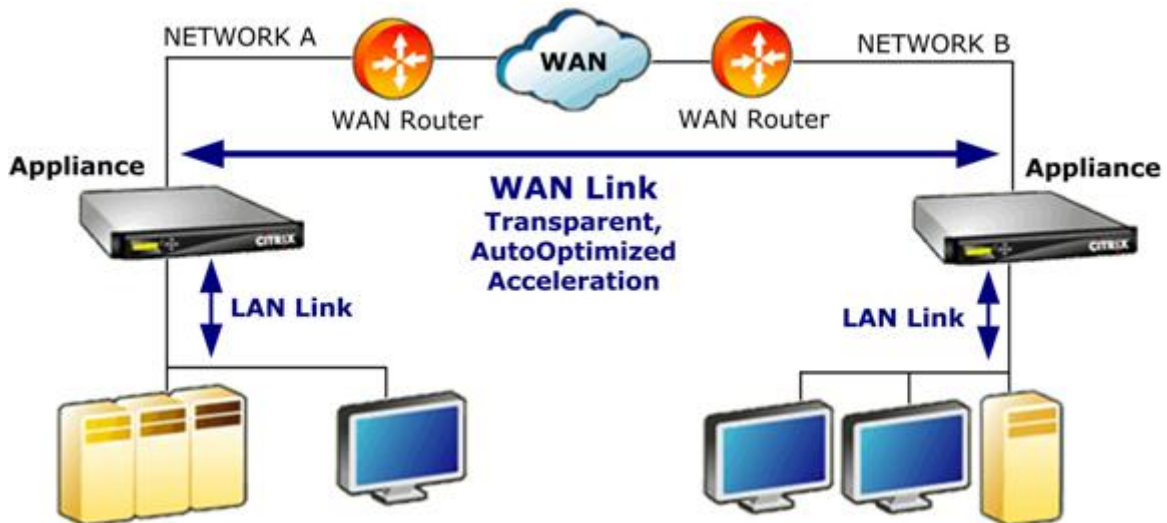
Die erfolgreiche Bereitstellung von Citrix SD-WAN WANOP-Appliances ist nicht schwierig, aber unsachgemäße Bereitstellungen können Probleme verursachen und eine unzureichende Beschleunigung ermöglichen. Achten Sie darauf, Appliances mit ausreichender Kapazität für die Links auszuwählen, die sie beschleunigen sollen. Die Produktauswahl ist auch einer der Faktoren, die bei der Entscheidung zu berücksichtigen sind, wie die Appliances am besten in Ihre Topologie passen.

Die grundlegendsten Bereitstellungskriterien sind:

- Alle Pakete in der TCP-Verbindung müssen eine unterstützte Kombination von zwei *Beschleunigungseinheiten* (Citrix SD-WAN WANOP Appliances oder Plug-ins) durchlaufen.
- Der Verkehr muss die beiden Beschleunigungseinheiten in beide Richtungen durchlaufen.

Wenn diese Kriterien erfüllt sind, erfolgt die Beschleunigung automatisch.

Beschleunigung verbessert die Leistung, wenn der Datenverkehr zwei Appliances durchläuft



Bei Standorten mit nur einem WAN-Netzwerk können diese Kriterien erfüllt werden, indem die Citrix SD-WAN WANOP-Appliance inline mit dem WAN platziert wird. In komplexeren Websites sind andere Optionen verfügbar. Einige, wie WCCP-Unterstützung, sind für alle Modelle verfügbar. Andere sind nur für bestimmte Modelle verfügbar. Daher können die Anforderungen einer komplexeren Site Ihre Wahl der Appliances einschränken.

Berücksichtigen Sie bei der Bewertung Ihrer Optionen, wie wichtig es ist, verschiedene Segmente Ihres Netzwerks aufrechtzuerhalten, falls ein Gerät ausfällt oder deaktiviert werden muss. Für Inline-Bereitstellungen empfiehlt Citrix eine *Ethernet-Bypass-Karte*. Diese Karte, die auf Citrix SD-WAN WANOP-Appliances optional ist, verfügt über ein Relay, das geschlossen wird, wenn die Appliance ausfällt, wodurch Pakete auch dann passieren können, wenn Strom verloren geht oder entfernt wird.

Redundanz ist eine Überlegung für alle Arten von Bereitstellungen. Citrix SD-WAN WANOP Appliances bieten verschiedene Arten von Redundanz:

- SD-WAN WANOP 4000/5000 Geräte haben zwei Netzteile.
- SD-WAN WANOP 4000/5000 Appliances verfügen über redundante Festplattenlaufwerke.
- Appliances können im Hochverfügbarkeitsmodus verwendet werden (zwei redundante Appliances mit automatischem Failover). Dieser Modus wird von allen Modellen unterstützt.

#### Hinweis

Weitere Informationen zu Citrix SD-WAN WANOP-Appliances und Bereitstellungsmodi finden Sie in der [Dokumentation der SD-WAN WANOP Plattform](#)

## Wählen Sie eine Appliance basierend auf der Kapazität

April 19, 2021

Für den ordnungsgemäßen Betrieb muss Ihre Citrix SD-WAN WANOP-Appliance über ausreichende Ressourcen verfügen, um die Anzahl der zu beschleunigenden WAN-Verbindungen zu unterstützen und alle Benutzer dieser Links zu unterstützen. Bei der Auswahl einer Citrix SD-WAN WANOP-Appliance sind drei Kapazitäten wichtig: Verbindungskapazität (Bandbreite), Benutzerkapazität und Festplattenkapazität.

### Verbindungskapazität

Bei der Auswahl einer Citrix SD-WAN WANOP-Appliance ist der wichtigste Faktor, dass sie Ihre WAN-Verbindungen unterstützt. Wenn Ihre Site über einen einzelnen WAN-Link verfügt, sollte Ihre Appliance die Verbindungsgeschwindigkeit unterstützen. Zum Beispiel kann ein Citrix SD-WAN WANOP 2000-010 Links von bis zu 10 Mbit/s unterstützen, was für einen 8 Mbit/s Link, aber keinen 12 Mbit/s Link geeignet wäre. Wenn Ihre Site über mehrere Links verfügt, die von einer einzelnen Appliance beschleunigt werden sollen, sollte die Appliance die Gesamtgeschwindigkeit aller hinzugefügten WAN-Verbindungen unterstützen.

Die maximale unterstützte Geschwindigkeit wird durch eine Kombination der Appliance-Hardware und der Produktlizenz bestimmt. Die lizenzierte Bandbreite ist die maximale Verbindungsgeschwindigkeit, die von der Lizenz unterstützt wird.

Produkt	Lizenzierte WAN BW Serie
<b>Aktuelle Produkte</b>	
SD-WAN WANOP Plug-in	Nicht zutreffend
SD-WAN WANOP 400	2-6 Mbit/s
SD-WAN WANOP 800	2-10 Mbit/s
SD-WAN WANOP 2000, 2000WS	10-50 Mbit/s
SD-WAN WANOP 3000	50-155
SD-WAN WANOP 4000	310-1.000 Mbit/s
SD-WAN WANOP 5000	1.500-2.000 Mbit/s
SD-WAN WANOP VPX	1-45 Mbit/s

Tabelle 1. Lizenzierte Bandbreitengrenzen nach Produktlinie



## Benutzerkapazität von Virtual Apps/Virtual Desktops

Jedes Gerät wird für eine maximale Anzahl von XenApp- oder Virtual Desktops-Benutzern bewertet. Dieser Wert darf nicht überschritten werden, wenn In der Bereitstellung Virtual Apps oder Virtual Desktops verwendet wird. Wenn Sie Virtual Apps oder Virtual Desktops nicht verwenden, beachten Sie diese Zahl für die Zahl der Benutzer anderer Anwendungen.

Produkt	Maximale Benutzer
SD-WAN WANOP Plug-in	1
SD-WAN WANOP 400	10-30
SD-WAN WANOP 800	20-100
SD-WAN WANOP 2000, 2000WS	100-300
SD-WAN WANOP 3000	300-500
SD-WAN WANOP VPX	20-350
SD-WAN WANOP 4000	750-2,500
SD-WAN WANOP 5000	3,500-5,000

Tabelle 2. Benutzerkapazität von Virtual Apps/Virtual Desktops

## Datenträgergröße

Festplattenspeicher wird hauptsächlich für den Komprimierungsverlauf verwendet, und mehr Speicherplatz führt zu einer höheren Komprimierungsleistung.

Die SD-WAN WANOP 4000/5000 Serie bietet eine Festplattenkapazität von 1,8 TB bis 2,4 TB. Im Vergleich zu 2,1 TB für das SD-WAN WANOP 3000, 470 GB für das SD-WAN WANOP 2000, 80 GB für das SD-WAN WANOP 800 und 40 GB für das SD-WAN WANOP 400. SD-WAN WANOP VPX hat eine Festplattenkapazität von 100-500 GB. Idealerweise sollte eine Appliance über eine Datenträgerkapazität verfügen, die größer ist als die Zykluszeit der Daten der Verbindung. Beispielsweise sollte ein Link, der hauptsächlich täglich Aktualisierungsdatenverkehr enthält, 24 Stunden Festplattenkapazität oder mehr. Mit einem Link, der hauptsächlich Benutzersitzungen trägt, kann dieses Fenster kleiner sein. (Ein 1 Mbit/s Link kann etwa 10 GB pro Tag bei voller Geschwindigkeit übertragen.)

Tabelle 3. Beispiele für die Datenlebensdauer für Datenträgergrößen

<b>Appliance- Modell</b>	<b>Verbindungsgeschwindigkeit 1 Mbit/s</b>	<b>Verbindungsgeschwindigkeit 10 Mbit/s</b>	<b>Verbindungsgeschwindigkeit 100 Mbit/s</b>	<b>Verbindungsgeschwindigkeit 1000 Mbit/s</b>
<b>Datenlebensdauer bei 33% Link-Auslastung</b>				
SD-WAN WANOP 800	23 Tage	2.3 Tage	Nicht verfügbar	Nicht verfügbar
SD-WAN WANOP 2000, 2000WS	141 Tage	14 Tage	Nicht verfügbar	Nicht verfügbar
SD-WAN WANOP 5000	717 Tage	72 Tage	7.2 Tage	17 Stunden
<b>Datenlebensdauer bei 100% Link-Auslastung</b>				
SD-WAN WANOP 800	8 Tage	19 Stunden	Nicht verfügbar	Nicht verfügbar
SD-WAN WANOP 2000, 2000WS	47 Tage	4.7 Tage	Nicht verfügbar	Nicht verfügbar
SD-WAN WANOP 5000	239 Tage	24 Tage	2.4 Tage	6 Stunden

## Auswählen des Bereitstellungsmodus basierend auf der Datenzentrumtopologie

April 19, 2021

Die Appliance kann mit Ihrem WAN-Link in Einklang gebracht werden. Die Appliance verwendet zwei überbrückte Ethernet-Ports für den Inlinemodus. Pakete geben einen Ethernet-Port ein und verlassen den anderen. In diesem Modus wird die Appliance zwischen Ihrem WAN-Router und Ihrem LAN platziert. Für den Rest des Netzwerks ist es, als ob die Appliance überhaupt nicht da wäre. Sein Betrieb ist völlig transparent.

Der Inlinemodus hat gegenüber den anderen Bereitstellungsmodi folgende Vorteile:

- Maximale Leistung.
- Sehr einfache Konfiguration, nur über die Schnellinstallationsseite.
- Keine Neukonfiguration Ihrer anderen Netzwerkgeräte.

Andere Modi (WCCP, Virtual Inline, Redirector) sind weniger bequem einzurichten, was im Allgemeinen erfordert, dass Sie Ihren Router neu konfigurieren, und sie haben eine etwas geringere Leistung.

Eine grundlegende Bereitstellungsüberlegung ist, ob Ihr Standort über einen einzelnen WAN-Router oder mehrere WAN-Router verfügt. Sie müssen auch darüber nachdenken, welche Features in welchen Modi verwendet werden können. Eine Anforderung zur Unterstützung von VPNs wirkt sich auf die Platzierung der Appliance in Ihrem Netzwerk aus.

Access Gateway-Appliances unterstützen Citrix SD-WAN WANOP TCP-Optimierungen und ermöglichen beschleunigte VPN-Verbindungen, wenn Citrix SD-WAN WANOP-Appliances mit Access Gateway bereitgestellt werden.

## Übersicht über die Bereitstellungsmodi

Die Appliance kann in den folgenden Modi bereitgestellt werden:

### Weiterleitungsmodi

- **Inlinemodus:** Höchste Leistung, transparenter Modus. Der Datenfluss erfolgt auf einem beschleunigten Ethernet-Port und auf dem anderen. Erfordert keine Router-Neukonfiguration jeglicher Art.
- **Inline mit zwei Brücken**—Wie inline, aber mit zwei unabhängigen beschleunigten Brücken.
- **WCCP-Modus**—Empfohlen, wenn der Inlinemodus nicht praktikabel ist. Unterstützt von den meisten Routern. Erfordert nur drei Zeilen der Router-Konfiguration. Um den WCCP-Modus auf einem Cisco-Router zu verwenden, sollte der Router mindestens IOS Version 12.0 (11) S oder 12.1 (3) T. (WCCP steht für Web Cache Communications Protocol, aber das Protokoll wurde mit Version 2.0 stark erweitert, um eine Vielzahl von Netzwerkgeräten zu unterstützen.)
- **Virtueller Inlinemodus**—Ähnlich wie im WCCP-Modus. Verwendet richtlinienbasiertes Routing. Im Allgemeinen ist ein dedizierter LAN-Anschluss am Router erforderlich. Nicht empfohlen für Geräte ohne Ethernet-Bypass Karte. Um den virtuellen Inlinemodus auf einem Cisco-Router zu verwenden, sollte der Router IOS Version 12.3 (4) T oder höher ausführen.
- **Gruppenmodus**—Wird mit zwei oder mehr Inline-Appliances (eine pro Link) innerhalb einer Site verwendet. Empfohlen nur, wenn mehrere Brücken, WCCP und virtuelle Inline-Modi unpraktisch sind.
- **Hochverfügbarkeitsmodus**—Kombiniert zwei Inline-oder virtuelle Inline-Appliances transparent zu einem primären/sekundären Paar. Die primäre Appliance verarbeitet den gesamten Datenverkehr. Wenn es fehlschlägt, übernimmt die sekundäre Appliance. Erfordert keine Routerkonfiguration. Erfordert eine Appliance mit einer Ethernet-Bypass-Karte.

- **Transparenter Modus**—Der empfohlene Modus für die Kommunikation mit dem Citrix SD-WAN WANOP Plug-in. Im transparenten Modus initiiert das Plug-In Verbindungen im Wesentlichen auf die gleiche Weise wie die Citrix SD-WAN WANOP-Appliance, wobei die ursprüngliche IP-Adresse und Portnummer der Verbindung beibehalten und Citrix SD-WAN WANOP-Optionen zu den TCP/IP-Headern ausgewählter Pakete hinzugefügt werden. Dagegen ändert das Plug-in im Redirector-Modus (nicht empfohlen) die Ziel-IP- und Portnummern der Pakete an die Signalisierungs-IP (und Port) der Appliance.
- **Redirectormodus** (nicht empfohlen) —Wird vom Citrix SD-WAN WANOP Plug-in verwendet, um den Datenverkehr an die Appliance weiterzuleiten. Kann als Standalone-Modus oder in Kombination mit einer der anderen Bereitstellungen verwendet werden. Erfordert keine Routerkonfiguration.

### Beschleunigungsmodi

- **Softboost-Modus**—Eine leistungsstarke TCP-Variante, die für die meisten Links empfohlen wird. Obwohl es weniger Leistung als der Hardboost Modus bietet, funktioniert es mit jeder Bereitstellung. Wirkt wie normales TCP, aber schneller.
- **Hardboost Modus**—Eine sehr aggressive, bandbreitenbeschränkte TCP-Variante, die für Hochgeschwindigkeitsverbindungen, interkontinentale Verbindungen, Satellitenverbindungen und andere Verbindungen mit fester Geschwindigkeit geeignet ist, für die es schwierig ist, volle Verbindungsgeschwindigkeit zu erreichen. Empfohlen für Punkt-zu-Punkt-Verbindungen mit fester Geschwindigkeit, bei denen keine Traffic Shaping erforderlich ist.

#### Hinweis

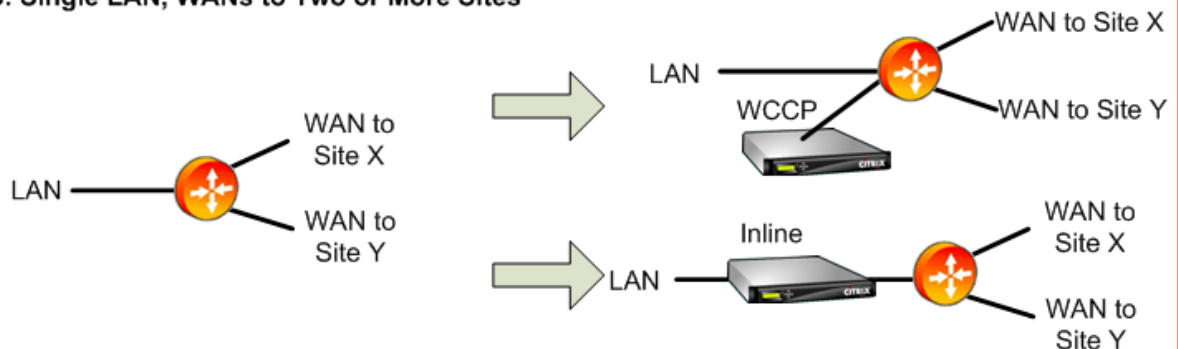
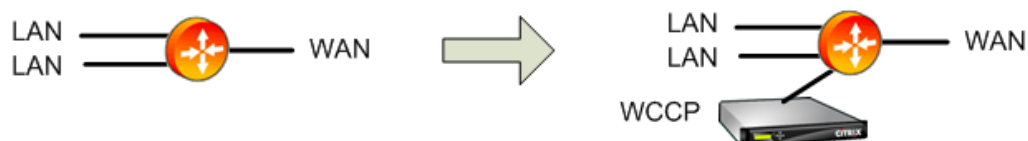
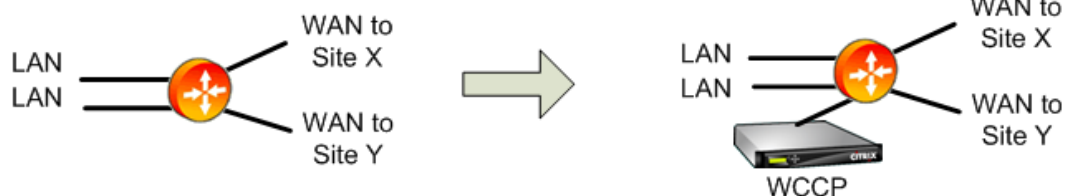
Weitere Informationen zu Citrix SD-WAN WANOP Appliances und Bereitstellungsmodi finden Sie im [Citrix SD-WAN WANOP Plattformdokumentation](#).

## Standorte mit einem WAN-Router

April 19, 2021

Bei einer Site mit nur einem WAN-Router besteht das Hauptproblem bei der Bereitstellung darin, dass die Citrix SD-WAN WANOP-Appliance im Einklang mit dem Router arbeitet. Die folgende Abbildung zeigt die empfohlenen Bereitstellungsmodi für einen einzelnen Router. Vergleichen Sie es mit Ihrer Routerverkabelung, um den besten Modus für Ihre Umgebung zu finden.

Empfohlene Bereitstellungsmodi, basierend auf WAN-Router-Topologie

**A. Single LAN, Single WAN****B. Single LAN, Redundant WANs****C. Single LAN, WANs to Two or More Sites****D. Dual LANs, Single WAN****E. Multiple LANs, Multiple WANs**

Kommentare zu den empfohlenen Bereitstellungsmodi:

1. **Ein LAN, ein WAN: Inline-Modus.** Der Router verfügt über eine einzige aktive LAN-Schnittstelle und eine einzige aktive WAN-Schnittstelle. Der empfohlene Modus für diesen Fall ist der Inlinemodus, der die einfachste Installation, die meisten Funktionen und die höchste Leistung eines jeden Modus bietet.
2. **Einzelnes LAN, Redundante WANs: Inline-Modus.** Auch für diese Konfiguration ist der Inlinemodus am besten.
3. **Ein LAN, mehrere WANs: Inline oder WCCP.** Diese Topologie fällt in zwei Kategorien: Hub-and-Spoke oder Multihop. Bei einer Hub-and-Spoke-Bereitstellung bestehen hauptsächlich

Verbindungen zwischen einem Spoke-Standort und dem Hub-Standort. In einer Multihop-Bereitstellung befinden sich viele Verbindungen zwischen zwei Spoke-Sites, wobei die Daten durch die Hub-Site geleitet werden. Eine einzelne MultiHop-Verbindung kann somit bis zu drei Appliances umfassen, je nachdem, wo sich die Appliance des Hub-Standorts im Verkehrsfluss befindet.

Für eine ordnungsgemäße Gestaltung des Datenverkehrs in Multihop-Bereitstellungen muss der gesamte WAN-Datenverkehr auf dem WAN-Router der Hub-Site auch die Appliance passieren, anstatt vom Router direkt zwischen WAN-Schnittstellen übergeben zu werden. In diesem Fall ist WCCP der bevorzugte Modus. Wenn es sich bei der Bereitstellung um Hub-and-Spoke handelt und der größte Datenverkehr auf der Hub-Site beendet wird, ist eine Inline-Bereitstellung vorzuziehen.

4. **Zwei LANs, ein WAN: Inline (mit Dual-Bridges) oder WCCP.** Dieser Modus wird von zwei beschleunigten Bridges, WCCP-Modus oder virtuellen Inlinemodus unterstützt.
5. **Mehrere LANs, mehrere WANs: Inline (Dual Bridges) oder WCCP.** Dies ist ähnlich wie Fall C, aber kompliziert durch das Vorhandensein mehrerer LAN-Schnittstellen sowie mehrerer WANs. WCCP kann hier immer verwendet werden. Im Zwei-LAN-Gehäuse kann eine Appliance mit zwei Brücken auch im Inlinemodus verwendet werden.

Weitere Informationen finden Sie in der [Tabelle](#)

## Standorte mit mehreren WAN-Routern

April 19, 2021

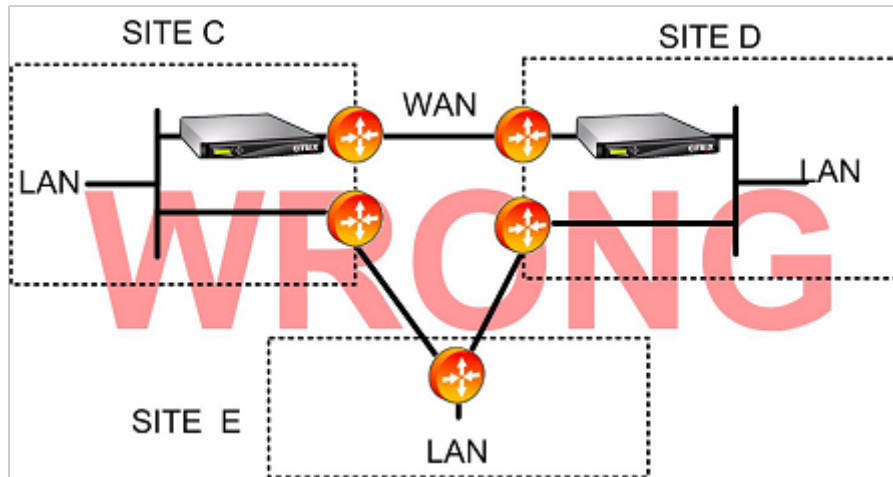
Mehr als ein WAN-Router am selben Standort erhöht die Möglichkeit eines *asymmetrischen Routing*. Normalerweise sind IP-Netzwerke nicht davon betroffen, welchen Pfad die Pakete benötigen, solange sie an ihrem Ziel ankommen. Die Appliance ist jedoch darauf angewiesen, jedes Paket in der Verbindung. "End-around"-Pakete sind nicht akzeptabel.

Bei einem Standort mit nur einem WAN-Router ist das asymmetrische Routing kein Problem, da die Appliance im Pfad zwischen dem Router und dem Rest der Site platziert werden kann, so dass der Datenverkehr in oder aus dem Router auch durch die Appliance geleitet wird. Aber mit zwei WAN-Routern kann asymmetrisches Routing ein Problem werden.

Asymmetrische Routingprobleme können während der Installation oder höher auftreten, als Folge eines Failovers auf eine sekundäre Verbindung oder anderer Formen des dynamischen Routing und Lastausgleichs. Die folgende Abbildung zeigt ein Beispiel für Standorte, die unter asymmetrischem Routing leiden könnten. Wenn die Sites C und D immer den direkten Pfad verwenden, C-D oder D-C, wenn sie Verkehr miteinander senden, ist alles in Ordnung. Pakete, die den längeren Pfad (C-E-D oder

D-E-C) verwenden, umgehen jedoch die Appliances, wodurch neue Verbindungen nicht beschleunigt werden und vorhandene Verbindungen hängen.

#### Asymmetrisches Routing

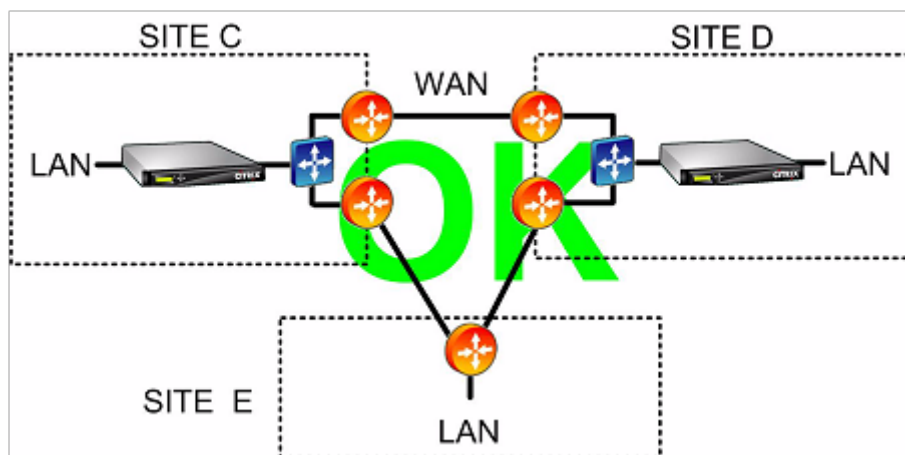


Asymmetrisches Routing kann durch Router-Konfiguration, Appliance-Platzierung oder Appliance-Konfiguration adressiert werden.

Wenn der Router so konfiguriert ist, dass sichergestellt wird, dass alle Pakete einer bestimmten Verbindung die Appliance immer in beide Richtungen passieren, gibt es keine Asymmetrie.

Wenn die Appliance nach dem Punkt positioniert ist, an dem alle WAN-Streams kombiniert werden, wird Asymmetrie vermieden, und der gesamte Datenverkehr wird beschleunigt, wie in der folgenden Abbildung dargestellt.

#### Vermeidung von asymmetrischem Routing durch die richtige Platzierung der Appliance



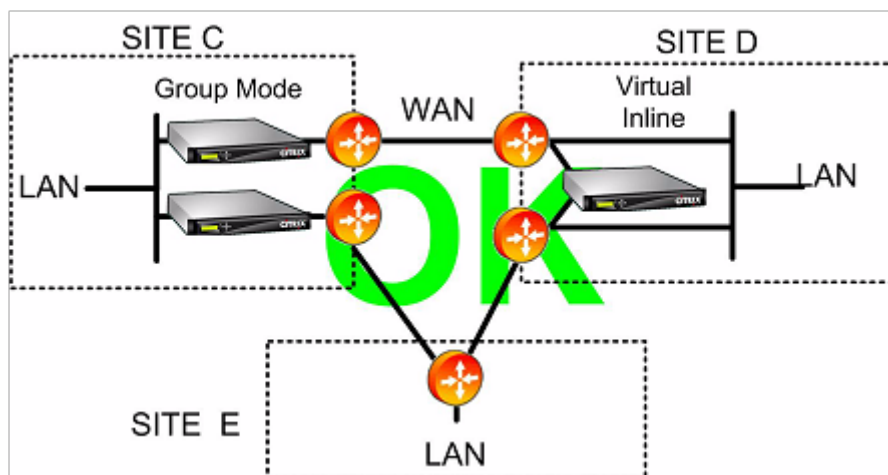
Durch die Konfiguration der Appliance für die Verwendung eines der folgenden asymmetrischen Weiterleitungsmodi kann das Problem behoben werden:

- *Mehrere Brücken.* Eine Appliance mit zwei beschleunigten Brücken oder *beschleunigten Paaren* (z. B. APA und aPb) ermöglicht das Beschleunigen von zwei Links im Inlinemodus. Die

beiden Links können völlig unabhängig, Lastenausgleich oder primär/Sicherungslinks sein.

- Im *WCCP-Modus* kann eine einzelne Appliance zwischen mehreren WAN-Routern geteilt werden, sodass sie den gesamten WAN-Datenverkehr unabhängig davon verarbeiten kann, auf welcher Verbindung sie ankommt.
- Mit dem *virtuellen Inlinemodus* kann eine einzelne Appliance zwischen mehreren WAN-Routern geteilt werden, sodass sie den gesamten WAN-Datenverkehr unabhängig davon, auf welcher Verbindung sie ankommt, verarbeiten kann.
- Der *Gruppenmodus* ermöglicht zwei oder mehr Inline-Appliances, den Datenverkehr miteinander zu teilen, wodurch sichergestellt wird, dass der Datenverkehr, der auf der falschen Verbindung ankommt, ordnungsgemäß weitergegeben wird. Da der Gruppenmodus mehrere Appliances erfordert, ist er eine teure Lösung, die sich am besten für Installationen eignet, bei denen die beschleunigten Verbindungen eine große physische Trennung aufweisen, was die anderen Alternativen erschwert. Wenn sich die beiden WAN-Verbindungen beispielsweise in verschiedenen Büros in derselben Stadt befinden (die Campus jedoch über eine LAN-Speed-Verbindung verbunden sind), kann der Gruppenmodus die einzige Wahl sein.

Asymmetrisches Routing mithilfe des Gruppenmodus oder des virtuellen Inlinemodus eliminieren

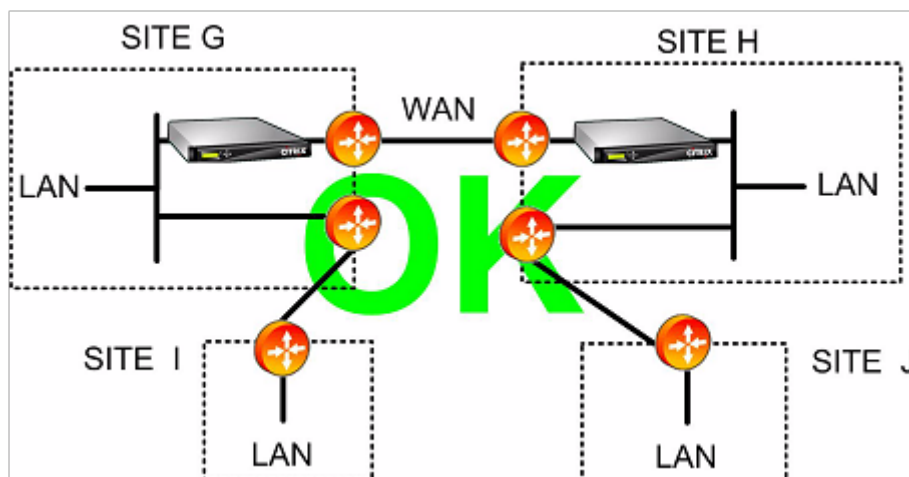


#### Hinweis

Ein Ende des Links kann den virtuellen Inlinemodus verwenden, während das andere Ende den Gruppenmodus verwendet. Die beiden Enden eines Links müssen nicht denselben Weiterleitungsmodus verwenden.

Sites mit nur einer WAN-Verbindung können keine asymmetrischen Routing-Probleme haben





## Appliance-Fehler in verschiedenen Bereitstellungsmodi behandelt

April 19, 2021

Citrix SD-WAN WANOP-Appliances bieten Schutz vor Verlust der Konnektivität bei Software-, Hardware- und Stromausfällen. Diese Sicherheitsvorkehrungen sind modusabhängig.

Im **Inlinemodus** halten Appliances bei Hardware-, Software- oder Stromausfall die Netzwerkkontinuität aufrecht. Falls vorhanden, wird das Bypass-Relais in der Appliance geschlossen, wenn Strom verloren geht oder ein anderer Fehler auftritt. Inline-Appliances ohne Bypass-Karte blockieren normalerweise den Datenverkehr im Falle eines schwerwiegenden Fehlers, aber sie leiten den Datenverkehr unter bestimmten Bedingungen weiter, nämlich wenn der Netzwerk-Stack läuft, die Beschleunigungssoftware jedoch deaktiviert wurde oder sich aufgrund anhaltender Fehler heruntergefahren hat.

Vorhandene beschleunigte Verbindungen reagieren in der Regel nach einem Fehler nicht mehr und werden schließlich von der Anwendung oder dem Netzwerkstapel an einem der Endpunkte beendet. Einige beschleunigte Verbindungen können nach dem Fehler als nicht beschleunigte Verbindungen fortgesetzt werden. Neue Verbindungen werden im nicht beschleunigten Modus ausgeführt.

Wenn die Appliance wieder online geschaltet wird, werden vorhandene Verbindungen als nicht beschleunigte Verbindungen fortgesetzt. Neue Verbindungen werden beschleunigt.

Im **WCCP-Modus** umgeht der Router eine Appliance, die nicht mehr reagiert, und öffnet die Verbindung erneut, wenn die Appliance erneut reagiert. Das WCCP-Protokoll verfügt über eine integrierte Gesundheitsprüfung.

Wenn die Option Verify-Availability im **virtuellen Inlinemodus** verwendet wird, verhält sich der Router wie im WCCP-Modus, wobei die Appliance umgangen wird, wenn sie nicht verfügbar ist, und

die Verbindung wieder hergestellt wird. Wenn die Verify-Availability nicht verwendet wird, werden alle an die Appliance weitergeleiteten Pakete gelöscht, wenn die Appliance nicht verfügbar ist.

Im **Gruppenmodus** kann eine Appliance so konfiguriert werden, dass sie Öffnen (Bridging deaktiviert) oder geschlossen (Bridging oder Umgehungsrelais aktiviert) fehlschlägt.

Wenn eine HA-Appliance im **Hochverfügbarkeitsmodus** ausfällt, übernimmt die andere automatisch. Die Bypasskarten der Geräte sind im HA-Modus deaktiviert. Wenn sich die HA-Appliances im Inlinemodus befinden und beide Appliances ausfallen, geht die Konnektivität verloren.

Im **Redirector-Modus** führt das Citrix SD-WAN WANOP Plug-in eine Zustandsprüfung auf Redirectormodus-Appliances durch und umgeht nicht reagierende Appliances, wobei stattdessen Datenverkehr direkt an Endpunktserver gesendet wird.

## Unterstützter Modus und Feature-Matrix

April 19, 2021

Im Allgemeinen sind alle Modi gleichzeitig aktiv. Einige Kombinationen sollten jedoch nicht zusammen verwendet werden, wie in der folgenden Tabelle gezeigt.

<b>**Unterstützte Kombinationen, Einheiten MIT Ethernet-Bypass Karten**</b>									
	—		—		—		—		—
<b>**Konfig.**</b>   <b>**Inline**</b>   <b>**Virtuelle Inline**</b>   <b>**WCCP- GRE**</b>   <b>**WCCP- L2**</b>   <b>**Mehrere Brücken**</b>   <b>**Hohe Verfügbarkeit**</b>   <b>**Gruppenmodus**</b>									
<b>**Citrixsd-WAN WANOP Einsteckbar**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>N</b>									
<b>**Inline**</b>   <b>**J**</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>									
<b>**Virtuelle Inline**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>N</b>									
<b>**WCCP- GRE**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>N</b>									
<b>**WCCP- L2**</b>   <b>**J**</b>   <b>**J**</b>   <b>**J**</b>   <b>N</b>									
<b>**Mehrere Brücken**</b>   <b>**J**</b>   <b>**J**</b>   <b>N</b>									
<b>**Hohe Verfügbarkeit**</b>   <b>**J**</b>   <b>**J**</b>									
<b>Unterstützte Kombinationen, Einheiten OHNE Ethernet-Bypass Karten</b>									
<b>Config.</b>   <b>Inline</b>   <b>Virtual Inline</b>   <b>WCCP- GRE</b>   <b>WCCP- L2</b>   <b>Multiple Bridges</b>   <b>High Avail.</b>   <b>Gruppenmodus</b>									
<b>Citrix SD-WAN WANOP-Plugin</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>									
<b>Inline</b>   <b>Y</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>									
<b>N</b>   <b>Virtual Inline</b>   <b>**Y</b>   <b>**Y</b>   <b>N</b>   <b>N</b>   <b>N</b>									
<b>WCCP- GRE</b>   <b>**Y</b>   <b>N</b>   <b>N</b>   <b>N</b>   <b>N</b>									
<b>WCCP- L2</b>   <b>Y</b>   <b>N</b>   <b>N</b>   <b>N</b>									

| **Mehrere Brücken** | | | | N | N | Y |

| **Hohe Vergeblichkeit.** | | | | | N | N |

**Y = Ja, unterstützt. N = Nicht unterstützt.**

## Konfigurieren des Citrix SD-WAN WANOP-Plug-Ins mit Access Gateway VPNs

April 19, 2021

Das Access Gateway Standard Edition-VPN unterstützt die Beschleunigung des Citrix SD-WAN WANOP Plug-ins, vorausgesetzt, dass eine Citrix SD-WAN WANOP-Appliance mit dem Access Gateway-Gerät bereitgestellt wird und die Access Gateway-Appliance für ihre Unterstützung konfiguriert ist.

Informationen zur Unterstützung von Citrix SD-WAN WANOP Plug-ins mit anderen VPNs finden Sie in Ihrer VPN-Dokumentation oder wenden Sie sich an Ihren Citrix Vertreter.

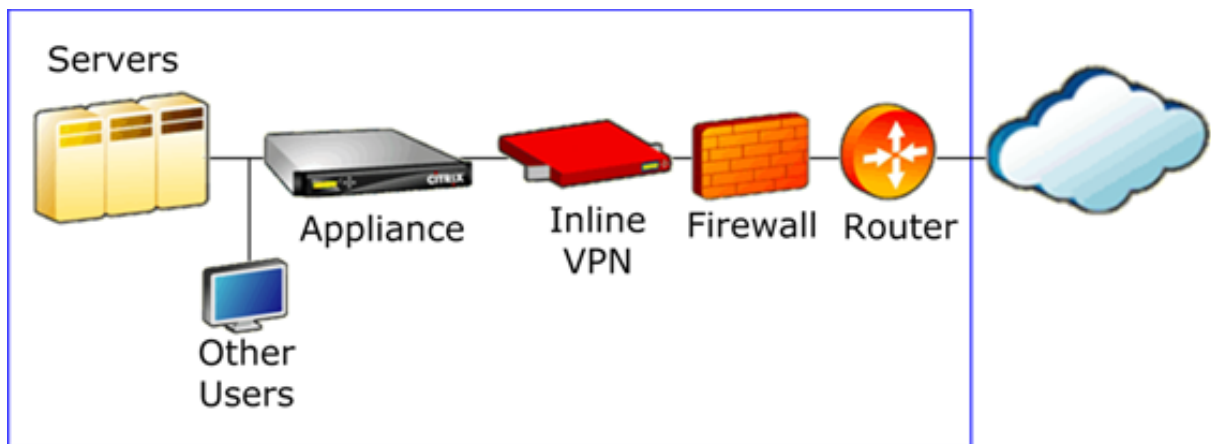
Um die Citrix SD-WAN WANOP-Unterstützung zu konfigurieren, verwenden Sie das Access Gateway-Verwaltungstool wie folgt:

1. **Aktivieren Sie auf der Seite Globale Clusterrichtlinien unter Erweiterte Optionen das Kontrollkästchen TCP-Optimierung mit Citrix SD-WAN WANOP Plug-in** aktivieren.
2. Stellen Sie sicher, dass die von Citrix SD-WAN WANOP (Redirector IP und Management IP) verwendeten IP-Adressen den Zugriff im Abschnitt Netzwerkressourcen auf der Seite Access Policy Manager aktiviert haben.
3. Aktivieren Sie für jede dieser Adressen alle Protokolle (TCP, UDP, ICMP) und aktivieren Sie TCP-Optionen beibehalten.
4. Stellen Sie sicher, dass die gleichen Adressen unter Benutzergruppen: Standard: Netzwerkrichtlinien auf der Seite Zugriffsrichtlinien-Manager enthalten sind.

### VPN-Unterstützungsoptionen

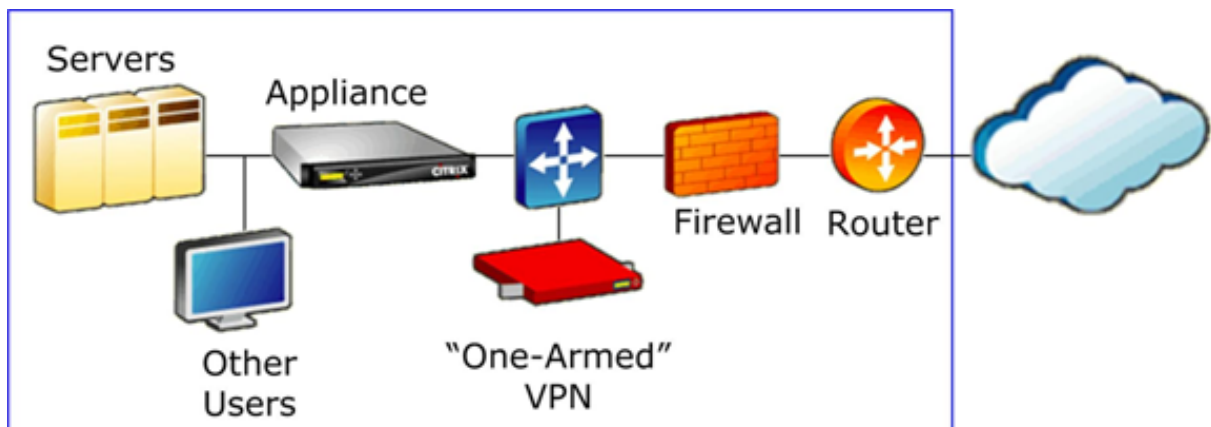
VPN-Unterstützung ist einfach nur eine Frage, die Appliance auf der LAN-Seite des VPN zu platzieren, wie in der folgenden Abbildung gezeigt. Diese Platzierung stellt sicher, dass die Appliance die entkapselte, entschlüsselte Klartext-Version des Link-Datenverkehrs empfängt und überträgt, wodurch Komprimierung und Anwendungsbeschleunigung funktioniert. (Anwendungsbeschleunigung und -komprimierung haben keine Auswirkungen auf den verschlüsselten Datenverkehr. Die TCP-Protokollbeschleunigung funktioniert jedoch bei verschlüsseltem Datenverkehr.)

VPN-Verkabelung für ein Inline-VPN



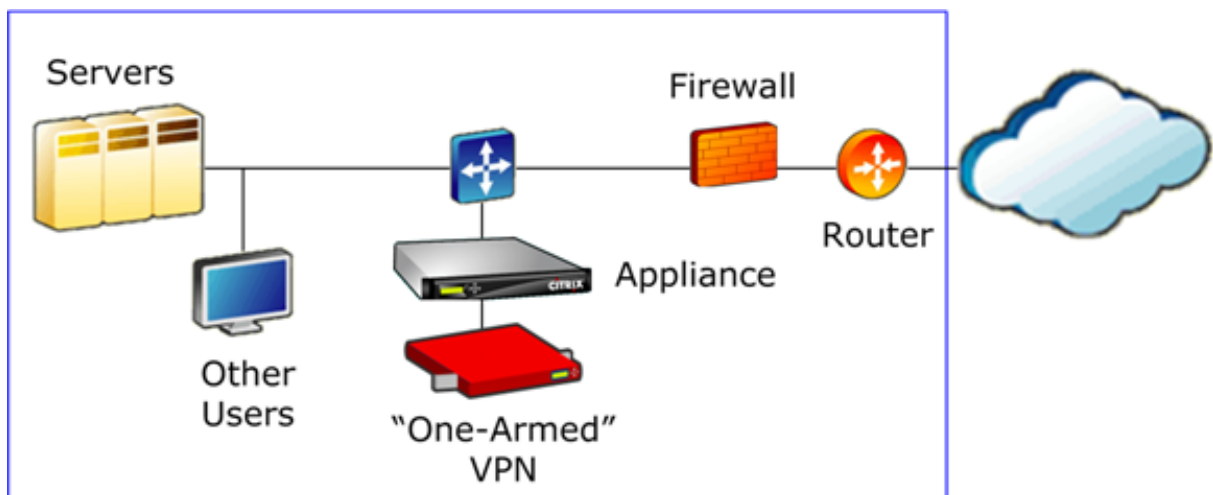
Die folgende Abbildung zeigt eine Option zum Beschleunigen von einarmigen VPNs. Die Appliance befindet sich auf der Serverseite des VPN. Der gesamte VPN-Datenverkehr mit einem lokalen Ziel wird beschleunigt. VPN-Datenverkehr mit einem entfernten Ziel wird nicht beschleunigt. Nicht-VPN-Datenverkehr kann auch beschleunigt werden.

Einarm-VPN-Beschleunigung, Option A



Die folgende Abbildung zeigt eine weitere Option zum Beschleunigen von Einarm-VPNs. Die Appliance befindet sich auf der Serverseite des VPN. Der gesamte VPN-Datenverkehr mit einem lokalen Ziel wird beschleunigt. VPN-Datenverkehr mit einem entfernten Ziel wird nicht beschleunigt. Nicht-VPN-Datenverkehr kann auch beschleunigt werden.

Einarmige VPN-Beschleunigung, Option B



### Wichtig

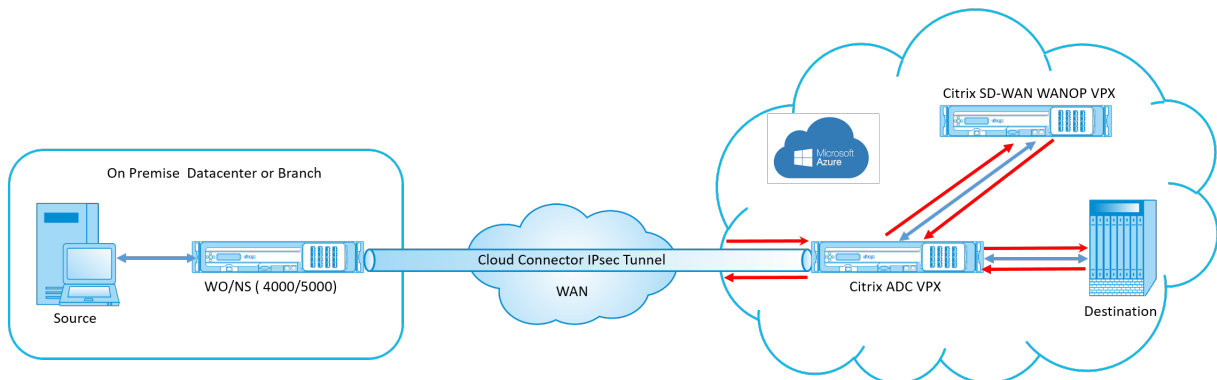
Damit die Beschleunigung wirksam ist, muss das VPN TCP-Header-Optionen beibehalten. Die meisten VPNs tun dies.

## Bereitstellen von SD-WAN WANOP VPX unter Microsoft Azure

April 19, 2021

Citrix SD-WAN WANOP Edition ist jetzt im Azure-Marktplatz verfügbar und ermöglicht die WAN-Optimierung zwischen Unternehmens-Rechenzentrum/Branch und Azure-Cloud. Da die Unterstützung des L2-Modus auf Cloud-Infrastrukturen nicht verfügbar ist, können Sie Citrix SD-WAN WANOP nicht als eigenständiges VPX in Azure Cloud bereitstellen. Sie können jedoch Citrix SD-WAN WANOP VPX zusammen mit Citrix ADC VPX in der Azure-Cloud-Infrastruktur bereitstellen. Citrix ADC verwendet Cloud-Connector, um einen IPSec-Tunnel zu erstellen, während der Citrix SD-WAN WANOP VPX die Verbindungen beschleunigt und LAN-ähnliche Leistung für Anwendungen bietet.

## Citrix SD-WAN WANOP in der Azure Cloudtopologie



Das Topologiediagramm zeigt ein Citrix SD-WAN 4000/5000, das im Rechenzentrum oder Zweigstellen bereitgestellt wird. Sie können auch Citrix SD-WAN WANOP- und Citrix ADC Appliance im Zwei-Box-Modus bereitstellen oder beide VPX sein. Im Azure-Cloud-VNET wird Citrix SD-WAN WANOP VPX im Onearm-Modus (PBR) mit dem Citrix ADC VPX bereitgestellt.

## Übersicht über die Bereitstellung

So stellen Sie SD-WAN WANOP unter Microsoft Azure bereit:

1. Stellen Sie eine Citrix ADC VPX Instanz in der Azure-Cloud bereit. Weitere Informationen finden Sie unter [Bereitstellen einer Citrix ADC VPX Instanz in Microsoft Azure](#). Konfigurieren Sie vier Netzwerkschnittstellen in vier verschiedenen Subnetzen und aktivieren Sie die IP-Weiterleitung auf allen Netzwerkschnittstellen. Die vier Netzwerkschnittstellen werden verwendet als:
  - Verwaltungsoberfläche
  - WAN-Seite Schnittstelle, für IPsec-Tunnel
  - LAN-seitige Schnittstelle, zur Verbindung mit dem Server
  - WANOP-Kommunikationsschnittstelle, um mit Citrix SD-WAN WANOP VPX in der Azure-Cloud zu kommunizieren.
2. Stellen Sie einen Citrix SD-WAN WANOP VPX in der Azure-Cloud bereit. Weitere Informationen finden Sie im folgenden Bereitstellungsverfahren.
 

**Hinweis:** Aktivieren Sie die IP-Weiterleitung auf der WANOP-Schnittstelle.
3. Konfigurieren Sie einen IPsec-Tunnel zwischen der lokalen Appliance und dem Citrix ADC VPX in der Azure-Cloud unter Verwendung der öffentlichen IP-Adresse der Citrix ADC WAN-Schnittstelle. Weitere Informationen zum Konfigurieren von IP-Tunneln finden Sie unter [IP-Tunnel](#).

4. Konfigurieren Sie Citrix ADC VPX, um die Pakete an Citrix SD-WAN WANOP VPX umzuleiten. Verwenden Sie die private IP-Adresse der WANOP-Kommunikationsschnittstelle und erstellen Sie einen virtuellen Lastausgleichsserver. Weitere Informationen finden Sie unter [Erstellen eines virtuellen Lastausgleichsservers](#).
5. Konfigurieren Sie die folgenden Routentabellen in Azure:
  - Routingtabelle für WANOP-Schnittstelle auf Citrix ADC VPX —Routentabelleneinträge sollten Quell- und Zieladresse als Client- bzw. Serversubnetze aufweisen. Die IP-Adresse der WANOP-Schnittstelle des Citrix ADC VPX ist der nächste Hop.
  - Routingtabelle für Citrix SD-WAN WANOP-Schnittstelle - Routingtabelleneinträge sollten Quell- und Zieladresse als Client- bzw. Serversubnetze aufweisen. Die Citrix SD-WAN WANOP-Schnittstelle IP-Adresse ist der nächste Hop.

Im obigen Beispiel, wenn die Quelle versucht, auf eine Anwendung auf dem Cloud-Ziel zuzugreifen, werden die Pakete durch den etablierten IPSec-Tunnel geleitet. Am Ende der Azure Cloud VNET empfängt der Citrix ADC VPX die Pakete, entschlüsselt und leitet sie an Citrix SD-WAN WANOP VPX weiter. Citrix SD-WAN WANOP VPX verarbeitet die Pakete, optimiert sie und sendet sie zurück an Citrix ADC VPX. Citrix ADC VPX sendet das Paket an das Ziel. Auf dem Rückgabepfad leitet Citrix ADC VPX die Pakete zur Optimierung an Citrix SD-WAN WANOP VPX weiter. Die optimierten Pakete werden über den etablierten IPSec-Tunnel an die Quelle übertragen.

## Bereitstellen von Citrix SD-WAN WANOP VPX unter Microsoft Azure

So stellen Sie Citrix SD-WAN WANOP VPX unter Microsoft Azure bereit:

1. Navigieren Sie in Microsoft Azure zu **Startseite > Marktplatz > Netzwerk**, suchen Sie nach **Citrix SD-WAN WANOP** und installieren Sie es.
2. Wählen Sie auf der Seite Citrix SD-WAN-OP aus der Dropdownliste **Ressourcen-Manager** aus, und klicken Sie auf **Erstellen**. Die Seite **Citrix SD-WAN-Optimierung erstellen** wird angezeigt.
3. Wählen Sie im Abschnitt **Grundlagen** den Abonnementtyp, die Ressourcengruppe und den Speicherort aus. Klicken Sie auf OK.

**Hinweis:** Sie können eine Ressourcengruppe erstellen. Eine Ressourcengruppe ist ein Container, der zugehörige Ressourcen für eine Azure-Lösung enthält. Die Ressourcengruppe kann alle Ressourcen für die Lösung oder nur die Ressourcen enthalten, die Sie als Gruppe verwalten möchten.

The screenshot shows the 'Create Citrix SD-WAN WANOP' wizard in the Azure portal. The left sidebar contains navigation links like 'Create a resource', 'All services', and 'FAVORITES'. The main area shows a progress bar with five steps: 1. Basics (selected), 2. Administrator settings, 3. Citrix SDWAN WANOpt myappl..., 4. Summary, and 5. Buy. The 'Basics' step is expanded, showing fields for 'Subscription' (Enterprise Dev/Test), 'Resource group' (surya\_wanpt-test, with 'Use existing' selected), and 'Location' (East US 2). An 'OK' button is highlighted with a red box at the bottom right.

4. Geben Sie im Abschnitt **Administrator** den Namen und die Anmeldeinformationen für die virtuelle Citrix SD-WAN WANOP Maschine ein. Klicken Sie auf **OK**.



The screenshot shows the 'Create Citrix SD-WAN WANOP' wizard in the 'Administrator settings' step. The left sidebar contains navigation options: 'Create a resource', 'All services', 'FAVORITES', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', and 'Advisor'. The main pane displays a progress bar with five steps: 1. Basics (Done), 2. Administrator settings (selected), 3. Citrix SDWAN WANOpt myappl..., 4. Summary, and 5. Buy. The 'Administrator settings' section on the right includes four fields: 'Virtual Machine name' (citrixwanopt), 'Username' (suryaprakp), 'Password' (masked), and 'Confirm password' (masked). Each field has a green checkmark indicating it is valid. An 'OK' button is highlighted with a red rectangle at the bottom right.

5. Konfigurieren Sie im **Abschnitt Citrix SD-WAN WANOP-Einstellungen** die Einstellung für Citrix SD-WAN WANOP VPX entsprechend Ihren Anforderungen. Klicken Sie auf **OK**.

1 Basics Done ✓

2 Administrator settings Done ✓

3 Citrix SDWAN WANOpt myappl... Configure Citrix SD-WAN WAN...

4 Summary Citrix SD-WAN WAN Optimisat...

5 Buy

\* Virtual machine size 1x Standard D3 v2

OS Disk Size(GB) 50

\* Storage account suryausregion

\* Public IP address for management... (new) sdwanwanopt-mgmt

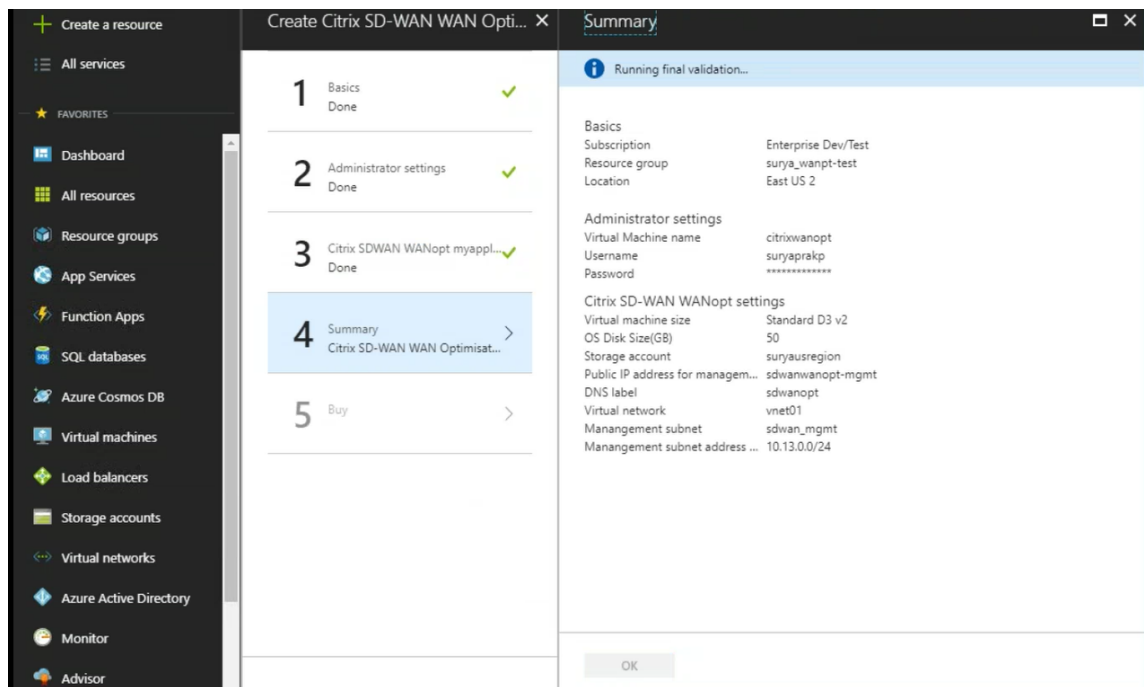
\* DNS label sdwanopt ✓ eastus2.cloudapp.azure.com

\* Virtual network (new) vnet01

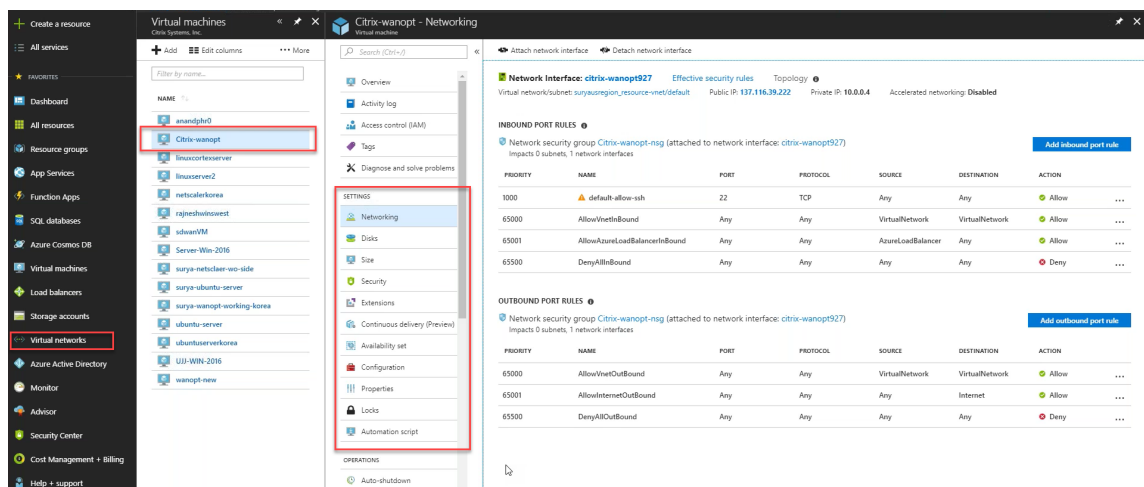
\* Subnets Review subnet configuration

OK

6. Die Konfiguration, die Sie in den vorherigen Schritten angegeben haben, wird überprüft und angewendet. Wenn Sie richtig konfiguriert haben, wird die Bestätigungsmeldung angezeigt. Klicken Sie auf **OK**.



7. Navigieren Sie nach erfolgreicher Bereitstellung zu **Virtuellen Netzwerken**, um Citrix SD-WAN WANOP VPX anzuzeigen. Sie können die Parameter der virtuellen Maschine weiter konfigurieren, indem Sie die Option Einstellungen verwenden.



## SD-WAN WANOP-Upgradeverfahren

December 14, 2022

Dieser Abschnitt enthält Informationen zum Herunterladen und Aktualisieren der Softwarepakete Citrix SD-WAN WAN Optimization (WANOP).

#### **Hinweis:**

Bevor Sie die Software herunterladen, müssen Sie eine Citrix SD-WAN -Softwarelizenz erwerben und registrieren. Weitere Informationen finden Sie unter [Lizenzierung](#).

### **Laden Sie die Softwarepakete herunter**

Um die Citrix SD-WAN WANOP-Softwarepakete herunterzuladen, gehen Sie zur URL; [Produktdownloads](#). Anweisungen zum Herunterladen der Software finden Sie auf dieser Seite.

So laden Sie das Citrix SD-WAN WANOP-Softwarepaket herunter:

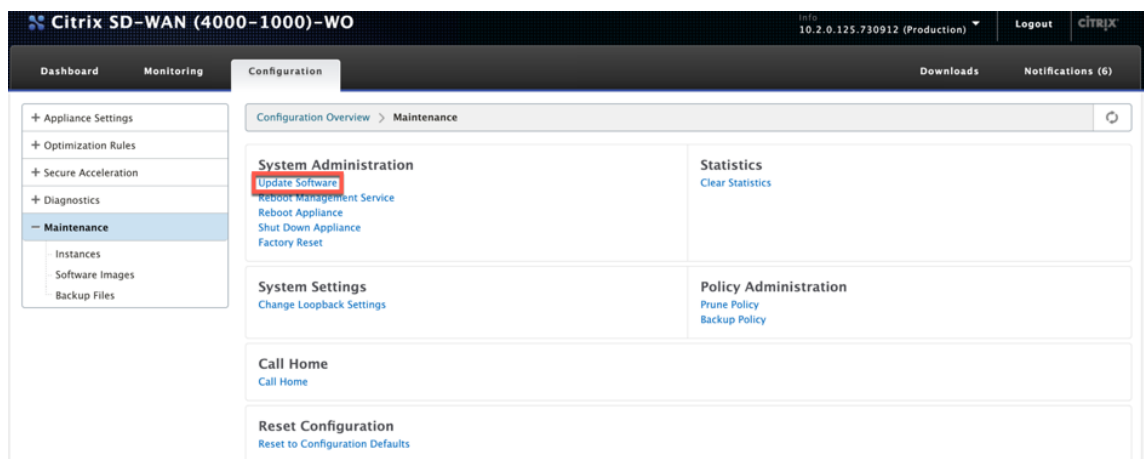
1. Melden Sie sich mit Ihren Anmeldeinformationen auf [citrix.com](#) an.
2. Gehen Sie zur [Download](#)-Seite und wählen Sie das Produkt (Citrix SD-WAN) aus der Dropdown-liste aus.
3. Erweitern Sie die **Citrix SD-WAN WANOP Edition** und wählen Sie die erforderliche Softwareversion aus.
4. Die folgenden Download-Optionen sind verfügbar. Laden Sie die erforderliche Software herunter.
  - Laden Sie die Upgrade-Datei .upg für SD-WAN WANOP 400/1000/2000/3000/4000/4100/5000/5100-Appliances herunter.
  - Laden Sie die BIN-Upgrade-Datei für SD-WAN WANOP VPX-Appliances herunter.

Weitere Informationen zu den von SD-WAN WANOP unterstützten Plattformen finden Sie unter [SD-WAN-Plattformmodelle und Softwarepakete](#).

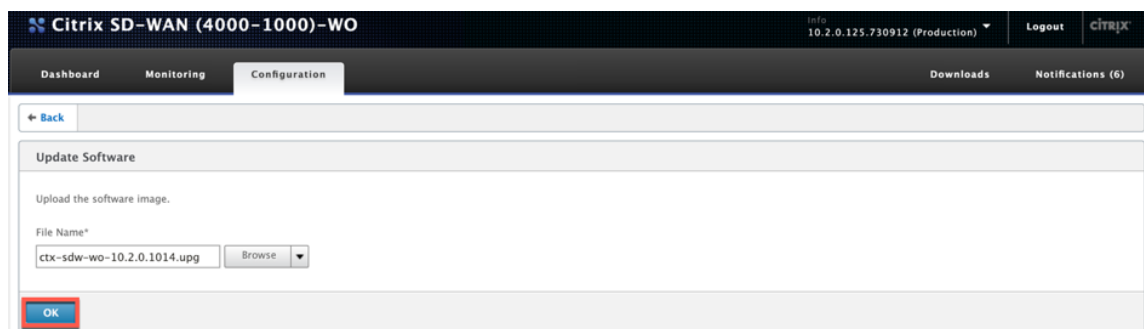
### **Upgradeverfahren**

Gehen Sie wie folgt vor, um die Software zu aktualisieren:

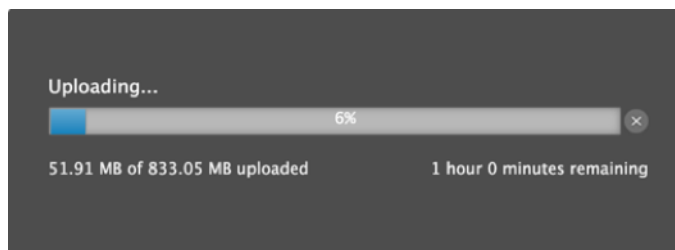
1. Navigieren Sie zu **Konfiguration > Wartung > Systemadministration** klicken Sie auf **Software aktualisieren**.



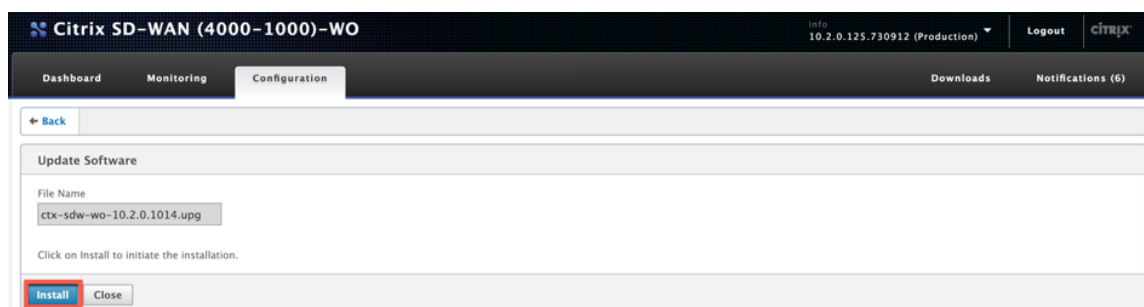
2. Klicken Sie auf **Durchsuchen**, um die Datei **ctx-sdw-wo-10.2.X.upg** bereitzustellen. Klicken Sie auf **OK**.



Sie können die Statusleiste für den Upload sehen.



3. Wenn eine Meldung darüber informiert wird, dass der Upload erfolgreich war, klicken Sie auf **Installieren**.



4. Die Appliance führt das Upgrade durch, das je nach Plattformmodell 10—40 Minuten dauert.

Es zeigt eine Reihe von Statusmeldungen an, beginnend mit **Vorbereitung des Upgrades** und endend mit **Abschluss des Upgrades erfolgreich**.

5. Klicken Sie auf **OK**, um die aktualisierte Benutzeroberfläche anzuzeigen.

## Erstkonfiguration

April 19, 2021

Nachdem Sie die Verbindungen überprüft haben, können Sie die SD-WAN-Appliances im Netzwerk bereitstellen.

Auf der von Citrix ausgelieferten Appliance sind standardmäßig IP-Adressen konfiguriert. Um die Appliance im Netzwerk bereitzustellen, müssen Sie die entsprechenden IP-Adressen auf der Appliance konfigurieren, um den Netzwerkverkehr zu beschleunigen.

Die Erstkonfiguration besteht aus folgenden Aufgaben:

- Identifizieren Sie die Voraussetzungen für die Erstkonfiguration.
- Erfassen Sie verschiedene Werte, die in der Erstkonfigurationsprozedur erforderlich sind.
- Konfigurieren Sie die Appliance, indem Sie sie an den Ethernet-Port anschließen.
- Weisen Sie die Verwaltungs-IP-Adresse über die serielle Konsole zu.

Standardmäßig wird die Appliance bei der Erstkonfiguration im Inlinemodus bereitgestellt.

## Voraussetzungen

April 19, 2021

Um eine Citrix SD-WAN 4100- oder 5100-Appliance bereitzustellen, müssen Sie die folgende erforderliche Einrichtung durchführen, bevor Sie die Appliance konfigurieren.

## Softwareversionen

Dieses Dokument behandelt die Veröffentlichung der SD-WAN-Software. In den Versionshinweisen finden Sie die empfohlenen Versionen der NetScaler -Software, die der gewünschten Version der SD-WAN-Software entsprechen. Verwenden Sie niemals andere Versionen als die für SD-WAN 4100 und 5100 Geräte empfohlenen.

## Lizenzdatei

Die Anzahl der Accelerator-Appliances hängt von der Hardwareplattform und der Art der Lizenz ab, die Sie für die Appliance anwenden. In der folgenden Liste wird die Anzahl der Beschleuniger angezeigt, die vom Konfigurations-Assistenten automatisch bereitgestellt werden:

- Modell 310: Zwei
- Modell 500: Drei
- Modelle 1000 und 1500: Six
- Modell 2000: Eight

Bevor Sie mit dem Provisioning der Appliance beginnen, empfiehlt Citrix, dass Sie die Lizenzdatei bei sich haben, da sie früh im Konfigurationsprozess erforderlich ist, um eine Lizenzdatei herunterzuladen, führen Sie das im Benutzerhandbuch My Account Alle Lizenzierungstools beschriebenen Verfahren durch.

## Installation der Hardware

Nachdem Sie die Hardware-Appliance von Citrix erhalten haben, müssen Sie sie im Netzwerk installieren. Um die Hardware der SD-WAN 4100/5100 Appliance zu installieren, befolgen Sie das Installationsverfahren unter [Installation der Hardware](#).

## Bereitstellungsarbeitsblatt

April 19, 2021

### Hinweis

Verwenden Sie dieses Arbeitsblatt nur, wenn Sie mit dem Konfigurationsassistenten Release 9.3 das Provisioning einer Appliance durchführen, die auf Werkseinstellungen zurückgesetzt wird. Wenn Sie einfach ein Upgrade eines zuvor konfigurierten Systems auf Version 9.3 durchführen, behält die Appliance die vorherige Konfiguration bei, die sich unterscheiden wird.

Die Appliance verwendet mindestens zwei Ports: den Verwaltungs-Port (normalerweise 0/1) und den Verkehr-Port (z. B. 10/1). Der Inlinemodus verwendet Verkehrsanschlüsse paarweise, z. B. die Ports 10/1 und 10/2. Ports müssen im Voraus ausgewählt werden, da die Konfiguration von ihrer Identität abhängt.

Die Appliance verwendet direkt drei Subnetze: das Verwaltungssubnetz, das Subnetz des externen Datenverkehrs und das Subnetz des internen Datenverkehrs. In jedem Subnetz werden mehrere IP-

Adressen verwendet. Jedes Subnetz muss zusammen mit der richtigen Subnetzmaske angegeben werden.

Die folgende Abbildung ist ein Arbeitsblatt für diese Parameter. Es unterstützt Inline- und WCCP-Modi mit und ohne hohe Verfügbarkeit. Die Tabelle unter der Abbildung beschreibt, was jeder Eintrag bedeutet.

**Tabelle 1. Deployment-Arbeitsblattparameter**

	Parameter	Beispiel	Ihr Wert	Beschreibung
Management-Subnetz	M2.	Gateway-IP-Adresse	10.199.79.254	Standardgateway für das Management-Subnetz.
	M3.	Subnetzmaske	255.255.255.128	Subnetzmaske für das Management-Subnetz.
	M4.	Xen Hypervisor-IP-Adresse	10.199.79.225	IP-Adresse von Xen Hypervisor.
	M5.	IP-Adresse der Dienst-VM	10.199.79.226	IP-Adresse der Verwaltungsdienst-VM, die die Konfiguration steuert.
	M6.	Accelerator-Benutzeroberfläche	10.199.79.227	Accelerator GUI, auch Broker UI genannt, die die Instanzen als Einheit verwaltet.
	M7.	NetScaler Verwaltungs-IP-Adresse	10.199.79.245	IP-Adresse der GUI- und CLI-Schnittstellen der NetScaler Instanz.



	Parameter	Beispiel	Ihr Wert	Beschreibung
Subnetz für externes Datenverkehr				
T1.	IP-Adresse des Routers	172.17.17.1		IP-Adresse des Routers im Subnetz des externen Datenverkehrs.
T2.	Subnetzmaske	255.255.255.0		Subnetzmaske des externen Datenverkehr-Subnetzes.
T3.	NetScaler-IP-Adresse	172.17.17.2		NetScaler IP-Adresse im Subnetz des externen Datenverkehrs.
T4.	Externe Signalisierungs-IP-Adresse	172.17.17.10		Der Datenverkehr zu dieser IP-Adresse wird zwischen den signalisierenden IP-Adressen der Beschleuniger Lastausgleich durchgeführt.
T5.	Externe WCCP IP-Adresse #1	172.17.17.11		Karten über NAT zu WCCP VIP auf Beschleuniger #1.
T6.	Externe WCCP IP-Adresse #2	172.17.17.12		Karten über NAT zu WCCP VIP auf Beschleuniger #2.

	Parameter	Beispiel	Ihr Wert	Beschreibung
T7.	Lokale LAN-Subnetze	10.200.0.0/16		Das lokale LAN-Subnetz, das beschleunigt werden soll. Dies ist das einzige Subnetz, das Beschleunigung erhält.
T8.	Host-ID des GRE-Routers	Nicht verfügbar		Nur WCCP-GRE. Host-ID des GRE-Routers.
T9.	Verkehrsport	10/1		Port, der für beschleunigten Datenverkehr verwendet wird.
T10+.	(Inline) mehr Traffic Port			Andere Verkehrsport paarweise.
T11, T12	(WCCP) Dienstgruppen: TCP, UDP	71, 72		Service-Gruppen, die vom Beschleuniger #1 für WCCP verwendet werden. Die erste ist für TCP-Datenverkehr, die zweite für UDP.
T13, T14	(Nicht verwendet)			
T15, T16	(Inline) Ports verwendet von link #2	10/5, 10/6		Wenn mehrere Links im Inlinemodus verwendet werden, werden diese Ports für den Link #2 verwendet.

	Parameter	Beispiel	Ihr Wert	Beschreibung
T17, T18	(Inline) Ports verwendet von link #3	10/7, 10/8		Wenn mehrere Links im Inlinemodus verwendet werden, werden diese Ports für den Link #3 verwendet.
VLAN1.1, VLAN1.2, VLAN1.3, VLAN1.4	Externe VLANs für Bridge #1	412		Wenn VLAN-Trunking verwendet wird, sind diese getaggt VLANs crossing bridge #1.
VLAN2.1, VLAN2.2, VLAN2.3, VLAN2.4				Wenn VLAN-Trunking verwendet wird, sind diese getaggt VLANs crossing bridge #2.
VLAN3.1, VLAN3.2, VLAN3.3, VLAN3.4	Externe VLANs für Bridge #1			Wenn VLAN-Trunking verwendet wird, sind diese getaggt VLANs crossing bridge #3.

## Konfigurieren der Appliance

April 19, 2021

Bevor Sie mit der Konfiguration der Appliance beginnen, müssen Sie die IP-Adresse des Verwaltungsdienstes in das Verwaltungsnetzwerk ändern, damit Sie über das Netzwerk auf die Appliance

zugreifen können. Sie können die Verwaltungs-IP-Adresse ändern, indem Sie einen Computer über den Ethernet-Port oder die serielle Konsole mit der Appliance verbinden.

## **Zuweisen einer Management-IP-Adresse über den Ethernet-Port**

April 19, 2021

Verwenden Sie das folgende Verfahren für die Erstkonfiguration jeder SD-WAN 1000- oder 2000-Appliance mit Windows Server. Das Verfahren führt die folgenden Aufgaben aus:

- Konfigurieren Sie die Appliance für die Verwendung auf Ihrer Site.
- Installieren Sie die Citrix Lizenz.
- Beschleunigung aktivieren.
- Traffic Shaping aktivieren (nur Inlinemodus).

Bei Inline-Bereitstellungen ist diese Konfiguration möglicherweise alles, was Sie benötigen, da die meisten Beschleunigungsfunktionen standardmäßig aktiviert sind und keine zusätzliche Konfiguration erfordern.

Wenn Sie die Appliance konfigurieren möchten, indem Sie sie über die serielle Konsole mit dem Computer verbinden, weisen Sie die IP-Adresse des Verwaltungsdienstes in Ihrem Arbeitsblatt zu, indem Sie das Verfahren [Zuweisen einer Management-IP-Adresse über die serielle Konsole](#) abschließen, und führen Sie dann Schritte 4 bis 15 des folgenden Verfahrens.

### **Hinweis:**

Sie müssen physischen Zugriff auf die Appliance haben.

## **So konfigurieren Sie die Appliance durch Anschließen eines Computers an den Ethernet-Port 0/1 der SD-WAN-Appliance**

1. Stellen Sie die Ethernet-Port-Adresse eines Computers (oder eines anderen Browsers mit einem Ethernet-Port) auf 192.168.100.50 mit einer Netzwerkmaske von 255.255.0.0 ein. Auf einem Windows-Gerät erfolgt dies durch Ändern der Eigenschaften des Internetprotokolls Version 4 der LAN-Verbindung, wie unten gezeigt. Sie können die Felder für Gateway und DNS-Server leer lassen.
2. Schließen Sie diesen Computer über ein Ethernet-Kabel an den Port mit der Bezeichnung PRI an der SD-WAN-Einheit an.
3. Schalten Sie die Appliance ein. Verwenden Sie den Webbrowser auf dem Computer, indem Sie die standardmäßige IP-Adresse des Verwaltungsdienstes verwenden <http://192.168.100.1>.

4. Verwenden Sie auf der Anmeldeseite die folgenden Standardanmeldeinformationen, um sich bei der Appliance anzumelden:
  - **Benutzername:**nsroot
  - **Kennwort:**nsroot
1. Starten Sie den Konfigurationsassistenten, indem Sie auf **Erste Schritte** klicken.
2. Geben Sie auf der Seite **Plattformkonfiguration** die entsprechenden Werte aus Ihrem Arbeitsblatt ein, wie im folgenden Beispiel gezeigt:
3. Klicken Sie auf **Fertig**. Es wird ein Bildschirm mit der Meldung Installation in Progress ...angezeigt. Dieser Vorgang dauert etwa 2 bis 5 Minuten, abhängig von der Netzwerkgeschwindigkeit.
4. Es wird eine Umleitung zu neuen Verwaltungs-IP-Meldung angezeigt.
5. Klicken Sie auf **OK**.
6. Trennen Sie den Computer vom Ethernet-Port, und verbinden Sie den Port mit dem Verwaltungsnetzwerk.
7. Setzen Sie die IP-Adresse Ihres Computers auf die vorherige Einstellung zurück.
8. Melden Sie sich von einem Computer im Verwaltungsnetzwerk an der Appliance an, indem Sie die neue IP-Adresse des Verwaltungsdienstes (z. B. [https://<Management\\_IP\\_Address>](https://<Management_IP_Address>)) in einem Webbrowser eingeben.
9. Um die Konfiguration fortzusetzen, akzeptieren Sie das Zertifikat und fahren Sie fort. Die Option zum Fortfahren variiert je nach verwendeter Webbrowser.
10. Melden Sie sich bei der Appliance an, indem Sie den Benutzernamen **nsroot** und das Kennwort von Ihrem verwenden-Arbeitsblatt .
11. Informationen zum Abschließen des Konfigurationsprozesses finden Sie unter [Provisioning der Appliance](#).

## Zuweisen einer Management-IP-Adresse über den seriellen Port

April 19, 2021

Wenn Sie die Einstellungen des Computers nicht ändern möchten, können Sie die Appliance konfigurieren, indem Sie sie mit einem seriellen Nullmodemkabel an Ihren Computer anschließen. Sie müssen physischen Zugriff auf die Appliance haben.

### So konfigurieren Sie die Appliance über die serielle Konsole

1. Schließen Sie ein serielles Nullmodemkabel an den Konsolenanschluss der Appliance an.

2. Schließen Sie das andere Ende des Kabels an den seriellen COM-Anschluss eines Computers an, auf dem ein Terminalemulator ausgeführt wird, z. B. Microsoft HyperTerminal, mit den Einstellungen 9600, N, 8,1, p.
3. Drücken Sie in der HyperTerminal-Ausgabe die **Eingabetaste**. Auf dem Terminalbildschirm wird die Anmeldeaufforderung angezeigt. **Hinweis:** Je nach verwendetem Terminalprogramm müssen Sie möglicherweise zwei oder drei Mal die **Eingabetaste** drücken.
4. Melden Sie sich an der Anmeldeaufforderung an der Appliance mit den folgenden Standardanmeldeinformationen an:
  - **Benutzername:** nsroot
  - **Kennwort:** nsroot
1. Führen Sie an der Eingabeaufforderung **\$** den folgenden Befehl aus, um zur Shell-Eingabeaufforderung der Appliance zu wechseln: `$ ssh 169.254.0.10`
2. Geben Sie **Ja** ein, um die Verbindung mit dem Verwaltungsdienst fortzusetzen.
3. Melden Sie sich an der Shell-Eingabeaufforderung der Appliance mit den folgenden Standardanmeldeinformationen an:
  - Kennwort:** nsroot.
4. Führen Sie an der Anmeldeaufforderung den folgenden Befehl aus, um das Menü “Konfiguration der anfänglichen Netzwerkadressen des Verwaltungsdienstes” zu öffnen: `# networkconfig`
5. **Geben Sie 1 ein und drücken Sie die Eingabetaste**, um Option 1 auszuwählen, und geben Sie eine neue Verwaltungs-IP-Adresse für den Verwaltungsdienst an.
6. Geben Sie **2** ein und drücken Sie die **Eingabetaste**, um Option 2 auszuwählen, und geben Sie eine neue IP-Adresse für die Citrix Hypervisor an.
7. Geben Sie **3** ein und drücken Sie die **Eingabetaste**, um Option 3 auszuwählen, und geben Sie die Netzwerkmaske für die IP-Adressen an.
8. **Geben Sie 4 ein und drücken Sie die Eingabetaste**, um Option 4 auszuwählen, und geben Sie das Standard-Gateway für die IP-Adresse des Verwaltungsdienstes an.
9. Geben Sie **8** ein und drücken Sie die **Eingabetaste**, um die Einstellungen zu speichern und zu beenden.
10. Greifen Sie auf die SD-WAN-Appliance zu, indem Sie die neue Verwaltungsdienst-IP-Adresse der Appliance eingeben, z. B. `https://<Management_Service_IP_Address>` in einem Webbrowser eines Computers im Verwaltungsnetzwerk.
11. Um die Konfiguration fortzusetzen, akzeptieren Sie das Zertifikat und fahren Sie fort. Die Option zum Fortfahren variiert je nach verwendeter Webbrowser.
12. Informationen zum Abschließen des Konfigurationsprozesses finden Sie unter [Provisioning der Appliance](#).

## Provisioning der Appliance

April 19, 2021

Nachdem Sie dem Verwaltungsdienst eine IP-Adresse zugewiesen haben, können Sie die NetScaler er- und Accelerator-Instanzen bereitstellen. Wenn Sie sich bei der Appliance anmelden, wird der Konfigurationsassistent angezeigt.

Beachten Sie bei der Verwendung des Konfigurationsassistenten die folgenden Punkte:

- Bei der folgenden Prozedur wird davon ausgegangen, dass Sie das Konfigurationsarbeitsblatt bereits ausgefüllt haben.
- Wenn Sie die IP-Adressen des Verwaltungsnetzwerks ändern oder das Standardgateway in eine Adresse ändern, die nicht im Verwaltungsnetzwerk ist, verlieren Sie die Konnektivität mit der Appliance, wenn Sie sich nicht im selben Ethernet-Segment wie der Verwaltungsport befinden.
- Wenn Sie den Konfigurationsassistenten verwenden, überprüfen Sie Ihre Einträge sorgfältig. Der Assistent hat keine Schaltfläche Zurück. Wenn Sie den vorherigen Bildschirm ändern müssen, verwenden Sie die Schaltfläche **Zurück** in Ihrem Browser. Dadurch gelangen Sie zur Anmeldeseite und dann zum vorherigen Bildschirm.
- Der Konfigurationsassistent wird nur angezeigt, wenn Sie sich zum ersten Mal bei der Appliance anmelden, um die Appliance zu konfigurieren. Nachdem Sie die Konfiguration der Appliance abgeschlossen haben, wird der Zugriff auf diesen Assistenten nicht mehr möglich und wird erst nach einem Zurücksetzen auf die Werkseinstellungen angezeigt. Überprüfen Sie Ihre Eingaben sorgfältig.

Dieser Assistent führt Sie durch eine neue Konfiguration der Appliance.

### Notiz:

Wenn während dieser Prozeduren jederzeit ein Fehler #SESS\_CORRUPTED angezeigt wird, klicken Sie auf

**Abmelden**, löschen Sie Ihren Browsercache, schließen Sie Ihren Browser, und öffnen Sie ihn erneut.

So konfigurieren Sie die Appliance mithilfe des Konfigurationsassistenten:

1. Klicken Sie auf der Willkommenseite auf **Erste Schritte**.

### Hinweis:

Alle Seiten nach der Seite Erste Schritte haben eine Überschrift mit dem Titel Bereitstellungsmodus: Inline/L2-Modus, aber dieser Assistent wird für alle Bereitstellungsmodi verwendet.

2. Gehen Sie folgendermaßen vor, um ein vollständig 7.3-kompatibles System zu konfigurieren:

- Erwerben Sie die folgenden Software-Distributionen Version 7.3 von der Downloadseite von Release 7.3 auf My Citrix:
    - Verwaltungsdienst (als TGZ-Datei)
    - NetScaler VM (als XVA-Datei)
    - Accelerator-VM (als XVA-Datei)
    - Upgrade-Paket (als UPG-Datei)
  - Navigieren Sie zur Seite **System > Konfiguration > Management Service > Software-Images**, und wählen Sie **Upload** aus der Aktionsliste aus.
  - Laden Sie ein Release 7.3 Management Service-Image hoch (verteilt als TGZ-Datei).
  - Navigieren Sie zur Seite **System > Konfiguration > NetScaler\ > Software-Images**, und laden Sie dann ein NetScaler XVA-Image der Version 7.3 hoch.
  - Navigieren Sie zur Seite **System > Konfiguration > SD-WAN > Software-Images**, und laden Sie das Accelerator XVA-Image hoch.
  - Navigieren Sie zur Seite **System > Konfiguration > Verwaltungsdienst**, und klicken Sie dann auf den Link **Upgrade Management Service**.
  - Wählen Sie das kürzlich hochgeladene Management Service-Image aus, und klicken Sie auf **OK**.
  - Wenn in der unteren linken Ecke des Bildschirms Management Service erfolgreich aktualisiert angezeigt wird, melden Sie sich ab und löschen Sie den Browsercache. Melden Sie sich nach dem Neustart des Verwaltungsdienstes an (einige Minuten).
  - Klicken Sie auf der **Willkommenseite** auf **Erste Schritte**.
3. Geben Sie unter Verwaltungszugriffseinstellungen Werte für die verschiedenen Felder entsprechend den Netzwerkeinstellungen an. Im folgenden Screenshot werden Beispielwerte angezeigt, die in dieser Dokumentation verwendet werden. Geben Sie Werte wie folgt ein:
- **Citrix Hypervisor IP-Adresse:**(Element M4 im Arbeitsblättern oder H4, wenn dies das zweite Gerät in einem Hochverfügbarkeitspaar ist.) Die Verwaltungsadresse der integrierten Citrix Hypervisor. Dies muss eine gültige Adresse im Verwaltungsnetzwerk sein.
  - **Verwaltungsdienst-IP-Adresse**—(Element M5 auf Ihrem Arbeitsblatt oder H5, wenn es sich um die zweite Appliance in einem Paar mit hoher Verfügbarkeit handelt). Die Adresse der Verwaltungsdienst-VM, die Sie zum Ausführen der meisten Systemverwaltungsaufgaben verwenden. Dies muss eine gültige Adresse im Verwaltungsnetzwerk sein.
  - **Netzmaske**—(Artikel M3 auf Ihrem Arbeitsblatt). Die Subnetzmaske des Verwaltungsnetzwerks.
  - **Gateway**—(Element M2 auf Ihrem Arbeitsblatt). Das Standardgateway für das Verwaltungsnetzwerk.
  - **DNS-Server:** Die IP-Adresse des DNS-Servers. Dies ist ein obligatorischer Parameter.



- **NTP-Server**—IP- oder FQDN-Adresse Ihres Zeitervers. Dies wird von allen virtuellen Maschinen in der Appliance verwendet. > **Beachten** Sie, dass bei Verwendung der erweiterten CIFS- oder MAPI-Beschleunigung die Systemzeit der Appliance in der Nähe der des Windows-Domänenservers liegen muss. Wählen Sie daher einen NTP-Server aus, der eine enge Beziehung zur Zeit auf Ihrem Windows aufrechterhält. -Domänenserver.

**Hinweis:**

Wenn der NTP-Server nicht als IP-Adresse angegeben ist, wird er vom Beschleuniger nicht verwendet.

- **Zeitzone**—Wählen Sie Ihre Zeitzone aus dem Pulldownmenü aus.
- **Kennwort ändern**—Aktivieren Sie dieses Kontrollkästchen, und geben Sie zweimal ein neues nsroot-Kennwort ein, um das Kennwort zu ändern. Dasselbe Kennwort wird für den Verwaltungsdienst und die NetScaler Instanz für das Konto nsroot und für den Accelerator für das Administratorkonto verwendet. Wenn das Kennwort nicht geändert wird, bleibt es auf nsroot (Standardeinstellung) festgelegt.

Abbildung 1. Beispielwerte für die Seite Felder in Verwaltungszugriffseinstellungen der Konfiguration

4. Überprüfen Sie Ihre Einstellungen und klicken Sie auf **Weiter**.
  5. Sehen Sie im Abschnitt **Lizenzen verwalten**, ob bereits eine entsprechende Lizenz im Feld **Name** aufgeführt ist. Wenn ja, wählen Sie es aus und fahren Sie mit Schritt 8 fort.
  6. Klicken Sie im Abschnitt **Lizenzen aktualisieren** auf **Hochladen**.
  7. Navigieren Sie zu dem Ordner, der die Lizenzdatei enthält, und öffnen Sie die Datei.
  8. Klicken Sie auf **Lizenz hinzufügen**, und laden Sie die von Citrix bereitgestellte Lizenzdatei hoch. Die Lizenz wird der Appliance hinzugefügt, wie in der folgenden Abbildung dargestellt.
- Abbildung 2. Beispiellizenz zur Appliance auf der Seite Lizenzdateien verwalten des Konfigurations-Assistenten hinzugefügt

Sie können auch eine Lizenzdatei von der Citrix.com Website abrufen, indem Sie auf die Schaltfläche **hier** Link und verwenden Sie Ihre My Citrix Anmeldeinformationen.

9. Wählen Sie die Lizenz im Feld **Name** aus, und klicken Sie auf **Weiter**. Die Seite SD-WAN-Setup wird angezeigt. Füllen Sie die Felder wie folgt aus:
  - a) **Netzwerkeinstellungen**—In diesem Abschnitt werden die Beschleuniger des Verwaltungsnetzwerks informiert.
    - **SD-WAN Accelerator IP Address**—Geben Sie den Wert von M6 aus Ihrem Arbeitsblatt ein. Dies ist die IP-Adresse des Accelerators

- **NetScaler IP-Adresse**—Geben Sie den Wert von M7 aus dem Arbeitsblatt ein. Dies ist die IP-Adresse der NetScaler GUI.
- **Systemnetzmaske und Gateway verwenden**—Wählen Sie diese Option, wenn Sie die Netzwerkmaske und die Gateway-IP-Adressen verwenden möchten, die Sie auf der Seite Plattformkonfiguration angegeben haben.
- **Netmask**—Geben Sie den Wert von M3 aus dem Arbeitsblatt ein. Dies ist die Subnetzmaske (Netzmaske) des Verwaltungsnetzwerks (beachten Sie, dass Sie dies bereits auf einer vorherigen Seite eingegeben haben).
- **Gateway**—Geben Sie den Wert von M2 aus dem Arbeitsblatt erneut ein.
- **IP-Adresse signalisieren**—Geben Sie den Wert von T4 aus dem Arbeitsblatt ein. Dies ist die externe Signalisierungs-IP-Adresse des Beschleunigers, die von SD-WAN-Plug-Ins für die Verbindung mit der Appliance verwendet wird.
- **Signaling Netmask (Signaling Netmask)** —Geben Sie den Wert von T2 aus dem Arbeitsblatt ein. Dies ist die Subnetzmaske (Netzmaske) des externen Verkehrsnetzwerks.

- b) **XVA-Dateien**—In diesem Abschnitt können Sie zuvor hochgeladene XVA-Dateien (virtuelle Xen Maschinen) für die NetScaler er- und Accelerator-Instanzen angeben. Wählen Sie die XVA-Images aus, die Sie im Rahmen von Schritt 2 hochgeladen haben.

Abbildung 3. Seite SD-WAN-Setup

10. Klicken Sie auf **Weiter**. Der Assistent beginnt mit dem Provisioning der erforderlichen Instanzen, wie in der folgenden Abbildung dargestellt.

Abbildung 4. Fortschrittsindikator für das Provisioning

11. Fügen Sie nach der Bereitstellung der Instanzen eines Ihrer lokalen LAN-Subnetze zum Abschnitt **Verbindungskonfiguration** aus der Liste T7 in Ihrem Arbeitsblatt hinzu, wie in der folgenden Abbildung dargestellt. Dieses Subnetz wird im Accelerator als lokales LAN-Subnetz hinzugefügt. Wenn Sie mehr als ein LAN-Subnetz haben, können Sie diese nach Abschluss des Konfigurationsassistenten der **LAN-Link-Definition** in der Accelerator-GUI hinzufügen. Klicken Sie auf **Hinzufügen**, um das Subnetz hinzuzufügen.

Abbildung 5. Die Linkkonfiguration befindet sich am Ende dieser Seite

12. Melden Sie sich ab, und melden Sie sich wieder an. Wenn die Meldung Versionsinkompatibilität erkannt angezeigt wird, installieren Sie das Upgrade-Paket, das Sie in Schritt 2 heruntergeladen haben.

Die Grundkonfiguration ist abgeschlossen. Führen Sie als Nächstes die Bereitstellungsmodusspezifische Konfiguration durch (z. B. für den WCCP-Modus).

**Notiz:**

Nach Abschluss des Assistenten wird die Appliance für die Basisinstallation konfiguriert. Informationen zum Konfigurieren der Appliance für ein bestimmtes Bereitstellungsszenario finden Sie unter [Bereitstellungsmodi](#).

## Bereitstellungsmodi

April 19, 2021

Eine SD-WAN-Appliance fungiert als virtuelles Gateway. Es ist weder ein TCP-Endpunkt noch ein Router. Wie jedes Gateway besteht seine Aufgabe darin, eingehende Pakete zu puffern und sie mit der richtigen Geschwindigkeit auf den ausgehenden Link zu legen. Diese Paketweiterleitung kann auf verschiedene Arten erfolgen, z. B. im Inlinemodus, im virtuellen Inlinemodus und im WCCP-Modus. Obwohl diese Methoden *Modi* genannt werden, müssen Sie keinen Weiterleitungsmodus deaktivieren, um einen anderen zu aktivieren. Wenn Ihre Bereitstellung mehr als einen Modus unterstützt, wird der Modus, den die Appliance verwendet, automatisch durch das Ethernet- und IP-Format jedes Pakets bestimmt.

Da die Appliance verschiedene Weiterleitungsmodi und verschiedene Arten von nicht weitergeleiteten Verbindungen unterstützt, muss sie eine Art von Datenverkehr von einer anderen unterscheiden. Dies geschieht, indem die Ziel-IP-Adresse und die Ziel-Ethernet-Adresse (MAC-Adresse) untersucht werden, wie in der folgenden Tabelle gezeigt. Im Inlinemodus fungiert die Appliance beispielsweise als Brücke. Im Gegensatz zu anderen Datenverkehr werden überbrückte Pakete an ein System außerhalb der Appliance adressiert, nicht an die Appliance selbst. Die Adressfelder enthalten weder die IP-Adresse der Appliance noch die Ethernet-MAC-Adresse der Appliance.

Zusätzlich zu den reinen Weiterleitungsmodi muss die Appliance zusätzliche Verbindungstypen berücksichtigen, einschließlich Management-Verbindungen zur GUI und das Heartbeat-Signal, das zwischen Mitgliedern eines Hochverfügbarkeitspaares verläuft. Der Vollständigkeit halber sind diese zusätzlichen Verkehrsmodi auch in der nachstehenden Tabelle aufgeführt.

**Tabelle 1. Wie Ethernet- und IP-Adressen den Modus bestimmen**

Ziel-IP-Adresse	Ziel-Ethernet-Adresse	Modus
Keine Appliance	Keine Appliance	Inline oder Pass-Through

Ziel-IP-Adresse	Ziel-Ethernet-Adresse	Modus
Keine Appliance	Gerät	Virtual Inline oder L2 WCCP
Gerät	Gerät	Direkt (UI-Zugriff)
Gerät (VIP)	Gerät	Hohe Verfügbarkeit. Proxy-Modus
Appliance (WCCP GRE-Paket)	Gerät	WCCP GRE-Modus
Appliance (Signalisierungs-IP)	Gerät	Signalverbindung (SD-WAN-Plugin Signalverbindung (SD-WAN-Plugin, Secure Peer) oder Redirector Mode Verbindung (SD-WAN-Plugin)

Alle Modi können gleichzeitig aktiv sein. Der für ein gegebenes Paket verwendete Modus wird durch die Ethernet- und IP-Header bestimmt.

Die Weiterleitungsmodi sind:

- **Inlinemodus**, in dem die Appliance den Datenverkehr zwischen den beiden Ethernet-Ports transparent beschleunigt. In diesem Modus wird die Appliance (für den Rest des Netzwerks) als Ethernet-Bridge angezeigt. Der Inlinemodus wird empfohlen, da er die geringste Konfiguration erfordert.
- **WCCP-Modus**, der das Protokoll WCCP v. 2.0 verwendet, um mit dem Router zu kommunizieren. Dieser Modus ist auf den meisten Routern einfach zu konfigurieren. WCCP hat zwei Varianten: WCCP-GRE und WCCP-L2. WCCP-GRE kapselt den WCCP-Datenverkehr in GRE-Tunneln (Generic Routing Encapsulation). WCCP-L2 verwendet nicht gekapselten Netzwerk-Layer 2 (Ethernet) - Transport.
- **Virtueller Inlinemodus**, in dem ein Router WAN-Datenverkehr an die Appliance sendet und die Appliance an den Router zurückgibt. In diesem Modus scheint die Appliance ein Router zu sein, verwendet jedoch keine Routingtabellen. Es sendet den Rückkehrverkehr an den echten Router. Der virtuelle Inlinemodus wird empfohlen, wenn der Inlinemodus und der Hochgeschwindigkeits-WCCP-Betrieb nicht praktikabel sind.
- **Gruppenmodus**, mit dem zwei Appliances zusammenarbeiten können, um ein Paar von weit getrennten WAN-Verbindungen zu beschleunigen.
- **Hochverfügbarkeitsmodus**, mit dem Appliances als aktives/Standby-Hochverfügbarkeitspaar betrieben werden können. Wenn die primäre Appliance ausfällt, übernimmt die sekundäre Appliance.

Zusätzliche Traffic-Typen sind hier der Vollständigkeit halber aufgeführt:

- **Pass-Through-Datenverkehr** bezieht sich auf jeden Datenverkehr, den die Appliance nicht beschleunigt. Es ist eine Verkehrskategorie, kein Weiterleitungsmodus.
- **Direkter Zugriff**, bei dem die Appliance als gewöhnlicher Server oder Client fungiert. Die GUI und CLI sind Beispiele für den direkten Zugriff unter Verwendung der Protokolle HTTP, HTTPS, SSH oder SFTP. Der Direktzugriffsverkehr kann auch die Protokolle NTP- und SNMP umfassen.
- **Appliance-zu-Appliance-Kommunikation**, die Signalverbindungen (verwendet in Secure Peering und durch das SD-WAN-Plugin), VRRP-Heartbeats (im Hochverfügbarkeitsmodus) und verschlüsselte GRE-Tunnel (im Gruppenmodus verwendet) umfassen kann.
- **Veraltete Modi.** Proxy-Modus und Redirector-Modus sind Legacy-Weiterleitungsmodi, die in neuen Installationen nicht verwendet werden sollten.

SD-WAN 4100/5100 Appliances verfügen über zwei empfohlene Bereitstellungsmodi: WCCP und Inline. Diese Modi werden häufig ohne hohe Verfügbarkeit (hohe Verfügbarkeit) und seltener mit hoher Verfügbarkeit verwendet.

Derzeit empfiehlt Citrix den WCCP-Modus mit einem einzelnen Router und ohne hohe Verfügbarkeit für die meisten Bereitstellungen. Verwenden Sie den Inlinemodus, wenn WCCP nicht verfügbar ist.

Obwohl derzeit nicht alle der folgenden Modi empfohlen werden, werden sie alle unterstützt:

- WCCP-Modus mit einem einzelnen Router
- WCCP-Modus mit einem einzelnen Router und hoher Verfügbarkeit
- Kaskade von zwei oder mehr Appliances im WCCP-Modus zusammen mit einer NetScaler MPX Appliance
- Kaskade von zwei oder mehr Appliances im WCCP-Modus zusammen mit einer NetScaler MPX Appliance in hoher Verfügbarkeit
- Inlinemodus
- Inlinemodus bei hoher Verfügbarkeit
- Virtueller Inlinemodus
- Virtueller Inlinemodus in hoher Verfügbarkeit

#### Hinweis

Während andere Modi als WCCP und Inline unterstützt werden, sind sie nicht vollständig dokumentiert und werden für typische Installationen nicht empfohlen. Wenden Sie sich an Ihren Citrix Vertreter, wenn Sie einen dieser Modi in Betracht ziehen.

## Anpassen der Ethernet-Ports

April 19, 2021

Eine typische Appliance verfügt über vier Ethernet-Ports: zwei beschleunigte Bridged-Ports, die als *beschleunigtes Paar A* (APA.1 und APA.2) bezeichnet werden, mit einem Bypass (Fail-to-Wire-Relay) und zwei nicht beschleunigte Motherboard-Ports, die Primär und Aux1 genannt werden. Die überbrückten Ports sorgen für Beschleunigung, während die Motherboard-Ports manchmal für sekundäre Zwecke verwendet werden. Die meisten Installationen verwenden nur die überbrückten Ports.

Einige SD-WAN-Geräte haben nur die Motherboard-Ports. In diesem Fall werden die beiden Motherboard-Ports überbrückt.

Auf die Benutzeroberfläche der Appliance kann über ein VLAN- oder Nicht-VLAN-Netzwerk zugegriffen werden. Sie können ein VLAN zu Verwaltungszwecken jedem der überbrückten Ports oder Motherboard-Ports der Appliance zuweisen.

Abbildung 1. Ethernet-Ports

**Portliste**

Die Ports sind wie folgt benannt:

Ethernet-Anschluss	Name
Hauptplatinenanschluss 1	Primär (oder APA.1, wenn keine Bypasskarte vorhanden ist)
Hauptplatinenanschluss 2	Auxiliary1 oder Aux1 (oder APA.2, wenn keine Bypasskarte vorhanden ist)
Brücke #1	Beschleunigtes Paar A (APA, mit Ports APA.1 und APA.2)
Brücke #2	Beschleunigtes Paar B (aPb, mit Ports aB.1 und apB.2)

Tabelle 1. Ethernet-Portnamen

**Port-Parameter**

April 19, 2021

Jeder Bridge- und Motherboard-Anschluss kann sein:

- Aktiviert oder deaktiviert
- Zugewiesen einer IP-Adresse und einer Subnetzmaske

- Zugewiesen eines Standardgateway
- Einem VLAN zugewiesen
- Festlegen auf 1000 Mbps, 100 Mbps oder 10 Mbps
- Auf Vollduplex, Halbduplex oder Auto eingestellt (bei SD-WAN WANOP 4000/5000 Appliances können einige Ports auf 10 Gbit/s eingestellt werden)

Alle diese Parameter außer der Geschwindigkeit/Duplexeinstellung werden auf der Seite Konfiguration: IP-Adresse festgelegt. Die Geschwindigkeit/Duplexeinstellungen werden auf der Seite Konfiguration: Schnittstelle festgelegt.

#### **Hinweis** zu Parametern:

- Deaktivierte Ports reagieren auf keinen Datenverkehr.
- Die browserbasierte Benutzeroberfläche kann unabhängig von allen Ports aktiviert oder deaktiviert werden.
- Um die Benutzeroberfläche auf Ports mit IP-Adressen zu sichern, wählen Sie HTTPS anstelle von HTTP auf der Seite Konfiguration: Administratorschnittstelle: Web Access.
- Der Inlinemodus funktioniert auch dann, wenn eine Bridge keine IP-Adresse hat. Alle anderen Modi erfordern, dass dem Port eine IP-Adresse zugewiesen wird.
- Datenverkehr wird nicht zwischen Schnittstellen weitergeleitet. Beispielsweise wird eine Verbindung auf Bridge-APA nicht mit den Primäre- oder Aux1-Ports überquert, sondern auf Bridge-APA verbleibt. Alle Routing-Probleme werden Ihren Routern überlassen.

## **Beschleunigte Brücken (APA und aPb)**

April 19, 2021

Jede Appliance verfügt über mindestens ein Paar Ethernet-Ports, die als beschleunigte Brücke fungieren, genannt *APA* (für *beschleunigtes Paar A*). Eine Brücke kann im *\*Inlinemodus\** fungieren, der als transparente Brücke fungiert, als wäre es ein Ethernet-Switch. Pakete fließen in einem Port und aus dem anderen. Bridges können auch in einem *\*Arm-Modus\** agieren, in dem Pakete in einem Port fließen und denselben Port zurückkehren.

Eine Appliance, die über eine Bypasskarte verfügt, behält die Netzwerkkontinuität bei Fehlfunktionen einer Bridge oder Appliance aufrecht.

Einige Einheiten haben mehr als ein beschleunigtes Paar, und diese zusätzlichen beschleunigten Paare heißen aPb, aPC usw.

## **Bypass-Karte**

Wenn das Gerät Strom verliert oder auf andere Weise ausfällt, wird ein internes Relais geschlossen und die beiden überbrückten Ports sind elektrisch angeschlossen. Diese Verbindung behält die Netzwerkcontinuität bei, macht aber nicht auf die Bridge-Ports zugegriffen. Daher sollten Sie einen der Motherboard-Ports für den Verwaltungszugriff verwenden.

Achtung: Aktivieren Sie den primären Port nicht, wenn er nicht mit Ihrem Netzwerk verbunden ist. Andernfalls können Sie nicht auf die Appliance zugreifen, wie unter

[Ethernet-Bypass und Link-Down-Propagierung](#)

Bypass-Karten sind bei einigen Modellen standardmäßig und bei anderen optional. Citrix empfiehlt den Kauf von Appliances mit Bypasskarten für alle Inline-Bereitstellungen.

Die Bypass-Funktion ist so verdrahtet, als würde ein Cross-Over-Kabel die beiden Ports verbinden, was das korrekte Verhalten bei ordnungsgemäß verkabelten Installationen darstellt.

Wichtig: Bypass-Installationen müssen getestet werden - Unsachgemäße Verkabelung kann im normalen Betrieb funktionieren, aber nicht im Bypass-Modus. Die Ethernet-Ports sind tolerant gegen unsachgemäße Verkabelung und passen sich oft geräuschlos an. Der Bypass-Modus ist fest verdrahtet und hat keine solche Anpassungsfähigkeit. Testen Sie Inline-Installationen mit ausgeschaltetem Gerät, um sicherzustellen, dass die Verkabelung für den Bypass-Modus korrekt ist.

## **Verwenden mehrerer Brücken**

Wenn die Appliance mit zwei beschleunigten Brücken ausgestattet ist, können sie verwendet werden, um zwei verschiedene Verbindungen zu beschleunigen. Diese Links können entweder vollständig unabhängig sein, oder sie können redundante Links sein, die mit derselben Site verbinden. Redundante Links können entweder Lastenausgleich sein oder als Haupt- und Failoverlink verwendet werden.

Abbildung 1. Verwenden von Doppelbrücken

Wenn es an der Zeit ist, dass die Appliance ein Paket für eine bestimmte Verbindung sendet, wird das Paket über dieselbe Brücke gesendet, von der die Appliance das letzte Eingabepaket für diese Verbindung empfangen hat. Somit berücksichtigt die Appliance die vom Router getroffenen Verbindungsentscheidungen und verfolgt automatisch den vorherrschenden Lastausgleich oder den Main-Link-/Failover-Link-Algorithmus in Echtzeit. Bei Verbindungen ohne Lastenausgleich stellt der letztere Algorithmus sicher, dass Pakete immer die richtige Brücke verwenden.

## **WCCP und Virtual Inline Modi**

Mehrere Bridges werden sowohl im WCCP-Modus als auch im virtuellen Inlinemodus unterstützt. Die Verwendung ist dieselbe wie im Single-Bridge-Fall, mit der Ausnahme, dass WCCP die zusätzliche Ein-



schränkung hat, dass der gesamte Datenverkehr für eine bestimmte WCCP-Dienstgruppe auf derselben Brücke ankommen muss.

## **Hohe Verfügbarkeit mit mehreren Brücken**

Zwei Einheiten mit mehreren Brücken können in einem Hochverfügbarkeitspaar verwendet werden. Passen Sie einfach die Brücken an, so dass alle Links durch beide Appliances gehen.

## **Motherboard-Anschlüsse**

April 19, 2021

Obwohl die Ethernet-Ports einer Bypass-Karte nicht zugänglich sind, wenn das Bypass-Relais geschlossen wird, bleiben die Motherboard-Ports aktiv. Manchmal können Sie über die Motherboard-Ports auf eine ausgefallene Appliance zugreifen, wenn nicht auf die überbrückten Ports zugegriffen werden kann.

### **Der primäre Port**

Wenn der primäre Port aktiviert ist und ihm eine IP-Adresse zugewiesen ist, verwendet die Appliance diese IP-Adresse, um sich mit anderen Beschleunigungseinheiten zu identifizieren. Diese Adresse wird intern für eine Vielzahl von Zwecken verwendet und ist für Benutzer am meisten als Feld Partner Unit auf der Seite Überwachung: Optimierung: Verbindungen sichtbar. Wenn kein Motherboard-Port aktiviert ist, verwendet die Appliance die IP-Adresse von Accelerated Pair A.

Der primäre Port wird verwendet für:

- Administration über die webbasierte Benutzeroberfläche
- Ein Rückkanal für den Gruppenmodus
- Ein Rückkanal für Hochverfügbarkeitsmodus

### **Der Aux1-Anschluss**

Der Aux1-Anschluss ist identisch mit dem Primary Port. Wenn der Aux1-Port aktiviert ist und der primäre Port nicht ist, übernimmt die Appliance ihre Identität von der IP-Adresse des Aux1-Ports. Wenn beide aktiviert sind, ist die IP-Adresse des primären Ports die Identität der Einheit

## VLAN-Unterstützung

April 19, 2021

Ein Virtual Local Area Network (VLAN) verwendet einen Teil des Ethernet-Headers, um anzugeben, zu welchem virtuellen Netzwerk ein bestimmter Ethernet-Frame gehört. SD-WAN-Appliances unterstützen VLAN-Trunking in allen Weiterleitungsmodi (Inline, WCCP, Virtual Inline und Gruppen-Modus). Der Datenverkehr mit einer beliebigen Kombination von VLAN-Tags wird korrekt gehandhabt und beschleunigt.

Wenn beispielsweise ein Datenverkehr, der durch die beschleunigte Brücke führt, an 10.0.0.1, VLAN 100 adressiert und ein anderer an 10.0.0.1, VLAN 111 adressiert wird, weiß die Appliance, dass es sich um zwei unterschiedliche Ziele handelt, obwohl die beiden VLANs dieselbe IP-Adresse haben.

Sie können allen Ethernet-Ports der Appliance, einigen oder keinem der Ethernet-Ports ein VLAN zuweisen. Wenn einem Port ein VLAN zugewiesen ist, hören die Management-Schnittstellen (GUI und CLI) nur den Datenverkehr auf diesem VLAN ab. Wenn kein VLAN zugewiesen ist, hören die Verwaltungsschnittstellen nur Datenverkehr ohne VLAN ab. Diese Auswahl erfolgt auf der Registerkarte Konfiguration: Einheiteneinstellungen: Netzwerkadapter: IP-Adressen.

## Anpassen der Ethernet-Ports

April 19, 2021

Eine typische Appliance verfügt über vier Ethernet-Ports: zwei beschleunigte Bridged-Ports, die als *beschleunigtes Paar A* (APA.1 und APA.2) bezeichnet werden, mit einem Bypass (Fail-to-Wire-Relay) und zwei nicht beschleunigte Motherboard-Ports, die Primär und Aux1 genannt werden. Die überbrückten Ports sorgen für Beschleunigung, während die Motherboard-Ports manchmal für sekundäre Zwecke verwendet werden. Die meisten Installationen verwenden nur die überbrückten Ports.

Einige SD-WAN-Geräte haben nur die Motherboard-Ports. In diesem Fall werden die beiden Motherboard-Ports überbrückt.

Auf die Benutzeroberfläche der Appliance kann über ein VLAN- oder Nicht-VLAN-Netzwerk zugegriffen werden. Sie können ein VLAN zu Verwaltungszwecken jedem der überbrückten Ports oder Motherboard-Ports der Appliance zuweisen.

Abbildung 1. Ethernet-Ports

## Portliste

Die Ports sind wie folgt benannt:

Ethernet-Anschluss	Name
Hauptplatinenanschluss 1	Primär (oder APA.1, wenn keine Bypasskarte vorhanden ist)
Hauptplatinenanschluss 2	Auxiliary1 oder Aux1 (oder APA.2, wenn keine Bypasskarte vorhanden ist)
Brücke #1	Beschleunigtes Paar A (APA, mit Ports APA.1 und APA.2)
Brücke #2	Beschleunigtes Paar B (aPb, mit Ports aB.1 und apB.2)

Tabelle 1. Ethernet-Portnamen

## Ethernet-Bypass und Link-Down-Propagierung

April 19, 2021

Hinweis: Die Link-Down-Propagierung wurde den SD-WAN (früher SD-WAN) 1000, 2000, 3000, 4000 und 5000 Appliances mit 7.2.1 hinzugefügt.

Die meisten Appliance-Modelle verfügen über eine Fail-to-Wire (Ethernet-Bypass) -Funktion für den Inlinemodus. Wenn die Stromversorgung ausfällt, wird ein Relais geschlossen und die Eingangs- und Ausgangsanschlüsse werden elektrisch angeschlossen, sodass das Ethernet-Signal von einem Port zum anderen durchlaufen kann, als ob das Gerät nicht da wäre. Im Fail-to-Wire-Modus sieht die Appliance wie ein Cross-Over-Kabel aus, das die beiden Ports verbindet.

Bei einem Ausfall der Hardware oder Software der Appliance wird das Relay ebenfalls geschlossen. Wenn die Appliance neu gestartet wird, bleibt das Bypass-Relay geschlossen, bis die Appliance vollständig initialisiert ist, wodurch die Netzwerkkontinuität jederzeit aufrechterhalten wird. Diese Funktion ist automatisch und erfordert keine Benutzerkonfiguration.

Wenn das Bypass-Relais geschlossen ist, ist der Zugriff auf die Brückenanschlüsse der Appliance nicht möglich.

Wenn der Träger an einem der Bridge-Ports verloren geht, wird der Carrier am anderen Bridge-Anschluss abgelegt, um sicherzustellen, dass die Verbindungsbedingung auf das Gerät auf der

anderen Seite der Appliance übertragen wird. Einheiten, die den Verbindungsstatus überwachen (z. B. Router), werden daher über Bedingungen auf der anderen Seite der Brücke benachrichtigt.

Die Link-Down-Propagierung verfügt über zwei Betriebsmodi:

- Wenn der primäre Port nicht aktiviert ist, wird der Verknüpfungsstatus eines Bridge-Ports kurz auf dem anderen Bridge-Port gespiegelt, und dann wird der Port wieder aktiviert. Auf diese Weise kann die Appliance über den noch verbundenen Port für Verwaltung, Hochverfügbarkeits-Heartbeat und andere Aufgaben erreicht werden.
- Wenn der primäre Port aktiviert ist, geht die Appliance davon aus (ohne zu überprüfen), dass der primäre Port für die Verwaltung, Hochverfügbarkeits-Heartbeat und andere Aufgaben verwendet wird. Die Verbindungsbedingung eines Bridge-Ports wird dauerhaft auf dem anderen Port gespiegelt, bis der Träger wiederhergestellt oder das Gerät neu gestartet wird. Dies gilt auch dann, wenn der primäre Port in der GUI aktiviert ist, aber nicht mit einem Netzwerk verbunden ist. Daher sollte der primäre Port deaktiviert werden (Standardeinstellung), wenn er nicht verwendet wird.

## Beschleunigen einer gesamten Site

April 19, 2021

[Inlinemodus, Beschleunigung des gesamten Datenverkehrs auf einem WAN](#) zeigt eine typische Konfiguration für den Inlinemodus an. Bei beiden Standorten werden die Appliances zwischen dem LAN und dem WAN platziert, sodass der gesamte WAN-Datenverkehr beschleunigt wird, beschleunigt wird. Dies ist die einfachste Methode zur Implementierung von Beschleunigung, und es sollte verwendet werden, wenn es praktisch ist.

Da der gesamte Link-Verkehr durch die Appliances fließt, verhindern die Vorteile von Fair Queuing und Flow Control eine Überschreitung der Verbindung.

In IP-Netzwerken bestimmt das Engpassgateway das Warteschlangenverhalten für die gesamte Verbindung. Indem sie zum Engpassgateway wird, erhält die Appliance die Kontrolle über die Verbindung und kann sie intelligent verwalten. Dies geschieht, indem die Bandbreitengrenze etwas niedriger als die Verbindungsgeschwindigkeit eingestellt wird. Wenn dies getan wird, ist die Linkperformance ideal, mit minimaler Latenz und Verlust selbst bei voller Linkauslastung.

## Teilstandbeschleunigung

April 19, 2021

Um die beschleunigte Bandbreite der Appliance für eine bestimmte Gruppe von Systemen zu reservieren, z. B. für Remote-Sicherungsserver, können Sie die Appliance in einem Zweignetzwerk installieren, das nur diese Systeme umfasst. Dies ist in der folgenden Abbildung dargestellt.

Abbildung 1. Inlinemodus, nur ausgewählte Systeme beschleunigen

Die Gestaltung des SD-WAN-Datenverkehrs basiert auf der Steuerung der gesamten Verbindung. Daher ist die Traffic Shaping mit dieser Topologie nicht wirksam, da die Appliance nur einen Teil des Link-Datenverkehrs erkennt. Die Latenzkontrolle ist bis zum Engpass Gateway, und die interaktive Reaktionsfähigkeit kann beeinträchtigt werden.

## WCCP-Modus

April 19, 2021

Web Cache Communication Protocol (WCCP) ist ein dynamisches Routing-Protokoll, das von Cisco eingeführt wurde. Ursprünglich nur für das Web-Caching gedacht, wurde WCCP Version 2 zu einem allgemeineren Protokoll, das für die Verwendung durch Beschleuniger wie Citrix SD-WAN Appliances geeignet ist.

Der WCCP-Modus ist die einfachste Möglichkeit, eine SD-WAN-Appliance zu installieren, wenn der Inline-Betrieb unpraktisch ist. Es ist auch nützlich, wenn asymmetrisches Routing auftritt, das heißt, wenn Pakete aus derselben Verbindung über verschiedene WAN-Verbindungen ankommen. Im WCCP-Modus verwenden die Router das WCCP 2.0-Protokoll, um den Datenverkehr über die Appliance umzuleiten. Sobald die Appliance empfangen hat, wird der Datenverkehr von der Beschleunigungsmaschine und dem Traffic Shaper so behandelt, als ob er im Inlinemodus empfangen würde.

### Hinweis

- Für die Zwecke dieser Diskussion gilt WCCP Version 1 als veraltet und nur WCCP Version 2 wird vorgestellt.
- Die Standard-WCCP-Dokumentation ruft WCCP-Clients Caches auf. Um Verwechslungen mit tatsächlichen Caches zu vermeiden, vermeidet Citrix im Allgemeinen den Aufruf eines WCCP-Clients als Cache. Stattdessen werden WCCP-Clients in der Regel als Appliances bezeichnet.
- Diese Diskussion verwendet den Begriff Router, um WCCP-fähige Router und WCCP-fähige Switches anzuzeigen. Obwohl hier der Begriff Router verwendet wird, unterstützen einige High-End-Switches auch WCCP und können mit SD-WAN-Appliances verwendet werden.

Die SD-WAN-Appliances unterstützen zwei WCCP-Modi:

- WCCP ist das Original SD-WAN WCCP, das seit Release 3.x unterstützt wird. Es unterstützt eine einzelne Appliance-Dienstgruppe (kein Clustering).
- WCCP-Clustering, eingeführt in Version 7.2, ermöglicht Ihrem Router den Lastausgleich zwischen mehreren Appliances.

## **Funktionsweise des WCCP-Modus**

Der physische Modus für die WCCP-Bereitstellung eines SD-WAN-Geräts ist einarmigen Modus, in dem das Gerät direkt mit einem dedizierten Port auf dem WAN-Router verbunden ist. Der WCCP-Standard umfasst eine Protokollverhandlung, bei der sich die Appliance beim Router registriert und die beiden gemeinsam unterstützten Funktionen aushandeln. Sobald diese Verhandlung erfolgreich ist, wird der Datenverkehr zwischen dem Router und der Appliance gemäß dem WCCP-Router und den Umleitungsregeln, die auf dem Router definiert sind, weitergeleitet.

Eine WCCP-Modus-Appliance benötigt nur einen einzigen Ethernet-Port. Das Gerät muss entweder auf einem dedizierten Routerport (oder einem WCCP-fähigen Switchport) bereitgestellt werden oder von anderen Datenverkehr über ein VLAN isoliert sein. Mischen Sie den Inlinemodus und den WCCP-Modus nicht.

Die folgende Abbildung zeigt, wie ein Router so konfiguriert ist, dass Datenverkehr auf ausgewählten Schnittstellen abgefangen und an die WCCP-fähige Appliance weitergeleitet wird. Wenn die WCCP-fähige Appliance nicht verfügbar ist, wird der Datenverkehr nicht abgefangen und normal weitergeleitet.

Abbildung 1. WCCP-Datenfluss

## **Datenverkehrskapselung**

WCCP ermöglicht die Weiterleitung von Datenverkehr zwischen dem Router und der Appliance in einem der folgenden Modi:

- L2-Modus —Erfordert, dass sich Router und Appliance auf demselben L2-Segment befinden (typischerweise ein Ethernet-Segment). Das IP-Paket ist unverändert, und nur die L2-Adressierung wird geändert, um das Paket weiterzuleiten. In vielen Geräten wird die L2-Weiterleitung auf der Hardwareschicht durchgeführt, was ihm die maximale Leistung verleiht. Aufgrund seines Leistungsvorteils ist die L2-Weiterleitung der bevorzugte Modus, aber nicht alle WCCP-fähigen Geräte unterstützen ihn.
- GRE-Modus: Generisches Routing-Gekapselung (GRE) ist ein geroutetes Protokoll, und das Gerät kann theoretisch überall platziert werden. Aus Leistungsgründen muss es jedoch in der Nähe des Routers platziert werden, auf einem schnellen, nicht ausgelasteten Pfad, der so wenige Switches und Router wie möglich durchquert. GRE ist der ursprüngliche WCCP-Modus.

Ein GRE-Header wird erstellt und das Datenpaket wird an ihn angehängt. Das empfangende Gerät entfernt den GRE-Header. Bei der Verkapselung kann sich die Appliance in einem Subnetz befinden, das nicht direkt an den Router angeschlossen ist. Sowohl der Kapselungsprozess als auch das anschließende Routing fügen dem Router jedoch CPU-Overhead hinzu, und das Hinzufügen des 28-Byte-GRE-Headers kann zu Paketfragmentierung führen, was zusätzlichen Overhead hinzufügt.

Der WCCP-Modus unterstützt mehrere Router und sowohl GRE vs. L2-Weiterleitung. Jeder Router kann mehrere WAN-Verbindungen haben. Jeder Link kann eine eigene WCCP-Dienstgruppe haben.

Traffic Shaping ist nur wirksam, wenn die Appliance sowohl UDP-Datenverkehr als auch TCP-Datenverkehr verwaltet. Eine zweite Dienstgruppe mit einer UDP-Dienstgruppe für jede WAN-Verbindung wird empfohlen, wenn Traffic Shaping gewünscht ist.

## **Registrierung und Statusaktualisierungen**

Ein WCCP-Client (ein Gerät) verwendet UDP-Port 2048, um sich beim Router zu registrieren und auszuhandeln, welcher Datenverkehr an ihn gesendet werden muss und welche WCCP-Features für diesen Datenverkehr verwendet werden sollen. Die Appliance arbeitet mit diesem Datenverkehr und leitet den resultierenden Datenverkehr an den ursprünglichen Endpunkt weiter. Der Status einer Appliance wird durch den WCCP-Registrierungsprozess und ein Heartbeat-Protokoll verfolgt. Die Appliance kontaktiert den Router zuerst über den WCCP-Steuerkanal (UDP-Port 2048), und die Einheit und der Router tauschen Informationen mit Paketen mit den Namen Here\_I\_Am bzw. I\_See\_You aus. Standardmäßig wird dieser Vorgang alle 10 Sekunden wiederholt. Wenn der Router für drei dieser Intervalle keine Nachricht von der Appliance empfängt, hält er die Appliance für ausgefallen, und beendet die Weiterleitung des Datenverkehrs an sie, bis der Kontakt wieder hergestellt wird.

## **Services und Servicegruppen**

Verschiedene Appliances, die denselben Router verwenden, können verschiedene Dienste bereitstellen. Um zu verfolgen, welche Dienste welchen Appliances zugewiesen sind, verwendet das WCCP-Protokoll eine Service-Gruppen-ID, eine Ganzzahl von 1 Byte. Wenn sich eine Appliance bei einem Router registriert, enthält sie auch Servicegruppennummern.

- Eine einzelne Appliance kann mehr als eine Servicegruppe unterstützen.
- Ein einzelner Router kann mehr als eine Servicegruppe unterstützen.
- Eine einzelne Appliance kann dieselbe Servicegruppe mit mehr als einem Router verwenden.
- Ein einzelner Router kann dieselbe Servicegruppe mit mehr als einer Appliance verwenden. Für SD-WAN-Appliances werden mehrere Appliances im WCCP-Clustermodus unterstützt, und eine einzelne Appliance wird im WCCP-Modus unterstützt.

- Jede Appliance gibt einen Rückgabebetyp (L2 oder GRE) unabhängig für jede Richtung und jede Servicegruppe an. SD-WAN 4000/5000 Geräte geben immer denselben Rückgabebetyp für beide Richtungen an. Bei anderen SD-WAN-Appliances kann der Rückgabebetyp unterschiedlich sein.

Abbildung 2. Verwenden verschiedener WCCP-Dienstgruppen für verschiedene Dienste

**Mehrere Dienstgruppen** können mit WCCP auf derselben Appliance verwendet werden. Beispielsweise kann die Appliance Servicegruppe 51-Datenverkehr von einer WAN-Verbindung und Servicegruppe 62-Datenverkehr von einer anderen WAN-Verbindung empfangen. Die Appliance unterstützt auch mehrere Router. Es ist gleichgültig, ob alle Router dieselbe Servicegruppe verwenden oder verschiedene Router unterschiedliche Servicegruppen verwenden.

**Servicegruppenverfolgung.** Wenn ein Paket in einer Servicegruppe eintrifft, werden Ausgabepakete für dieselbe Verbindung für dieselbe Servicegruppe gesendet. Wenn Pakete für dieselbe Verbindung in mehreren Dienstgruppen ankommen, verfolgen Ausgabepakete die zuletzt gesehene Dienstgruppe für diese Verbindung.

## Hochverfügbarkeitsverhalten

Wenn WCCP im Hochverfügbarkeitsmodus verwendet wird, sendet die primäre Appliance eine eigene APA- oder APB-Verwaltungs-IP-Adresse, nicht die virtuelle Adresse des Hochverfügbarkeitspaars, wenn sie den Router kontaktiert. Wenn ein Failover auftritt, kontaktiert die neue primäre Appliance automatisch den Router und stellt den WCCP-Kanal wieder her. In den meisten Fällen überschneiden sich der WCCP-Zeitüberschreitungszeitraum und die Hochverfügbarkeits-Failover-Zeit. Infolgedessen ist der Netzerkausfall kleiner als die Summe der beiden Verzögerungen.

Standard-WCCP erlaubt nur eine einzelne Appliance in einer WCCP-Dienstgruppe. Wenn eine neue Appliance versucht, den Router zu kontaktieren, wird festgestellt, dass die andere Appliance die Servicegruppe verarbeitet, und die neue Appliance legt eine Warnung fest. Es überprüft regelmäßig, ob die Servicegruppe mit der anderen Appliance noch aktiv ist, und die neue Appliance verarbeitet die Servicegruppe, wenn die andere Appliance inaktiv wird. WCCP-Clustering ermöglicht mehrere Appliances pro Servicegruppe.

## Bereitstellungstopologie

Die folgende Abbildung zeigt eine einfache WCCP-Bereitstellung, die entweder für L2 oder GRE geeignet ist. Der Verkehrsanschluss (1/1) ist direkt an einen dedizierten Routerport (Gig 4/12) angeschlossen.

Abbildung 3. Einfache WCCP-Bereitstellung



In diesem Beispiel wird das SD-WAN 4000/5000 im Einarmmodus bereitgestellt, wobei der Verkehrsanschluss (1/1) und der Verwaltungsport (0/1) jeweils mit einem eigenen dedizierten Routerport verbunden ist.

Auf dem Router ist WCCP mit identischer IP-WCCP-Umleitung in Anweisungen auf den WAN- und LAN-Ports konfiguriert. Es werden zwei Service-Gruppen verwendet, 71 und 72. Die Dienstgruppe 71 wird für den TCP-Datenverkehr verwendet und die Dienstgruppe 72 wird für den UDP-Datenverkehr verwendet. Die Appliance beschleunigt den UDP-Datenverkehr nicht, kann aber Traffic Shaping-Richtlinien anwenden.

**Hinweis:** Die WCCP-Spezifikation erlaubt keine anderen Protokolle als TCP und UDP weitergeleitet werden, so dass Protokolle wie ICMP und GRE die Appliance immer umgehen.

## WCCP-Clustering

SD-WAN-Appliances unterstützen WCCP-Clustering, wodurch Ihr Router den Datenverkehr zwischen mehreren Appliances ausgleichen kann. Weitere Hinweise zum Bereitstellen von SD-WAN-Appliances als Cluster finden Sie unter [WCCP-Clustering](#).

## WCCP-Spezifikation

Weitere Informationen zu WCCP finden Sie unter Web Cache Communication Protocol V2, Revision 1, <http://tools.ietf.org/html/draft-mclaggan-wccp-v2rev1-00>.

### Hinweis

Bei der Bereitstellung von SD-WAN in WCCP für Switch-Redundanz können wir Switch 2 mit aPb verbinden. Erstellen Sie eine andere SG für aPb, geben Sie ihm eine niedrigere Priorität als die SG für APA. Wenn APA höher SG ist, wird dies für die Umleitung verwendet. Ist dies nicht möglich, wird aPb SG verwendet. ApA und apB müssen sich in verschiedenen Subnetzen befinden.

## WCCP-Modus (nicht gruppiert)

April 19, 2021

Der WCCP-Modus erlaubt nur eine einzelne Appliance in einer WCCP-Dienstgruppe. Wenn eine neue Appliance versucht, den Router zu kontaktieren, wird festgestellt, dass die andere Appliance die Servicegruppe verarbeitet, und die neue Appliance legt eine Warnung fest. Es überprüft regelmäßig, ob die Servicegruppe mit der anderen Appliance noch aktiv ist, und die neue Appliance verarbeitet die Servicegruppe, wenn die andere Appliance inaktiv wird.

**Hinweis:** WCCP-Clustering ermöglicht mehrere Appliances pro Service-Gruppe.

## Einschränkungen und Best Practices

Im Folgenden sind Einschränkungen und Best Practices für den (nicht gruppierten) WCCP-Modus aufgeführt:

- Bei Appliances mit mehr als einem beschleunigten Paar muss der gesamte Datenverkehr für eine bestimmte WCCP-Dienstgruppe auf demselben beschleunigten Paar ankommen.
- Vermischen Sie den Inline- und WCCP-Datenverkehr auf derselben Appliance nicht. Die Appliance erzwingt diese Richtlinie nicht, kann jedoch zu Schwierigkeiten bei der Beschleunigung führen. (WCCP und virtuelle Inlinemodi können gemischt werden, aber nur, wenn der WCCP und der virtuelle Inline-Datenverkehr von verschiedenen Routern stammen.)
- Verwenden Sie für Sites mit einem einzelnen WAN-Router WCCP, wenn der Inlinemodus nicht praktisch ist.
- Pro Servicegruppe wird nur eine Appliance unterstützt. Wenn mehrere Appliances versuchen, eine Verbindung mit demselben Router mit derselben Servicegruppe herzustellen, ist die Aushandlung nur für die erste Appliance erfolgreich.
- Bei Standorten mit mehreren WAN-Routern, die von derselben Appliance bedient werden, kann WCCP verwendet werden, um einen, einige oder alle Ihre WAN-Router zu unterstützen. Andere Router können den virtuellen Inlinemodus verwenden.

## Router-Unterstützung für WCCP

Die Konfiguration des Routers für WCCP ist sehr einfach. Die Unterstützung von WCCP Version 2 ist in allen modernen Routern enthalten, die Cisco IOS bei Release 12.0 (11) S und 12.1 (3) T hinzugefügt wurden. Die beste Router-Konfigurationsstrategie hängt von den Eigenschaften Ihres Routers und Switches ab. Traffic Shaping erfordert zwei Service-Gruppen.

Wenn Ihr Router Reverse Path Forwarding unterstützt, müssen Sie es auf allen Ports deaktivieren, da es WCCP-Datenverkehr mit gefälschtem Datenverkehr verwechseln kann. Diese Funktion wird in neueren Cisco Routern wie dem Cisco 7600 gefunden.

## Router-Konfigurationsstrategien

Es gibt zwei grundlegende Ansätze zum Umleiten von Datenverkehr vom Router zur Appliance:

**Nur auf dem WAN-Port:** Fügen Sie eine Anweisung "WCCP Redirect in" und eine Anweisung "WCCP Redirect out" hinzu.

**Jedem Port des Routers hinzufügen, außer dem an die Appliance angeschlossenen Port**, fügen Sie eine Anweisung “WCCP redirect in” hinzu.

Die erste Methode leitet nur WAN-Datenverkehr an die Appliance weiter, während die zweite Methode den gesamten Routerverkehr an die Appliance weiterleitet, unabhängig davon, ob es sich um WAN-bezogene oder nicht. Auf einem Router mit mehreren LAN-Ports und erheblichem LAN-zu-LAN-Datenverkehr kann das Senden des gesamten Datenverkehrs an die Appliance sein LAN-Segment überladen und die Appliance mit dieser unnötigen Last belasten. Wenn GRE verwendet wird, kann der unnötige Datenverkehr auch den Router herunterladen.

Bei einigen Routern ist der Redirect in -Pfad schneller und belastet die CPU des Routers weniger als der Redirect Out -Pfad. Falls erforderlich, kann dies durch direkte Experimente auf Ihrem Router ermittelt werden: Testen Sie beide Umleitungsmethoden unter voller Netzwerklast, um zu sehen, welche die höchsten Übertragungsraten liefert.

Einige Router und WCCP-fähige Switches unterstützen WCCP-Umleitung nicht, daher muss die zweite Methode verwendet werden. Um eine Überlastung des Routers zu vermeiden, empfiehlt es sich, eine große Anzahl von Router-Ports über die Appliance umzuleiten, vielleicht durch Verwendung von zwei Routern, einen für WAN-Routing und einen für LAN-zu-LAN-Routing.

Im Allgemeinen ist Methode 1 einfacher, während Methode 2 eine höhere Leistung bieten kann.

### **Traffic Shaping und WCCP**

Eine Dienstgruppe kann entweder TCP oder UDP sein, aber nicht beides. Damit der Traffic Shaper wirksam ist, müssen beide Arten von WAN-Datenverkehr durch die Appliance geleitet werden. Daher:

Die Beschleunigung erfordert eine Servicegruppe für TCP-Datenverkehr.

Traffic Shaping erfordert zwei Dienstgruppen, eine für TCP-Datenverkehr und eine für UDP-Datenverkehr. Der Unterschied zwischen den beiden ist auf der Appliance konfiguriert, und der Router akzeptiert diese Konfiguration.

### **Konfigurieren des Routers**

Die Appliance verhandelt automatisch WCCP-GRE oder WCCP-L2. Die Hauptwahl besteht zwischen dem *Unicast-Vorgang* (bei dem die Appliance mit der IP-Adresse jedes Routers konfiguriert ist) oder dem *Multicast-Vorgang* (bei dem sowohl die Appliance als auch die Router mit der Multicast-Adresse konfiguriert sind).

**Normal (Unicast) -Operation:** Für den normalen Betrieb wird WCCP Version 2 und die WCCP-Gruppen-ID für den Router als Ganzes deklariert und dann die Umleitung für jede WAN-Schnittstelle aktiviert. Es folgt ein Cisco IOS Beispiel:

```
1 config term
2 ip wccp version 2
3 ! We will configure the appliance to use group 51 for TCP and 52 for
  UDP.
4 ip wccp 51
5 ip wccp 52
6
7 ! Repeat the following three lines for each WAN interface
8 ! you wish to accelerate:
9 interface your_wan_interface
10 ! If Reverse Path Forwarding is enabled (with an ip verify unicast
11 ! source reachable " statement), delete or comment out the statement:
12 ! ip verify unicast source reachable-via any
13 ! Repeat on all ports.
14
15 ip wccp 51 redirect out
16 ip wccp 51 redirect in
17 ip wccp 52 redirect out
18 ip wccp 52 redirect in
19
20 ! If the appliance is inline with one of the router interfaces
21 ! (NOT SUPPORTED), add the following line for that interface
22 ! to prevent loops:
23 ip wccp redirect exclude in
24 ^Z
25 <!--NeedCopy-->
```

Wenn mehrere Router dieselbe Appliance verwenden sollen, wird jeder wie oben dargestellt konfiguriert, wobei entweder dieselben oder unterschiedliche Servicegruppen verwendet werden.

**Multicastbetrieb**—Wenn der Appliance und jedem Router eine Multicastadresse zugewiesen wird, unterscheidet sich die Konfiguration geringfügig von der für den normalen Betrieb. Es folgt ein Cisco IOS Beispiel:

```
1 config term
2 ip wccp version 2
3 ip wccp 51 group-address 225.0.0.1
4
5 ! Repeat the following three lines for each WAN interface
6 ! you wish to accelerate:
7 interface your_wan_interface
8 ! If Reverse Path Forwarding is enabled (with an ip verify unicast
9 ! source reachable " statement), delete or comment out the statement:
10 ! ip verify unicast source reachable-via any
11
12 ip wccp 51 redirect out
13 ip wccp 51 redirect in
14 !
15 ! The following line is needed only on the interface facing the other
   router,
16 ! if there is another router participating in this service group.
17 ip wccp 51 group-listen
```

```
18
19 !If the appliance is inline with one of the router interfaces,
20 !(which is supported but not recommended), add
21 !the following line for that interface to prevent loops:
22 ip wccp redirect exclude in
23 ^Z
24 <!--NeedCopy-->
```

## Grundlegende Konfigurationsprozedur für den WCCP-Modus auf der SD-WAN-Appliance

Für die meisten Standorte können Sie das folgende Verfahren verwenden, um den WCCP-Modus auf der Appliance zu konfigurieren. Die Prozedur hat mehrere Parameter auf sinnvolle Standardwerte gesetzt. Erweiterte Bereitstellungen erfordern möglicherweise, dass Sie diese Parameter auf andere Werte festlegen. Wenn beispielsweise die WCCP-Dienstgruppe 51 bereits von Ihrem Router verwendet wird, müssen Sie einen anderen Wert für die Appliance verwenden.

So konfigurieren Sie den WCCP-Modus auf der Appliance:

1. Auf der Seite Konfiguration: Appliance-Einstellungen: WCCP.
2. Wenn keine Servicegruppen definiert wurden, wird die Seite Modus auswählen angezeigt. Die Optionen sind Single SD-WAN und Cluster (Mehrere SD-WANs). Wählen Sie Single SD-WAN aus. Sie werden zur WCCP-Seite weitergeleitet.  
Hinweis: Die Modusbeschriftungen sind irreführend. Der Modus Single SD-WAN wird auch für SD-WAN-Hochverfügbarkeitspaare verwendet.
3. Wenn der WCCP-Modus nicht aktiviert ist, klicken Sie auf **Aktivieren**.
4. Klicken Sie auf **Dienstgruppe hinzufügen**.
5. Die Werte für Standardschnittstelle (APA), Protokoll (TCP), WCCP-Priorität (0), Router-Kommunikation (Unicast), (Kennwort leer) und Time to Live (1) müssen normalerweise nicht für die erste von Ihnen erstellte Servicegruppe geändert werden, aber wenn dies der Fall ist, geben Sie neue Werte in die bereitgestellten Felder ein.
6. Geben Sie im Feld **Routeradressierung** (wenn Sie Unicast verwenden) oder im Feld **Multicastadresse** (wenn Sie Multicast verwenden) die IP-Adresse des Routers ein. Verwenden Sie die IP für den Routerport, der für die WCCP-Kommunikation mit der Appliance verwendet wird.
7. Wenn mehr als ein Router WCCP für die Kommunikation mit dieser Appliance verwendet, fügen Sie jetzt weitere Router hinzu.
8. Wenn Ihre Router spezielle Anforderungen haben, legen Sie die Felder Routerweiterleitung (Auto/GRE/Level-2), Routerpaketrückkehr (Auto/GRE/Level-2) und Routerzuweisung (Mask/Hash) entsprechend fest. Die Standardwerte liefern bei den meisten Routern optimale Ergebnisse.
9. Klicken Sie auf **Hinzufügen**.

10. Wiederholen Sie die vorherigen Schritte, um eine andere Dienstgruppe für UDP-Datenverkehr zu erstellen (z. B. Dienstgruppen-ID 52 und Protokoll UDP).
11. Rufen Sie die Seite Überwachung: Appliance-Leistung: WCCP auf. Das Feld **Status** sollte innerhalb von 60 Sekunden in Verbunden geändert werden.
12. Senden Sie Datenverkehr über den Link und überprüfen Sie auf der Seite Verbindungen, ob Verbindungen eintreffen und beschleunigt werden.

## WCCP-Dienstgruppen-Konfigurationsdetails

In einer Servicegruppe verhandeln ein WCCP-Router und eine SD-WAN-Appliance ("WCCP-Cache" in WCCP-Terminologie) Kommunikationsattribute (Funktionen). Der Router wirbt seine Fähigkeiten in der Nachricht Ich sehe dich an. Die Kommunikationsattribute sind:

- Weiterleitungsmethode: GRE oder Level-2
- Paketrückgabemethode (nur Multicast): GRE oder Level-2
- Zuweisungsmethode: Hash oder Maske
- Kennwort (Standardwert ist none)

Die Appliance löst eine Warnung aus, wenn sie eine Inkompatibilität zwischen ihren Attributen und denen des Routers erkennt. Die Appliance ist möglicherweise aufgrund eines bestimmten Attributs einer Servicegruppe (z. B. GRE oder Level-2) nicht kompatibel. Seltener kann in einer Multicastdienstgruppe eine Warnung ausgelöst werden, wenn die Auswahl Auto ein bestimmtes Attribut mit einem bestimmten Router auswählt, aber das Attribut ist mit einem nachfolgenden Router nicht kompatibel.

Im Folgenden sind die grundlegenden Regeln für die Kommunikationsattribute innerhalb einer SD-WAN-Appliance aufgeführt.

Für Router-Weiterleitung:

- Wenn Auto ausgewählt ist, ist die Voreinstellung für Level-2, da sie sowohl für Router als auch für Appliance effizienter ist. Level-2 wird ausgehandelt, wenn der Router es unterstützt und sich der Router im selben Subnetz wie die Appliance befindet.
- Router in einer Unicast-Service-Gruppe können verschiedene Methoden aushandeln, wenn Auto ausgewählt ist.
- Router in einer Multicastdienstgruppe müssen alle dieselbe Methode verwenden, unabhängig davon, ob sie mit GRE oder Level-2 oder mit Auto erzwungen wird, wie vom ersten Router in der Servicegruppe festgelegt wird.
- Für eine Inkompatibilität gibt eine Warnung bekannt, dass der Router eine inkompatible Routerweiterleitung hat.

Für Router-Zuweisung:

- Der Standardwert ist Hash.
- Wenn Auto ausgewählt ist, wird der Modus mit dem Router ausgehandelt.
- Alle Router in einer Servicegruppe müssen dieselbe Zuweisungsmethode (Hash oder Maske) unterstützen.
- Wenn dieses Attribut für jede Servicegruppe als Auto konfiguriert ist, wählt die Appliance Hash oder Maske, wenn der erste Router angeschlossen ist. Hash wird gewählt, wenn der Router es unterstützt. Andernfalls ist Maske ausgewählt. Das Problem, dass nachfolgende Router nicht mit der automatisch ausgewählten Methode kompatibel sind, kann minimiert werden, indem manuell eine Methode ausgewählt wird, die allen Routern in der Servicegruppe gemeinsam ist.
- Für eine Inkompatibilität gibt eine Warnung bekannt, dass der Router eine inkompatible Router-Zuweisungsmethode hat.
- Bei beiden Methoden weist die einzelne Appliance in der Dienstgruppe alle Router in der Dienstgruppe an, alle TCP- oder UDP-Pakete an die Appliance zu leiten. Router können dieses Verhalten mit Zugriffslisten ändern oder indem sie auswählen, welche Schnittstellen an die Dienstgruppe weitergeleitet werden sollen.

Bei der Mask-Methode verhandelt die Appliance die Maske Quell-IP-Adresse. Die Appliance bietet keinen Mechanismus zur Auswahl der Ziel-IP-Adresse oder der Ports für Quelle oder Ziel. Die Maske Quell-IP-Adresse identifiziert keine spezifische IP-Adresse oder einen bestimmten Bereich. Das Protokoll bietet keine Möglichkeit, eine bestimmte IP-Adresse anzugeben. Da in der Dienstgruppe nur eine einzelne Appliance vorhanden ist, wird standardmäßig eine Ein-Bit-Maske verwendet, um Routerressourcen zu sparen. (Release 6.0 verwendet eine größere Maske.)

Für Kennwort:

- Wenn der Router ein Kennwort benötigt, muss das auf der Appliance definierte Kennwort übereinstimmen. Wenn der Router kein Kennwort benötigt, muss das Kennwortfeld auf der Appliance leer sein.

## WCCP-Tests und Fehlerbehebung

Wenn Sie mit WCCP arbeiten, bietet die Appliance verschiedene Möglichkeiten, den Status der WCCP-Schnittstelle zu überwachen, und Ihr Router sollte auch Informationen bereitstellen.

**Überwachung: Appliance-Leistung: Seite WCCP**—Die Seite WCCP meldet den aktuellen Status des WCCP-Links und meldet die meisten Probleme.

**Protokolleinträge**—Auf der Seite Überwachung: Appliance-Leistung: Protokollierung wird jedes Mal ein neuer Eintrag angezeigt, wenn der WCCP-Modus eingerichtet oder verloren geht.

Abbildung 1. WCCP-Protokolleinträge (Format variiert je nach Veröffentlichung etwas)

**Router-Status**—Auf dem Router zeigt der Befehl `show ip wccp` den Status des WCCP-Links an:

```

1 Router>enable
2 Password:
3 Router#show ip wccp
4 Global WCCP information:
5     Router information:
6         Router Identifier:          172.16.2.4
7         Protocol Version:          2.0
8
9     Service Identifier: 51
10        Number of Cache Engines:    0
11        Number of routers:          0
12        Total Packets Redirected:    19951
13        Redirect access-list:        -none-
14        Total Packets Denied Redirect: 0
15        Total Packets Unassigned:    0
16        Group access-list:           -none-
17        Total Messages Denied to Group: 0
18        Total Authentication failures: 0
19 <!--NeedCopy-->

```

## WCCP-Modus überprüfen

Sie können die WCCP-Konfiguration über die SD-WAN-GUI überwachen.

So überwachen Sie die WCCP-Konfiguration

1. Navigieren Sie zur Seite **Überwachung > Applianceleistung > WCCP**.
2. Wählen Sie einen Cache aus und klicken Sie auf **Informationen abrufen**. Auf der Seite Cache-Status wird die WCCP-Konfiguration angezeigt, wie in der folgenden Abbildung dargestellt.
3. Starten Sie den Datenverkehr, der über die SD-WAN-Appliance weitergeleitet werden soll, und überwachen Sie die Verbindung auf der Seite **Überwachung > Optimierung > Verbindungen**.
  - Wenn die Verbindungen auf der Registerkarte **Beschleunigte Verbindungen** angezeigt werden, ist dies ein Indikator dafür, dass alles funktioniert.
  - Wenn sich die Verbindungen auf der Registerkarte **Nicht beschleunigte Verbindungen** befinden, sehen Sie sich die Spalte **Details** an. Eine Routingasymmetrie erkannte Nachricht impliziert, dass eine der IP-WCCP-Umleitungslinien auf dem Router fehlt oder einen Fehler aufweist oder dass unterschiedliche Pfade vom Client-Server- und Server-Client-Datenverkehr übernommen werden.
  - Wenn keine Verbindungen angezeigt werden, aber die Appliance meldet, dass sie mit dem Router verbunden ist und auf der WCCP-Überwachungsseite keine Fehler angezeigt wird, liegt das Problem wahrscheinlich bei der Routerkonfiguration.



## WCCP-Clustering

December 14, 2022

Mit der WCCP-Clustering-Funktion können Sie Ihre Beschleunigungskapazität multiplizieren, indem Sie denselben Links mehr als eine SD-WAN-Appliance zuweisen. Sie können bis zu 32 identische Appliances mit einer bis zu 32-fachen Kapazität clustern. Da es den WCCP 2.0-Standard verwendet, funktioniert WCCP-Clustering auf den meisten Routern und einigen Smart-Switches, höchstwahrscheinlich einschließlich der bereits verwendeten.

Da es ein dezentrales Protokoll verwendet, ermöglicht WCCP-Clustering das Hinzufügen oder Entfernen von SD-WAN-Appliances nach Bedarf. Wenn eine Appliance ausfällt, wird ihr Datenverkehr an die verbleibenden Appliances weitergeleitet.

Im Gegensatz zu SD-WAN-Hochverfügbarkeit, einem aktiv/passiven Paar, das zwei Appliances verwendet, um die Leistung einer einzelnen Appliance zu gewährleisten, haben dieselben Appliances, die wie ein WCCP-Cluster bereitgestellt werden, doppelt so viel Leistung wie eine einzelne Appliance, was sowohl Redundanz als auch eine verbesserte Leistung bietet.

Zusätzlich zum Hinzufügen weiterer Appliances, wenn die Anforderungen Ihrer Site steigen, können Sie die Citrix Funktion Pay as You Grow nutzen, um die Funktionen Ihrer Appliances durch Lizenzaktualisierungen zu erhöhen.

Citrix **Command Center** wird für die Verwaltung von WCCP-Clustern empfohlen. Die folgende Abbildung zeigt ein Basisnetzwerk eines Clusters von SD-WAN-Appliances im WCCP-Modus, das mithilfe von Citrix Command Center verwaltet wird.

Abbildung 1. Mit Citrix Command Center verwaltete SD-WAN-Cluster

### WCCP-Cluster mit Lastenausgleich

Das WCCP-Protokoll unterstützt bis zu 32 Appliances in einem fehlertoleranten Lastenausgleichsarray, das als Cluster bezeichnet wird. Im folgenden Beispiel sind drei identische Appliances (dasselbe Modell, dieselbe Softwareversion) identisch verkabelt und mit Ausnahme ihrer IP-Adressen identisch konfiguriert. Appliances, die dieselben Servicegruppen mit demselben Router verwenden, können zu einem Lastenausgleich WCCP-Cluster werden. Wenn sich eine neue Appliance beim Router registriert, kann sie dem vorhandenen Appliance-Pool beitreten und ihren Anteil am Datenverkehr erhalten. Wenn eine Appliance das Netzwerk verlässt (wie durch das Fehlen von Heartbeat-Signalen angezeigt), wird der Cluster neu ausbalanciert, sodass nur die verbleibenden Appliances verwendet werden.

Abbildung 2. Ein Lastenausgleich WCCP-Cluster mit drei Appliances

Eine Appliance im Cluster wird als zugewiesener Cache ausgewählt und steuert das Lastenausgleichsverhalten der Appliances im Cluster. Der angegebene Cache ist die Appliance mit der niedrigsten

IP-Adresse. Da die Appliances identische Konfigurationen aufweisen, spielt es keine Rolle, welche der angegebene Cache ist. Wenn der aktuell angegebene Cache offline geschaltet wird, wird eine andere Appliance zum angegebenen Cache.

Der zugewiesene Cache bestimmt, wie der Lastenausgleich Datenverkehr zugewiesen wird, und informiert den Router über diese Entscheidungen. Der Router teilt Informationen mit allen Mitgliedern des Clusters, sodass der Cluster auch dann betrieben werden kann, wenn der angegebene Cache offline geschaltet wird.

**Hinweis:** Wie üblich konfiguriert wird, wird eine SD-WAN 4000/5000 Appliance als zwei WCCP-Caches auf dem Router angezeigt.

## Lastenausgleichsalgorithmus

Der Lastenausgleich in WCCP ist statisch, außer wenn eine Appliance den Cluster betritt oder verlässt, wodurch der Cluster unter den aktuellen Mitgliedern neu ausbalanciert wird.

Der WCCP-Standard unterstützt den Lastenausgleich basierend auf einer Maske oder einem Hash. Beispielsweise verwendet die SD-WAN-WCCP-Clustering nur die Maskenmethode, wobei eine Maske von 1-6 Bits der 32-Bit-IP-Adresse verwendet wird. Diese Adressbits können nicht aufeinanderfolgend sein. Alle Adressen, die dasselbe Ergebnis ergeben, wenn maskiert wird, werden an dieselbe Appliance gesendet. Die Wirksamkeit des Lastenausgleichs hängt von der Auswahl eines geeigneten Maskenwerts ab: Eine schlechte Maskenauswahl kann zu einem schlechten Lastenausgleich führen oder gar keinem, wobei der gesamte Datenverkehr an eine einzelne Appliance gesendet wird.

## Bereitstellungstopologie

Je nach Netzwerktopologie können Sie WCCP-Cluster entweder mit einem einzelnen Router oder mit mehreren Routern bereitstellen. Unabhängig davon, ob sie mit einem einzelnen Router oder mehreren Routern verbunden sind, muss jede Appliance im Cluster identisch mit allen verwendeten Routern verbunden sein.

### Bereitstellung eines einzelnen Routers

Im folgenden Diagramm beschleunigen drei SD-WAN-Appliances das 200 Mbit/s WAN des Rechenzentrums. Die Site unterstützt 750 Virtual Apps-Benutzer.

Wie auf im [Datenblatt SD-WAN](#) gezeigt, kann ein SD-WAN 3000-100 100 Mbit/s und 400 Benutzer unterstützen, so dass ein Paar dieser Appliances 200 Mbit/s und 800 Benutzer unterstützt, was die Anforderungen des Rechenzentrums an eine 200 Mbit/s Verbindung erfüllt. und 750 Benutzer.

Zur Fehlertoleranz sollte der WCCP-Cluster jedoch weiterhin funktionieren, ohne überlastet zu werden, wenn eine Appliance ausfällt. Dies kann erreicht werden, indem drei Appliances verwendet werden, wenn die Berechnungen zwei erfordern. Dies wird die N+1-Regel genannt.

Fehler ist ein ungewöhnliches Ereignis, daher sind normalerweise alle drei Geräte in Betrieb. In diesem Fall unterstützt jede Appliance nur 67 Mbit/s und 250 Benutzer, lässt viel Spielraum und nutzt die Tatsache, dass der Cluster die dreifache CPU-Leistung und den dreifachen Komprimierungsverlauf einer einzelnen Appliance hat.

Ohne WCCP-Clustering würde so viel Kapazität und Fehlertoleranz ein Paar SD-WAN 4000-500 Appliances im Hochverfügbarkeitsmodus erfordern. Nur eine dieser Appliances ist gleichzeitig aktiv.

### **Mehrere Router-Bereitstellungen**

Die Verwendung mehrerer WAN-Router ähnelt der Verwendung eines einzelnen WAN-Routers. Wenn das vorherige Beispiel geändert wird, um zwei 100 Mbit/s Verknüpfungen anstelle eines 200 Mbit/s Hyperlinks einzuschließen, ändert sich die Topologie, die Berechnungen jedoch nicht.

### **Einschränkungen**

Das Konfigurieren von Appliances in einem WCCP-Cluster hat folgende Einschränkungen:

- Alle Appliances innerhalb eines Clusters müssen dasselbe Modell aufweisen und dieselbe Softwareversion verwenden.
- Die Parametersynchronisierung zwischen Appliances innerhalb des Clusters erfolgt nicht automatisch. Verwenden Sie das Command Center, um die Appliances als Gruppe zu verwalten.
- Die Gestaltung des SD-WAN-Datenverkehrs ist nicht wirksam, da sie darauf beruht, die gesamte Verbindung als Einheit zu steuern, und keines der Appliances ist dazu in der Lage. Router QoS können stattdessen verwendet werden.
- Die WCCP-basierten Load-Balancing-Algorithmen variieren nicht dynamisch von der Last, so dass ein guter Lastausgleich einige Tuning erfordern kann.
- Die Hash-Methode der Cache-Zuweisung wird nicht unterstützt. Maskenzuweisung ist die unterstützte Methode.
- Während der WCCP-Standard Maskenlängen von 1-7 Bit zulässt, unterstützt die Appliance Masken von 1-6 Bit.
- Multicastdienstgruppen werden nicht unterstützt. Es werden nur Unicast-Service-Gruppen unterstützt.
- Alle Router, die dasselbe Servicegruppenpaar verwenden, müssen dieselbe Weiterleitungsmethode (GRE oder L2) unterstützen.
- Die Weiterleitungs- und Rückgabemethode, die mit dem Router ausgehandelt wird, muss übereinstimmen: Beide müssen GRE oder beide müssen L2 sein. Einige Router unterstützen L2 nicht

in beide Richtungen, was zu einem Fehler Routers Vorwärts- oder Rückgabe- oder Zuweisungsfähigkeit nicht übereinstimmen. In diesem Fall muss die Servicegruppe als GRE konfiguriert sein.

- SD-WAN VPX unterstützt WCCP-Clustering nicht.
- Die Appliance unterstützt (und verhandelt) nur ungewichtete (gleiche) Cache-Zuweisungen. Gewichtete Zuordnungen werden nicht unterstützt.
- Einige ältere Appliances, z. B. das SD-WAN 700, unterstützen WCCP-Clustering nicht.
- (Nur SD-WAN 4000/5000) Pro Schnittstelle sind zwei Accelerator-Instanzen im L2-Modus erforderlich. Pro Appliance werden drei Schnittstellen unterstützt (und dann nur auf Appliances mit sechs oder mehr Accelerator-Instanzen.)
- (nur SD-WAN 4000/5000) WCCP-Steuerpakete vom Router müssen mit einer der auf der Appliance für die Dienstgruppe konfigurierten Router-IP-Adressen übereinstimmen. In der Praxis sollte die IP-Adresse des Routers für die Schnittstelle verwendet werden, die ihn mit der Appliance verbindet. Die Loopback-IP des Routers kann nicht verwendet werden.

### Einschränkungen bei der Bereitstellung von Arbeitsblättern und Clustern

Im folgenden Arbeitsblatt können Sie die Anzahl der Appliances, die für die Installation benötigt werden, und die empfohlene Maskenfeldgröße berechnen. Die empfohlene Maskengröße ist 1—2 Bit größer als die minimale Maskengröße für Ihre Installation.

Parameter	Wert	Hinweise
Verwendetes Appliance-Modell		—
Unterstützte Citrix Virtual Apps and Desktops Benutzer pro Gerät	$Uspec =$	Aus Datenblatt
Citrix Virtual Apps and Desktops von WAN-Link für Benutzer	$Uwan =$	—
Benutzerüberlastungsfaktor	$Uoverload = Uwan/Uspec =$	—
Unterstütztes BW pro Appliance	$BWspec =$	Aus Datenblatt
WAN-Verbindung BW	$BWwan =$	—
BW-Überlastfaktor	$BWoverload = BWwan/BWspec =$	—
Anzahl der benötigten Geräte	$N = \max(Uoverload, BWoverload) + 1 =$	Inklusive einem Ersatz

		—
Min. Anzahl der Buckets	$B_{min} = N$ , aufgerundet um $2^2 =$	—
Wenn SD-WAN 4000 oder 5000	$B_{min} = 2N$ , aufgerundet um $2^2 =$	—
Empfohlener Wert	$B = 4 B_{min}$ , wenn $B_{min} \leq 16$ , sonst $2 B_{min} =$	—
Anzahl der 1 Bits in der Adressmaske	$M = \log_2(B)$	Wenn $B=16$ , $M=4$ .

Maskenwert: Der Maskenwert ist eine 32-Bit-Adressmaske mit mehreren 1 Bits gleich M im zuvor bereitgestellten Arbeitsblatt. Oft können diese Bits die am wenigsten signifikanten Bits in der WAN-Subnetzmaske sein, die von Ihren Remote-Standorten verwendet wird. Wenn sich die Masken an Ihren Remotestandorten unterscheiden, verwenden Sie die Medianmaske. (Beispiel: Bei /24-Subnetzen sind die kleinsten signifikanten Bits des Subnetzes 0x00 00 nn 00. Die Anzahl der Bits, die auf eins gesetzt werden sollen, ist  $\log_2$  (Maskengröße): Wenn Maskengröße 16 ist, setzen Sie 4 Bits auf eins. Legen Sie also bei einer Maskengröße von 16 und einem /24-Subnetz den Maskenwert auf 0x00 00 0f 00 fest.)

Die obigen Richtlinien funktionieren nur, wenn das ausgewählte Subnetzfeld gleichmäßig im Datenverkehr verteilt ist, d. h., dass jedes von der Maske ausgewählte Adress-Bit ein Eins für die Hälfte der entfernten Hosts und eine Null für die andere Hälfte ist. Andernfalls ist der Lastenausgleich beeinträchtigt. Diese gleichmäßige Verteilung kann nur für wenige Bits im Netzwerkfeld zutreffen (nur 2 Bits). Wenn dies der Fall ist, verlagern Sie diese Bits in einem Teil des Hostadressfeldes, anstatt Bits im verletzenden Bereich des Subnetzfeldes zu maskieren, der die 50/50-Eigenschaft hat. Wenn beispielsweise nur drei Subnetzbits in einem /24-Subnetz die Eigenschaft 50/50 haben und Sie vier Maskenbits verwenden, vermeidet eine Maske von 0x00 00 07 10 das beleidigende Bit bei 0x00 00 0800 und verdrängt es auf 0x00 00 00 10, ein Teil des Adressfelds, der wahrscheinlich die 50/50 Eigenschaft hat, wenn Ihre entfernten Subnetze verwenden in der Regel mindestens 32 IP-Adressen.

Parameter	Wert	Hinweise
Endgültiger Maskenwert		—
Beschleunigte Brücke		Normalerweise APA

---

WAN-Service-Gruppe	Eine Servicegruppe, die noch nicht auf Ihrem Router verwendet wird (51-255)
LAN-Service-Gruppe	Eine weitere ungenutzte Servicegruppe
IP-Adresse des Routers	IP-Adresse der Routerschnittstelle am Anschluss zur Appliance
WCCP-Protokoll (normalerweise Auto)	—
DC-Algorithmus	Verwenden Sie Deterministic, wenn Sie nur zwei Appliances haben oder einen dynamischen Lastausgleich wie HSRP oder GSLB verwenden. Andernfalls verwenden Sie Am wenigsten störend.

---

Das Konfigurieren von Appliances in einem WCCP-Cluster hat folgende Einschränkungen:

- Alle Appliances innerhalb eines Clusters müssen dasselbe Modell aufweisen und dieselbe Softwareversion verwenden.
- Die Parametersynchronisierung zwischen Appliances innerhalb des Clusters erfolgt nicht automatisch. Verwenden Sie das Command Center, um die Appliances als Gruppe zu verwalten.
- Die Gestaltung des SD-WAN-Datenverkehrs ist nicht wirksam, da sie darauf beruht, die gesamte Verbindung als Einheit zu steuern, und keines der Appliances ist dazu in der Lage. Router QoS können stattdessen verwendet werden.
- Die WCCP-basierten Load-Balancing-Algorithmen variieren nicht dynamisch von der Last, so dass ein guter Lastausgleich einige Tuning erfordern kann.
- Die Hash-Methode der Cache-Zuweisung wird nicht unterstützt. Maskenzuweisung ist die unterstützte Methode.
- Während der WCCP-Standard Maskenlängen von 1-7 Bit zulässt, unterstützt die Appliance Masken von 1-6 Bit.
- Multicastdienstgruppen werden nicht unterstützt; nur Unicastdienstgruppen werden unterstützt.
- Alle Router, die dasselbe Servicegruppenpaar verwenden, müssen dieselbe Weiterleitungsmethode (GRE oder L2) unterstützen.

- Die Weiterleitungs- und Rückgabemethode, die mit dem Router ausgehandelt wird, muss übereinstimmen: Beide müssen GRE oder beide müssen L2 sein. Einige Router unterstützen L2 nicht in beide Richtungen, was zu einem Fehler Routers Vorwärts- oder Rückgabe- oder Zuweisungsfähigkeit nicht übereinstimmen. In diesem Fall muss die Servicegruppe als GRE konfiguriert sein.
- SD-WAN VPX unterstützt WCCP-Clustering nicht.
- Die Appliance unterstützt (und verhandelt) nur ungewichtete (gleiche) Cache-Zuweisungen. Gewichtete Zuordnungen werden nicht unterstützt.
- Einige ältere Appliances, z. B. das SD-WAN 700, unterstützen WCCP-Clustering nicht.
- (nur SD-WAN WANOP 4000/5000) Pro Schnittstelle werden zwei Beschleunigerinstanzen im L2-Modus benötigt. Pro Appliance werden nicht mehr als drei Schnittstellen unterstützt (und dann auf Appliances mit sechs oder mehr Accelerator-Instanzen).
- (nur SD-WAN 4000/5000) WCCP-Steuerpakete vom Router müssen mit einer der auf der Appliance für die Dienstgruppe konfigurierten Router-IP-Adressen übereinstimmen. In der Praxis sollte die IP-Adresse des Routers für die Schnittstelle verwendet werden, die ihn mit der Appliance verbindet. Die Loopback-IP des Routers kann nicht verwendet werden.

## Testen und Problembehandlung

Auf der Seite **Überwachung > Appliance > Anwendungsleistung > WCCP** wird der aktuelle Status nicht nur der lokalen Appliance, sondern aller anderen Appliances angezeigt, die dem Cluster beigetreten sind. Wählen Sie einen WCCP-Cache aus, und klicken Sie auf **Informationen abrufen**.

Auf der Registerkarte **Cache-Status** wird der Status der lokalen Appliance angezeigt. Wenn alles gut ist, ist der Status 25: hat Zuweisung. Sie müssen die Seite manuell aktualisieren, um Statusänderungen zu überwachen. Wenn die Appliance innerhalb eines Zeitlimits den Status 25: hat Zuweisung nicht erreicht, werden weitere informative Statusmeldungen angezeigt.

Zusätzliche Informationen werden angezeigt, wenn Sie auf die Registerkarte **Servicegruppe oder Router** klicken.

Auf der Registerkarte **Clusterzusammenfassung** werden Informationen zum WCCP-Cluster als Ganzes angezeigt. Als Nebeneffekt des WCCP-Protokolls verfügt jedes Mitglied des Clusters über Informationen über alle anderen, sodass diese Informationen von jeder Appliance im Cluster überwacht werden können.

Ihr Router kann auch Statusinformationen bereitstellen. Sehen Sie sich die Router-Dokumentation an.

## Konfigurieren von WCCP-Clustering

Nachdem Sie die Bereitstellungstopologie abgeschlossen, alle Einschränkungen berücksichtigt und das Bereitstellungsarbeitsblatt ausgefüllt haben, können Sie Ihre Appliances in einem WCCP-Cluster bereitstellen. Um den WCCP-Cluster zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- [Konfigurieren der NetScaler Instanzen](#)
- [Konfigurieren des Routers](#)
- [Konfigurieren der Appliance](#)

## Virtueller Inlinemodus

April 19, 2021

**Hinweis:** Verwenden Sie den virtuellen Inlinemodus nur, wenn sowohl der Inlinemodus als auch der WCCP-Modus unpraktisch sind. Mischen Sie den Inlinemodus und den virtuellen Inlinemodus nicht innerhalb derselben Appliance. Sie können jedoch virtuelle Inline- und WCCP-Modi innerhalb derselben Appliance mischen. Citrix empfiehlt keinen virtuellen Inlinemodus mit Routern, die die Integritätsüberwachung nicht unterstützen.

Im virtuellen Inlinemodus verwendet der Router Policy Based Routing-Regeln (PBR), um eingehenden und ausgehenden WAN-Datenverkehr zur Beschleunigung an die Appliance umzuleiten, und die Appliance leitet die verarbeiteten Pakete zurück an den Router weiter. Fast alle Konfigurationsaufgaben werden auf dem Router ausgeführt. Das einzige, was auf der Appliance konfiguriert werden muss, ist die Weiterleitungsmethode, und die Standardmethode wird empfohlen.

Wie WCCP erfordert die virtuelle Inline-Bereitstellung keine Neuverkabelung und keine Ausfallzeiten. Sie bietet eine Lösung für asymmetrische Routing-Probleme bei einer Bereitstellung mit zwei oder mehr WAN-Verbindungen. Im Gegensatz zu WCCP enthält es keine integrierte Statusüberwachung oder Zustandsprüfung, was die Fehlerbehebung erschwert. WCCP ist daher der empfohlene Modus, und virtueller Inlinemodus wird nur empfohlen, wenn Inline- und WCCP-Modi nicht praktikabel sind.

## Beispiel

Die folgende Abbildung zeigt ein einfaches Netzwerk, in dem der gesamte Datenverkehr, der für die Remotesite bestimmt oder empfangen wird, an die Appliance weitergeleitet wird. In diesem Beispiel verwenden sowohl der lokale Standort als auch die Remotesite den virtuellen Inlinemodus.



### Abbildung 1. Virtuelles Inline-Beispiel

Im Folgenden finden Sie einige Konfigurationsdetails für das Netzwerk in diesem Beispiel:

- Endpunktsysteme haben ihre Gateways auf den lokalen Router eingestellt (was nicht eindeutig für den virtuellen Inlinemodus ist).
- Jeder Router ist so konfiguriert, dass sowohl eingehenden als auch ausgehenden WAN-Datenverkehr an die lokale Appliance umgeleitet werden.
- Jede Appliance verarbeitet den vom lokalen Router empfangenen Datenverkehr und leitet ihn zurück an den Router weiter.
- PBR-Regeln, die auf dem Router konfiguriert sind, verhindern Routingschleifen, da Pakete nur einen Ausflug zur Appliance durchführen können. Die Pakete, die die Appliance an den Router zurückleitet, werden an ihr ursprüngliches (lokales oder entferntes) Ziel gesendet.
- Jede Appliance hat ihr Standardgateway wie üblich auf die Adresse des lokalen Routers gesetzt (auf der Seite **Konfiguration: Netzwerkadapter**). Die Optionen für die Weiterleitung von Paketen an den Router sind Return to Ethernet Sender und Send to Gateway.

## Konfigurieren der Paketweiterleitung auf der Appliance

April 19, 2021

Der virtuelle Inlinemodus bietet zwei Optionen zur Paketweiterleitung:

**Return to Ethernet Sender (Standard)**—In diesem Modus können mehrere Router eine Appliance gemeinsam nutzen. Die Appliance leitet virtuelle Inline-Ausgabepakete zurück, wie durch die Ethernet-Adresse des eingehenden Pakets angezeigt. Wenn zwei Router eine einzelne Appliance gemeinsam nutzen, erhält jeder seinen eigenen Datenverkehr zurück, aber nicht den Datenverkehr vom anderen Router. Dieser Modus funktioniert auch mit einem einzelnen Router.

**An Gateway senden (nicht empfohlen)**: In diesem Modus werden virtuelle Inline-Ausgabepakete zur Auslieferung an das Standardgateway weitergeleitet, selbst wenn sie für Hosts im lokalen Subnetz bestimmt sind. Diese Option ist normalerweise weniger wünschenswert als die Option Return to Ethernet Sender, da sie der Routingstruktur ein leicht vergessenes Element der Komplexität hinzufügt.

**So geben Sie die Option Paketweiterleitung an:** Wählen Sie auf der Seite “Konfiguration > Optimierungsregeln > Tuning” neben “Virtual Inline” die Option “Zurück zu Ethernet-Sender” oder “An Gateway senden” aus.

## Router-Konfiguration

April 19, 2021

Der Router hat drei Aufgaben bei der Unterstützung des virtuellen Inlinemodus:

1. Es muss sowohl eingehenden als auch ausgehenden WAN-Datenverkehr an die SD-WAN-Appliance weiterleiten.
2. Er muss SD-WAN-Datenverkehr an sein Ziel (WAN oder LAN) weiterleiten.
3. Er muss den Zustand der Appliance überwachen, damit die Appliance bei einem Ausfall umgangen werden kann.

### Policy-basierte Regeln

Im virtuellen Inlinemodus können die Paketweiterleitungsmethoden Routingschleifen erstellen, wenn die Routingregeln nicht zwischen einem Paket unterscheiden, das von der Appliance weitergeleitet wurde und einem Paket, das nicht vorhanden ist. Sie können jede Methode verwenden, die diese Unterscheidung macht.

Eine typische Methode besteht darin, einen der Ethernet-Ports des Routers der Appliance zuzuweisen und Routingregeln zu erstellen, die auf dem Ethernet-Port basieren, an dem Pakete ankommen. Pakete, die auf der für die Appliance dedizierten Schnittstelle eintreffen, werden nie wieder an die Appliance weitergeleitet, aber Pakete, die auf einer anderen Schnittstelle eintreffen, können sein.

Der grundlegende Routing-Algorithmus ist:

- Leiten Sie keine Pakete von der Appliance zurück an die Appliance weiter.
- Wenn das Paket aus dem WAN kommt, leiten Sie es an die Appliance weiter.
- Wenn das Paket für das WAN bestimmt ist, leiten Sie es an die Appliance weiter.
- Kein LAN-zu-LAN-Datenverkehr an die Appliance weiterleiten.
- Traffic Shaping ist nur wirksam, wenn der gesamte WAN-Datenverkehr die Appliance durchläuft.

**Hinweis: Beachten Sie** bei der Berücksichtigung von Routing-Optionen, dass die Rückgabe von Daten, nicht nur ausgehende Daten, durch die Appliance fließen muss. Wenn die Appliance beispielsweise im lokalen Subnetz platziert und als Standardrouter für lokale Systeme festgelegt wird, funktioniert dies nicht in einer virtuellen Inline-Bereitstellung. Ausgehende Daten würden durch die Appliance fließen, aber eingehende Daten würden sie umgehen. Um Daten über die Appliance ohne Neukonfiguration des Routers zu erzwingen, verwenden Sie den Inlinemodus.

## Gesundheitsüberwachung

Wenn die Appliance fehlschlägt, sollten Daten nicht an sie weitergeleitet werden. Standardmäßig führt Cisco richtlinienbasiertes Routing keine Zustandsüberwachung durch. Um die Zustandsüberwachung zu aktivieren, definieren Sie eine Regel zur Überwachung der Verfügbarkeit der Appliance und geben Sie die Option Verify-Availability für den Befehl set ip next-hop an. Wenn die Appliance bei dieser Konfiguration nicht verfügbar ist, wird die Route nicht angewendet und die Appliance wird umgangen.

Wichtig: Citrix empfiehlt den virtuellen Inlinemodus nur, wenn er mit der Integritätsüberwachung verwendet wird. Viele Router, die richtlinienbasiertes Routing unterstützen, unterstützen die Gesundheitsprüfung nicht. Die Funktion zur Überwachung der Gesundheit ist relativ neu. Es wurde in Cisco IOS Version 12.3 (4) T.

Es folgt ein Beispiel für eine Regel zur Überwachung der Verfügbarkeit der Appliance:

“pre codeblock

!- Use a ping (ICMP echo) to see if appliance is connected track 123 rtr 1 reachability ! rtr 1 type echo protocol Iplcmpecho 192.168.1.200 schedule 1 life forever start-time now

```

1 Diese Regel pingt die Appliance regelmäßig bei 192.168.1.200 an. Sie können gegen 123 testen, um zu sehen, ob das Gerät oben ist.
2
3 ## Routing-Beispiele
4
5 Die folgenden Beispiele veranschaulichen die Konfiguration von Cisco-Routern für die in gezeigten lokalen und Remotesites: [Virtuelles Inline-Beispiel](/de-de/citrix-sd-wan-wanop/11/cb-deployment-modes-con/br-adv-virt-inline-mode-con.html). Zur Veranschaulichung der Integritätsüberwachung umfasst die Konfiguration für den lokalen Standort die Integritätsüberwachung, die Konfiguration für den Remotestandort jedoch nicht.
6
7 Hinweis: Die Konfiguration für den lokalen Standort setzt voraus, dass bereits ein Ping-Monitor konfiguriert wurde.
8
9 Die Beispiele entsprechen der Cisco IOS CLI. Sie sind möglicherweise nicht auf Router anderer Anbieter anwendbar.
10
11 Lokaler Standort, Gesundheitsprüfung aktiviert:
12
13 ``` pre codeblock
14 !
15 ! For health-checking to work, do not forget to start
16 ! the monitoring process.
17 !
18 ! Original configuration is in normal type.
19 ! appliance-specific configuration is in bold.
20 !
21 ip cef

```

```
22 !
23 interface FastEthernet0/0
24 ip address 10.10.10.5 255.255.255.0
25 ip policy route-map client_side_map
26 !
27 interface FastEthernet0/1
28 ip address 172.68.1.5 255.255.255.0
29 ip policy route-map wan_side_map
30 !
31 interface FastEthernet1/0
32 ip address 192.168.1.5 255.255.255.0
33 !
34 ip classless
35 ip route 0.0.0.0 0.0.0.0 171.68.1.1
36 !
37 ip access-list extended client_side
38 permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
39 ip access-list extended wan_side
40 permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
41 !
42 route-map wan_side_map permit 20
43 match ip address wan_side
44 !- Now set the appliance as the next hop, if it's up.
45 set ip next-hop verify-availability 192.168.1.200 20 track 123
46 !
47 route-map client_side_map permit 10
48 match ip address client_side
49 set ip next-hop verify-availability 192.168.1.200 10 track 123
50 <!--NeedCopy-->
```

Remote-Standort (keine Integritätsprüfung):

“pre codeblock

! This example does not use health-checking.

! Remember, health-checking is always recommended,

! so this is a configuration of last resort.

!

!

ip cef

!

interface FastEthernet0/0

ip address 20.20.20.5 255.255.255.0

ip policy route-map client\_side\_map

!

interface FastEthernet0/1

ip address 171.68.2.5 255.255.255.0

ip policy route-map wan\_side\_map

!

```
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!_
```

```
1  Jedes der obigen Beispiele wendet eine Zugriffsliste auf eine
    Routenkarte an und fügt die Routenkarte an eine Schnittstelle an.
    Die Zugriffslisten identifizieren den gesamten Datenverkehr, der an
    einem beschleunigten Standort anfängt und an der anderen beendet
    wird (eine Quell-IP von 10.10.10.0/24 und Ziel 20.20.20.0/24 oder
    umgekehrt). Details zu Zugriffslisten und Routenkarten finden Sie in
    der Dokumentation Ihres Routers.
2
3  Diese Konfiguration leitet den gesamten übereinstimmenden IP-
    Datenverkehr an die Appliances um. Wenn Sie nur TCP-Datenverkehr
    umleiten möchten, können Sie die Zugriffslisten-Konfiguration wie
    folgt ändern (nur die Konfiguration der Remote-Seite wird hier
    gezeigt):
4
5  ``` pre codeblock
6  !
7  ip access-list extended client_side
8  permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
9  ip access-list extended wan_side
10 permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
11 !
12 <!--NeedCopy-->
```

Beachten Sie, dass für Zugriffslisten keine gewöhnlichen Masken verwendet werden. Platzhaltermasken werden stattdessen verwendet. Beachten Sie, dass beim Lesen einer Platzhaltermaske in Binärdatei 1 als egal-Bit betrachtet wird.

## Virtual Inline für Multiple-WAN-Umgebungen

April 19, 2021

Unternehmen mit mehreren WAN-Verbindungen verfügen häufig über asymmetrische Routing-Richtlinien, die anscheinend erfordern, dass sich eine Inline-Appliance an zwei Stellen gleichzeitig befindet. Der virtuelle Inlinemodus löst das asymmetrische Routing-Problem, indem die Routerkonfiguration verwendet wird, um den gesamten WAN-Datenverkehr über die Appliance zu senden, unabhängig von der verwendeten WAN-Verbindung. Die folgende Abbildung zeigt ein einfaches Beispiel für die Bereitstellung von mehreren WAN-Verbindungen.

Die beiden lokalen Router leiten den Datenverkehr an die lokale Appliance um. Die FE 0/0-Ports für beide Router befinden sich in derselben Broadcast-Domäne wie die Appliance. Die lokale Appliance muss die standardmäßige virtuelle Inline-Konfiguration (Return to Ethernet Sender) verwenden.

Abbildung 1. Virtueller Inlinemodus mit zwei WAN-Routern

## Virtueller Inlinemodus und hohe Verfügbarkeit

April 19, 2021

Der virtuelle Inlinemodus kann in einer Konfiguration mit hoher Verfügbarkeit (Hochverfügbarkeit) verwendet werden. Die folgende Abbildung zeigt eine einfache Bereitstellung mit hoher Verfügbarkeit. Im virtuellen Inlinemodus fungiert ein Appliance-Paar als eine virtuelle Appliance. Die Router-Konfiguration ist für ein Hochverfügbarkeitspaar dieselbe wie bei einer einzelnen Appliance, mit der Ausnahme, dass die virtuelle IP-Adresse des Hochverfügbarkeitspaars, nicht die IP-Adresse einer einzelnen Appliance, in den Router-Konfigurationstabellen verwendet wird. In diesem Beispiel müssen die lokalen Appliances die standardmäßige virtuelle Inline-Konfiguration (Return to Ethernet Sender) verwenden.

Abbildung 1. Beispiel für hohe Verfügbarkeit

## Überwachung und Fehlerbehebung

April 19, 2021

Im virtuellen Inlinemodus bietet die Appliance im Gegensatz zum WCCP-Modus keine virtuelle inline-spezifische Überwachung. Um eine virtuelle Inline-Bereitstellung zu beheben, melden Sie sich bei

der Appliance an und verwenden Sie die Dashboard-Seite, um zu überprüfen, ob Datenverkehr in die Appliance und aus ihr fließt. Fehler bei der Datenverkehrweiterleitung werden in der Regel durch Fehler in der Routerkonfiguration verursacht.

Wenn auf den Seiten Überwachung: Verwendung oder Überwachung: Verbindungen angezeigt wird, dass Datenverkehr weitergeleitet wird, aber keine Beschleunigung stattfindet (vorausgesetzt, dass eine Appliance bereits am anderen Ende der WAN-Verbindung installiert ist), überprüfen Sie, ob sowohl eingehenden WAN-Datenverkehr als auch ausgehenden WAN-Datenverkehr an der Appliance. Wenn nur eine Richtung weitergeleitet wird, kann keine Beschleunigung erfolgen.

Um die Gesundheitsprüfung zu testen, schalten Sie die Appliance herunter. Der Router sollte die Weiterleitung des Datenverkehrs beenden, nachdem der Algorithmus für die Gesundheitsprüfung ein Timeout erreicht hat.

## Gruppenmodus

April 19, 2021

Im Gruppenmodus werden zwei oder mehr Appliances zu einer einzigen virtuellen Appliance. Dieser Modus ist eine Lösung für das Problem des asymmetrischen Routing, das in jedem Fall definiert ist, in dem einige Pakete in einer bestimmten Verbindung durch eine bestimmte Appliance passieren, andere aber nicht. Eine Einschränkung der Appliance-Architektur besteht darin, dass die Beschleunigung nur dann erfolgen kann, wenn alle Pakete in einer bestimmten Verbindung dieselben zwei Appliances durchlaufen. Der Gruppenmodus überwindet diese Einschränkung.

Der Gruppenmodus kann mit mehreren oder redundanten Verbindungen verwendet werden, ohne die Router neu zu konfigurieren.

### Hinweis

Der Gruppenmodus wird auf den SD-WAN 4000- oder 5000-Einheiten nicht unterstützt.

Der Gruppenmodus gilt nur für die Appliances auf einer Seite der WAN-Verbindung. Die lokalen Appliances wissen nicht, ob die Remote-Appliances den Gruppenmodus verwenden.

Der Gruppenmodus verwendet einen Heartbeat-Mechanismus, um zu überprüfen, ob andere Mitglieder der Gruppe aktiv sind. Pakete werden nur an aktive Gruppenmitglieder weitergeleitet.

Das Vermeiden von asymmetrischem Routing ist der Hauptgrund für die Verwendung des Gruppenmodus, aber der Gruppenmodus ist nicht die einzige für diesen Zweck verfügbare Methode. Wenn Sie sich entscheiden, dass es die beste Methode für Ihre Umgebung ist, können Sie sie aktivieren, indem Sie einige Parameter festlegen. Wenn der Standardmechanismus zum Bestimmen, welche Appliance

für eine bestimmte Verbindung verantwortlich ist, keine optimale Beschleunigung bietet, können Sie die Weiterleitungsregeln ändern.

Abbildung 1. Gruppenmodus mit redundanten Verknüpfungen

Abbildung 2. Gruppenmodus mit nicht redundanten Verbindungen mit möglichem asymmetrischem Routing

Abbildung 3. Gruppenmodus auf nahe gelegenen Campus

## Verwendung des Gruppenmodus

April 19, 2021

Verwenden Sie den Gruppenmodus unter folgenden Umständen:

- Sie haben mehrere WAN-Verbindungen.
- Es besteht die Wahrscheinlichkeit eines asymmetrischen Routing (ein Paket auf einer bestimmten Verbindung kann über einen der beiden Links reisen).
- Der Gruppenmodus scheint einfacher und praktischer zu sein als Alternativen, die eine einzige Appliance verwenden.

Die Alternativen sind:

- WCCP-Modus, in dem der Datenverkehr von zwei oder mehr Verbindungen von WAN-Routern über das WCCP-Protokoll an dieselbe Appliance gesendet wird.
- Virtueller Inlinemodus, in dem Ihre Router Datenverkehr von zwei oder mehr Verbindungen über dieselbe Appliance (oder ein Hochverfügbarkeitspaar) senden.
- Mehrere Brücken, bei denen jede Verbindung eine andere beschleunigte Brücke in derselben Appliance durchläuft.
- Aggregation auf LAN-Ebene, bei der eine Appliance (oder ein Paar mit hoher Verfügbarkeit) näher am LAN platziert wird, bevor der WAN-Datenverkehr in zwei oder mehr Pfade aufgeteilt wird.

## Funktionsweise des Gruppenmodus

April 19, 2021

Im Gruppenmodus übernehmen die Einheiten, die Teil der Gruppe sind, jeweils den Besitz eines Teils der Verbindungen der Gruppe. Wenn eine bestimmte Appliance der Besitzer einer Verbindung ist, trifft



sie alle Beschleunigungsentscheidungen über diese Verbindung und ist für Komprimierung, Flusssteuerung, Paketweiterleitung usw. verantwortlich.

Wenn eine Appliance ein Paket für eine Verbindung empfängt, für die sie nicht der Besitzer ist, leitet sie das Paket an die Appliance weiter, die der Eigentümer ist. Der Besitzer untersucht das Paket, trifft die entsprechenden Beschleunigungsentscheidungen und leitet alle Ausgabepakete zurück an die nicht besitzende Appliance weiter. Dieser Prozess behält die vom Router getroffene Linkauswahl bei, während alle Pakete in der Verbindung von der eigentümlichen Appliance verwaltet werden können. Für die Router hat die Einführung der Appliances keine Konsequenzen. Die Router müssen in keiner Weise neu konfiguriert werden, und die Appliances müssen den Routing-Mechanismus nicht verstehen. Sie akzeptieren einfach die Weiterleitungsentscheidungen der Router.

Abbildung 1. Senden-seitiger Datenverkehr im Gruppenmodus

Abbildung 2. Empfangsseitiger Datenfluss im Gruppenmodus

Der Gruppenmodus verfügt über zwei vom Benutzer auswählbare Fehlermodi, die steuern, wie die Gruppenmitglieder miteinander interagieren, wenn einer von ihnen ausfällt. Der Fehlermodus bestimmt auch, ob die Umgehungskarte der ausgefallenen Appliance geöffnet wird (blockiert den Datenverkehr durch die Appliance) oder geschlossen bleibt (so dass der Datenverkehr weitergeleitet wird). Die Fehlermodi sind:

**Beschleunigen Sie fort-** Wenn ein Gruppenmitglied ausfällt, wird seine Umgehungskarte geöffnet und kein Datenverkehr wird durch die ausgefallene Appliance geleitet. Das Ergebnis ist vermutlich ein Failover, wenn redundante Links verwendet werden. Andernfalls ist der Link einfach nicht zugänglich. Die anderen Appliances in der Gruppe beschleunigen sich weiter. Der übliche Hashing-Algorithmus behandelt die geänderten Bedingungen. (Das heißt, der alte Hashing-Algorithmus wird verwendet, und wenn die fehlgeschlagene Einheit als Eigentümer angegeben wird, wird ein Hashing-Algorithmus angewendet, der auf der neuen, kleineren Gruppe basiert. Dadurch bleiben so viele ältere Verbindungen wie möglich erhalten.)

**Nicht beschleunigen - Wenn** ein Gruppenmitglied ausfällt, wird seine Umgehungskarte geschlossen, sodass der Datenverkehr ohne Beschleunigung durchlaufen kann. Da ein nicht beschleunigter Pfad ein asymmetrisches Routing einführt, gehen die anderen Mitglieder der Gruppe auch in den Pass-Through-Modus, wenn sie den Fehler erkennen.

## Gruppenmodus aktivieren

April 19, 2021

Um den Gruppenmodus zu aktivieren, erstellen Sie eine Gruppe von zwei oder mehr Appliances. Eine Appliance kann nur Mitglied einer Gruppe sein. Gruppenmitglieder werden anhand der IP-Adresse und des allgemeinen SSL-Namens in der Appliance-Lizenz identifiziert.

Alle Gruppenmodusparameter befinden sich auf der Seite Einstellungen: Gruppenmodus in der Tabelle Einstellungen konfigurieren: Gruppenmodus.

Abbildung 1. Seite Gruppen-Modus

### So aktivieren Sie den Gruppenmodus

1. Wählen Sie die Adresse aus, die für die Gruppenkommunikation verwendet werden soll. Oben in der Tabelle Gruppenmoduskonfiguration auf der Registerkarte Konfiguration: Erweiterte Bereitstellungen: Gruppenmodus enthält die Tabellenzeile unter Mitglieder-VIP die Verwaltungsadresse des Ports, der für die Kommunikation mit anderen Gruppenmitgliedern verwendet wird. Verwenden Sie das Dropdown-Menü (ohne Beschriftung), um die richtige Adresse auszuwählen (z. B. um den Aux1-Port zu verwenden, wählen Sie die IP-Adresse aus, die Sie dem Aux1-Port zugewiesen haben). Klicken Sie dann auf VIP ändern.
2. Fügen Sie der Liste mindestens ein weiteres Gruppenmitglied hinzu. (Gruppen von drei oder mehr werden unterstützt, werden aber selten verwendet.) Geben Sie in die nächste Zelle der Spalte Mitglied VIP die IP-Adresse des Ports ein, der von der anderen Appliance für die Gruppenmodus-Kommunikation verwendet wird.
3. Geben Sie den allgemeinen SSL-Namen des anderen Gruppenmitglieds in die Spalte SSL-Common Name ein. Der allgemeine SSL-Name wird auf der Registerkarte Konfigurieren: Erweiterte Bereitstellungen: Hochverfügbarkeit der anderen Appliance aufgeführt. Wenn es sich bei dem anderen Gruppenmitglied um ein Hochverfügbarkeitspaar handelt, handelt es sich bei dem aufgelisteten Namen um den allgemeinen SSL-Namen der primären Appliance.

**Hinweis:** Wenn die lokale Appliance nicht Teil eines Hochverfügbarkeitspaars ist, ist die erste Zelle im sekundären SSL-Standardnamen mit hoher Verfügbarkeit leer. Wenn das andere Gruppenmitglied ein Paar mit hoher Verfügbarkeit ist, geben Sie den SSL-Common Name der sekundären Hochverfügbarkeits-Appliance in der Hochverfügbarkeit an. Sekundäre SSL-Spalte Common Name.

4. Klicken Sie auf 'Hinzufügen'.
5. Wiederholen Sie die Schritte 2-4 für weitere Appliances oder Hochverfügbarkeitspaare in der Gruppe.
6. Die drei Schaltflächen unter der Liste der Gruppenmitglieder sind umschaltbar, so dass jeder als das Gegenteil seiner aktuellen Einstellung bezeichnet wird:
  - a) Auf der oberen Schaltfläche wird entweder angezeigt, **Nicht beschleunigen, wenn ein Mitgliedsfehler erkannt wird**, oder **Weiter, um zu beschleunigen, wenn ein Mitgliedsfehler erkannt wird**. Die Einstellung Nicht beschleunigen...funktioniert immer und blockiert den Datenverkehr nicht, aber wenn ein Mitglied fehlschlägt, gehen die

anderen Gruppenmitglieder in den Umgehungsmodus, was einen vollständigen Verlust der Beschleunigung verursacht. Mit der Option Weiter zu beschleunigen wird die Brücke der fehlerhaften Appliance zu einem offenen Stromkreis, und die Verbindung schlägt fehl. Diese Option ist geeignet, wenn der WAN-Router reagiert, indem er ein Failover verursacht. Neue Verbindungen und offene Verbindungen, die zu den überlebenden Appliances gehören, werden beschleunigt.

- b) Die untere Schaltfläche sollte nun mit der Bezeichnung Gruppenmodus deaktivieren gekennzeichnet werden. Ist dies nicht der Fall, aktivieren Sie den Gruppenmodus, indem Sie auf die Schaltfläche klicken.
7. Aktualisieren Sie den Bildschirm. Oben auf der Seite sollten die Gruppenmoduspartner auflisten, aber Warnungen über ihren Status anzeigen, da sie noch nicht für den Gruppenmodus konfiguriert wurden. Es kann beispielsweise darauf hinweisen, dass der Partner nicht gefunden werden kann oder eine andere Softwareversion ausführt.
8. Wiederholen Sie diesen Vorgang mit den anderen Mitgliedern der Gruppe. Innerhalb von 20 Sekunden nach dem Aktivieren des letzten Mitglieds der Gruppe sollte die Zeile Gruppenmodusstatus NORMAL angezeigt werden, und die anderen Gruppenmodusmitglieder sollten mit Status: Online und Konfiguration: OK aufgeführt werden.

## Weiterleitungsregeln

April 19, 2021

Standardmäßig wird der *Besitzer* einer Gruppenmodusverbindung durch einen Hash der Quell- und Ziel-IP-Adressen festgelegt. Jede Appliance in der Gruppe verwendet denselben Algorithmus, um zu bestimmen, welches Gruppenmitglied eine bestimmte Verbindung besitzt. Diese Methode erfordert keine Konfiguration. Der Besitzer kann optional durch benutzereinstellbare Regeln angegeben werden.

Da der Gruppen-Mode-Hash nicht identisch mit dem von Load Balancern verwendeten ist, wird etwa die Hälfte des Datenverkehrs in einer Gruppe mit zwei Appliances an die besitzende Appliance weitergeleitet. Im schlimmsten Fall bewirkt die Weiterleitung, dass die Last auf der LAN-seitigen Schnittstelle verdoppelt wird, was die Spitzenweiterleitungsrate der Appliance für den tatsächlichen WAN-Datenverkehr halbiert.

Diese Geschwindigkeitseinbuße kann reduziert werden, wenn die primären oder Aux1-Ethernet-Ports für den Datenverkehr zwischen Gruppenmitgliedern verwendet werden. Wenn Sie beispielsweise über eine Gruppe von zwei Appliances verfügen, können Sie ein Ethernet-Kabel verwenden, um die Primär Ports der beiden Einheiten zu verbinden und dann auf der Seite Gruppen-Modus auf jeder Ein-

heit den Primär Port angeben. Die maximale Leistung wird jedoch erreicht, wenn der zwischen den Gruppenmodusmitgliedern weitergeleitete Datenverkehr minimiert wird.

Der Besitzer kann optional nach bestimmten IP/Port-basierten Regeln eingestellt werden. Diese Regeln müssen für alle Appliances in der Gruppe identisch sein. Jedes Mitglied der Gruppe überprüft, ob seine Gruppenmodus-Konfiguration mit den anderen identisch ist. Wenn nicht alle Konfigurationen identisch sind, wechselt keine der Mitglieds-Appliances in den Gruppenmodus.

Wenn der Datenverkehr zuerst bei der Appliance eintrifft, die Eigentümer der Verbindung ist, wird er beschleunigt und normal weitergeleitet. Wenn es zuerst bei einer anderen Appliance in der Gruppe ankommt, wird es über einen GRE-Tunnel an seinen Besitzer weitergeleitet, der ihn beschleunigt und zur Weiterleitung an die ursprüngliche Appliance zurückgibt. Somit lässt der Gruppenmodus die Linkauswahl des Routers unverändert.

Die Verwendung von expliziten IP-basierten Weiterleitungsregeln kann die Menge der Gruppenmodus-Weiterleitung reduzieren. Dies ist besonders nützlich in Szenarien mit Primärverknüpfung/Backup-Link-Szenarien, bei denen jeder Link einen bestimmten Bereich von IP-Adressen verarbeitet, aber als Backup fungieren kann, wenn der andere Link ausgefallen ist.

#### Abbildung 1. IP-basierte Besitzerauswahl

Weiterleitungsregeln können sicherstellen, dass Gruppenmitglieder nur ihren natürlichen Datenverkehr verarbeiten. In vielen Installationen, bei denen der Verkehr normalerweise über die normale Verbindung geleitet wird und nur selten die andere überquert, können diese Regeln den Overhead erheblich reduzieren.

Regeln werden in der Reihenfolge von oben nach unten ausgewertet, und die erste Übereinstimmungsregel wird verwendet. Regeln werden mit einem optionalen IP-Adresse/Maskenpaar (das mit Quell- und Zieladressen verglichen wird) und mit einem optionalen Portbereich abgeglichen.

Unabhängig von der Reihenfolge der Regeln wird, wenn die Partner-Appliance nicht verfügbar ist, kein Datenverkehr an sie weitergeleitet, unabhängig davon, ob eine Regel übereinstimmt oder nicht.

In der folgenden Abbildung ist beispielsweise Mitglied 172.16.1.102 der Eigentümer des gesamten Datenverkehrs in oder aus seinem eigenen Subnetz (172.16.1.0/24), während Mitglied 172.16.0.184 der Eigentümer des gesamten anderen Datenverkehrs ist.

Wenn ein Paket bei Unit 172.16.1.102 eintrifft und nicht an/von net 172.16.1.0/24 adressiert wird, wird es an 172.16.0.184 weitergeleitet.

Wenn Unit 172.16.0.184 fehlschlägt, leitet Unit 172.16.1.102 keine Pakete mehr weiter. Es versucht, den Verkehr selbst zu handhaben. Dieses Verhalten kann verhindert werden, indem Sie auf der Registerkarte Gruppenmodus auf **Nicht beschleunigen, wenn Mitgliedsfehler erkannt wird** .

Schreiben Sie in einem Setup mit einer primären WAN-Verbindung und einer Backup-WAN-Verbindung die Weiterleitungsregeln, um den gesamten Datenverkehr an die Appliance auf der primären Verbindung zu senden. Wenn die primäre WAN-Verbindung fehlschlägt, aber die primäre

Appliance nicht, wird ein Failover des WAN-Routers durchgeführt und Datenverkehr über die sekundäre Verbindung gesendet. Die Appliance auf der sekundären Verbindung leitet den Datenverkehr an die primäre Link-Appliance weiter, und die Beschleunigung wird ungestört fortgesetzt. Diese Konfiguration verwaltet beschleunigte Verbindungen nach dem Link-Failover.

Abbildung 2. Weiterleitungsregeln

## Überwachung und Fehlerbehebung Gruppenmodus

April 19, 2021

Zwei Dinge sollten in einer Gruppenmodus-Installation überprüft werden:

- Dass die beiden Appliances in den Gruppenmodus gegangen sind, der auf der Seite Konfiguration: Erweiterte Bereitstellungen: Gruppenmodus der beiden Appliances ermittelt werden kann.
- Das Verhalten des Gruppenmoduspaars ist wie gewünscht, wenn das andere Mitglied ausfällt und wenn eine der Links fehlschlägt, wie dies durch Deaktivieren der anderen Appliance bzw. vorübergehend Trennen einer der Links bestimmt wird.

## Anpassen der Ethernet-Ports

April 19, 2021

Eine typische Appliance verfügt über vier Ethernet-Ports: zwei beschleunigte Bridged-Ports, die als *beschleunigtes Paar A* (APA.1 und APA.2) bezeichnet werden, mit einem Bypass (Fail-to-Wire-Relay) und zwei nicht beschleunigte Motherboard-Ports, die Primär und Aux1 genannt werden. Die überbrückten Ports sorgen für Beschleunigung, während die Motherboard-Ports manchmal für sekundäre Zwecke verwendet werden. Die meisten Installationen verwenden nur die überbrückten Ports.

Einige SD-WAN-Geräte haben nur die Motherboard-Ports. In diesem Fall werden die beiden Motherboard-Ports überbrückt.

Auf die Benutzeroberfläche der Appliance kann über ein VLAN- oder Nicht-VLAN-Netzwerk zugegriffen werden. Sie können ein VLAN zu Verwaltungszwecken jedem der überbrückten Ports oder Motherboard-Ports der Appliance zuweisen.

Abbildung 1. Ethernet-Ports

## Portliste

Die Ports sind wie folgt benannt:

Ethernet-Anschluss	Name
Hauptplatinenanschluss 1	Primär (oder APA.1, wenn keine Bypasskarte vorhanden ist)
Hauptplatinenanschluss 2	Auxiliary1 oder Aux1 (oder APA.2, wenn keine Bypasskarte vorhanden ist)
Brücke #1	Beschleunigtes Paar A (APA, mit Ports APA.1 und APA.2)
Brücke #2	Beschleunigtes Paar B (aPb, mit Ports aB.1 und apB.2)

Tabelle 1. Ethernet-Portnamen

## Funktionsweise des Hochverfügbarkeitsmodus

April 19, 2021

Bei einem Paar mit hoher Verfügbarkeit (Hochverfügbarkeit) ist eine Einheit primär und die andere sekundär. Der primäre überwacht seinen eigenen Status und den Status des sekundären. Wenn ein Problem festgestellt wird, wird ein Failover der Datenverkehrsverarbeitung an die sekundäre Appliance durchgeführt. Vorhandene TCP-Verbindungen werden beendet. Um ein erfolgreiches Failover sicherzustellen, halten die beiden Appliances ihre Konfigurationen synchronisiert. In einer Hochverfügbarkeitskonfiguration im WCCP-Modus unterhält die Appliance, die den Datenverkehr verarbeitet, die Kommunikation mit dem Upstream-Router.

**Statusüberwachung**—Wenn Hochverfügbarkeit aktiviert ist, sendet die primäre Appliance das VRRP-Protokoll einmal pro Sekunde ein Heartbeat-Signal an die sekundäre Appliance. Darüber hinaus überwacht die primäre Appliance den Carrier-Status ihrer Ethernet-Ports. Der Verlust von Carrier an einem zuvor aktiven Port bedeutet einen Verlust der Konnektivität.

**Failover** Wenn das Heartbeat-Signal der primären Appliance ausfällt oder wenn die primäre Appliance fünf Sekunden lang an einem zuvor aktiven Ethernet-Port verliert, übernimmt die sekundäre Appliance die primäre Appliance. Wenn die fehlgeschlagene Appliance neu gestartet wird, wird sie zur sekundären. Die neue primäre kündigt sich im Netzwerk mit einer ARP-Sendung an. MAC-Spoofing wird nicht verwendet. Die Ethernet-Bridging ist auf der sekundären Appliance deaktiviert, sodass die

primäre Appliance als einziger Pfad für den Inline-Datenverkehr bleibt. Fail-to-Wire wird auf beiden Appliances gehemmt, um Schleifen zu verhindern.

**Warnung**

Die Ethernet-Bypass Funktion ist im Hochverfügbarkeitsmodus deaktiviert. Wenn beide Appliances in einem Inline-Hochverfügbarkeitspaar Strom verlieren, geht die Konnektivität verloren. Wenn bei Stromausfällen WAN-Konnektivität erforderlich ist, muss mindestens eine Appliance an eine Sicherungsstromquelle angeschlossen sein.

**Hinweis**

Die sekundäre Appliance im Hochverfügbarkeitspaar hat einen ihrer Bridge-Ports, Port APA.1, deaktiviert, um Weiterleitungsschleifen zu verhindern. Wenn die Appliance über zwei Brücken verfügt, ist APB.1 ebenfalls deaktiviert. Verwenden Sie bei einer einarmigen Installation Port APA.2. Andernfalls wird auf die sekundäre Appliance nicht zugegriffen, wenn die hohe Verfügbarkeit aktiviert ist.

**Primäre/sekundäre Zuweisung**—Wenn beide Appliances neu gestartet werden, wird die erste, die sich vollständig initialisiert hat, zur primären. Das heißt, den Appliances sind keine zugewiesenen Rollen zugewiesen, und die erste, die verfügbar ist, übernimmt als primäre. Die Appliance mit der höchsten IP-Adresse auf der Schnittstelle, die für den VRRP-Heartbeat verwendet wird, wird als Tie-Breaker verwendet, wenn beide gleichzeitig verfügbar sind.

**Verbindungsbeendigung während des Failovers**—Sowohl beschleunigte als auch nicht beschleunigte TCP-Verbindungen werden als Nebeneffekt des Failovers beendet. Nicht-TCP-Sitzungen sind nicht betroffen, mit Ausnahme der Verzögerung, die durch den kurzen Zeitraum (mehrere Sekunden) zwischen dem Ausfall der primären Appliance und dem Failover auf die sekundäre Appliance verursacht wird. Benutzer erleben das Schließen offener Verbindungen, aber sie können neue Verbindungen öffnen.

**Konfigurationssynchronisierung**—Die beiden Appliances synchronisieren ihre Einstellungen, um sicherzustellen, dass die sekundäre für die primäre Version übernommen werden kann. Wenn die Konfiguration des Paares über die browserbasierte Schnittstelle geändert wird, aktualisiert die primäre Appliance die sekundäre Appliance sofort.

Hochverfügbarkeit kann nur aktiviert werden, wenn beide Appliances dieselbe Softwareversion ausführen.

**hohe Verfügbarkeit im WCCP-Modus**—Wenn WCCP mit einem Hochverfügbarkeitspaar verwendet wird, stellt die primäre Appliance die Kommunikation mit dem Router her. Die Appliance verwendet ihre Verwaltungs-IP-Adresse auf APA oder aPb, nicht ihre virtuelle IP-Adresse, um mit dem Router zu kommunizieren. Nach einem Failover richtet die neue primäre Appliance die WCCP-Kommunikation mit dem Router ein.

## Verkabelungsanforderungen

April 19, 2021

Die beiden Appliances im Hochverfügbarkeitspaar werden entweder in paralleler oder einarmiger Anordnung im selben Subnetz installiert, die beide in der folgenden Abbildung dargestellt sind. Verwenden Sie in einer Einarm-Anordnung den APA.2-Port (und optional den APB.2-Port), nicht den APA.1-Port. Einige Modelle benötigen ein separates Verwaltungs-LAN, unabhängig davon, ob sie im Inlinemodus oder im einarmigen Modus bereitgestellt werden. Dies ist nur im mittleren Diagramm dargestellt.

Abbildung 1. Verkabelung für Hochverfügbarkeitspaare

Unterbrechen Sie die obige Topologie nicht mit zusätzlichen Switches. Random Switch-Arrangements werden nicht unterstützt. Jeder der Schalter muss entweder ein einzelner, monolithischer Schalter, ein einziger logischer Schalter oder ein Teil desselben Gehäuses sein.

Wenn das Spanning-Tree-Protokoll (STP) an den an die Appliances angeschlossenen Router- oder Switch-Ports aktiviert ist, funktioniert das Failover. Die Failoverzeit kann jedoch auf etwa 30 Sekunden ansteigen. Ohne STP beträgt die Failover-Zeit ungefähr fünf Sekunden. Um das möglichst kurze Failover-Intervall zu erreichen, deaktivieren Sie STP an den Ports, die mit den Appliances verbunden sind.

## Sonstige Anforderungen

April 19, 2021

Beide Appliances in einem Paar mit hoher Verfügbarkeit müssen die folgenden Kriterien erfüllen:

- Sie verfügen über identische Hardware, wie im Eintrag Systemhardware auf der Seite Dashboard gezeigt.
- Führen Sie genau die gleiche Software-Version aus.
- Mit Ethernet-Bypass Karten ausgestattet sein. Informationen zum Bestimmen, was in Ihren Appliances installiert ist, finden Sie auf der Seite Dashboard .

Appliances, die keine hohe Verfügbarkeit unterstützen, zeigen auf der Seite Konfiguration: Hohe Verfügbarkeit eine Warnung an.



## Management-Zugriff auf das Hochverfügbarkeitspaar

April 19, 2021

Wenn Sie ein Paar mit hoher Verfügbarkeit (Hochverfügbarkeit) konfigurieren, weisen Sie dem Paar eine virtuelle IP-Adresse (VIP) zu, mit der Sie die beiden Appliances so verwalten können, als wären sie eine einzelne Einheit. Nachdem Sie den Hochverfügbarkeitsmodus aktiviert haben, ist die Verwaltung der sekundären Appliance über ihre IP-Adresse meist deaktiviert, wobei die meisten Parameter ausgegraut sind. Eine Warnmeldung zeigt den Grund auf jeder Seite an. Verwenden Sie die Hochverfügbarkeits-VIP für alle Verwaltungsaufgaben. Sie können jedoch den Hochverfügbarkeitsstatus der sekundären Appliance über die Verwaltungsschnittstelle deaktivieren.

## Konfigurieren des Hochverfügbarkeitspaars

April 19, 2021

Sie können zwei neu installierte Appliances als Hochverfügbarkeitspaar konfigurieren, oder Sie können ein Hochverfügbarkeitspaar erstellen, indem Sie einer vorhandenen Installation eine zweite Appliance hinzufügen.

Voraussetzungen: Physische Installation und grundlegende Konfigurationsverfahren

So konfigurieren Sie Hochverfügbarkeit

1. Stellen Sie sicher, dass nicht mehr als eine Appliance mit den Verkehrsnetzen (auf den beschleunigten Brücken) verbunden ist. Wenn beide miteinander verbunden sind, trennen Sie ein Brückenkabel von den aktiven Brücken der zweiten Einheit. Dies verhindert Weiterleitungsschleifen.
2. Deaktivieren Sie auf der Seite Features der ersten Appliance die Datenverkehrsverarbeitung. Dadurch wird die Beschleunigung deaktiviert, bis das Hochverfügbarkeitspaar konfiguriert ist.
3. Wiederholen Sie dies für die zweite Appliance.
4. Wechseln Sie auf der ersten Appliance zur Registerkarte Konfiguration: Erweiterte Bereitstellungen: Hohe Verfügbarkeit, siehe unten.
5. Aktivieren Sie das Kontrollkästchen Aktiviert.
6. Klicken Sie auf den Link Virtuelle IP-Adresse konfigurieren, und weisen Sie der APA-Schnittstelle eine virtuelle IP-Adresse zu. Diese Adresse wird später verwendet, um beide Geräte als Einheit zu steuern.
7. Kehren Sie zur Seite Hochverfügbarkeit zurück und weisen Sie dem Paar im Feld VRRP VRID eine VRRP-ID zu. Obwohl der Wert standardmäßig Null ist, beträgt der gültige Bereich der VRRP-ID-Nummern 1 bis 255. Innerhalb dieses Bereichs können Sie einen beliebigen Wert angeben, der nicht zu einem anderen VRRP-Gerät im Netzwerk gehört.

8. Geben Sie im Feld Partner-SSL-Standardname den allgemeinen SSL-Namen der anderen Appliance ein, der auf der Registerkarte Konfiguration: Erweiterte Bereitstellungen: Hochverfügbarkeit in das Feld Partner-SSL-Standardname angezeigt wird. Die hier verwendeten SSL-Anmeldeinformationen sind werkseitig installiert.
9. Klicken Sie auf Aktualisieren.
10. Wiederholen Sie die Schritte 3-8 auf der zweiten Appliance. Wenn Sie die Appliance über eine beschleunigte Bridge (z. B. APA) verwalten, müssen Sie möglicherweise das in Schritt 1 entfernte Ethernet-Kabel erneut anschließen, um eine Verbindung mit der zweiten Appliance herzustellen. Wenn ja, schließen Sie dieses Kabel an und trennen Sie das entsprechende Kabel an der ersten Appliance.
11. Navigieren Sie mit Ihrem Browser zur virtuellen IP-Adresse des Hochverfügbarkeitspaares. Aktivieren Sie die Datenverkehrsverarbeitung auf der Seite Features. Jede weitere Konfiguration erfolgt über diese virtuelle Adresse.
12. Schließen Sie das abgeschaltete Kabel an.
13. Auf jeder Appliance sollte auf der Seite Konfiguration: Erweiterte Bereitstellungen: Hohe Verfügbarkeit nun angezeigt werden, dass Hochverfügbarkeit aktiv ist und dass eine Appliance die primäre und die andere die sekundäre ist. Ist dies nicht der Fall, wird oben auf dem Bildschirm ein Warnbanner angezeigt, das die Art des Problems anzeigt.

Abbildung 1. Seite Hochverfügbarkeitskonfiguration

## Aktualisieren von Software auf einem Hochverfügbarkeitspaar

April 19, 2021

Das Aktualisieren der SD-WAN-Software auf einem Hochverfügbarkeitspaar führt zu einem Failover während des Updates.

Hinweis: Wenn Sie auf die Schaltfläche Aktualisieren klicken, werden alle geöffneten TCP-Verbindungen beendet.

### So aktualisieren Sie die Software auf einem Hochverfügbarkeitspaar

1. Melden Sie sich bei beiden Appliances an.
2. Aktualisieren Sie die Software auf der sekundären Appliance, und starten Sie sie neu. Nach dem Neustart ist die Appliance weiterhin die sekundäre. Überprüfen Sie, ob die Installation erfolgreich war. Die primäre Appliance sollte zeigen, dass die sekundäre Appliance vorhanden ist, dass die automatische Parametersynchronisierung jedoch aufgrund eines Versionsfehlers nicht funktioniert.

3. Aktualisieren Sie die Software auf der primären Appliance, und starten Sie sie neu. Der Neustart verursacht ein Failover, und die sekundäre Appliance wird zur primären. Wenn der Neustart abgeschlossen ist, sollte die hohe Verfügbarkeit vollständig hergestellt werden, da beide Appliances dieselbe Software ausführen.

## **Speichern/Wiederherstellen von Parametern eines Hochverfügbarkeitspaares**

April 19, 2021

Die Funktion Systemwartung: Sicherung/Wiederherstellung kann verwendet werden, um Parameter eines Hochverfügbarkeitspaares wie folgt zu speichern und wiederherzustellen:

### **So sichern Sie die Parameter**

Verwenden Sie die Sicherungsfunktion wie gewohnt. Melden Sie sich also an der GUI über die VIP-Adresse mit hoher Verfügbarkeit an (wie üblich bei der Verwaltung des Hochverfügbarkeitspaares) und klicken Sie auf der Seite Systemverwaltung: Sicherung/Wiederherstellung auf Download-Einstellungen.

### **So stellen Sie die Parameter wieder her**

1. Deaktivieren Sie die hohe Verfügbarkeit auf beiden Appliances, indem Sie das Kontrollkästchen Aktiviert auf der Registerkarte Konfiguration: Erweiterte Bereitstellungen: Hohe Verfügbarkeit (hohe Verfügbarkeit) deaktivieren.
2. Ziehen Sie ein Netzkabel von der Brücke einer Appliance ab. (Nennen Sie es Appliance A.)
3. Ziehen Sie das Netzkabel von Gerät A ab.
4. Stellen Sie die Parameter auf der anderen Appliance (Appliance B) wieder her, indem Sie einen zuvor gespeicherten Satz von Parametern auf der Seite "Systemwartung: Backup/Wiederherstellung" hochladen und auf "Einstellungen wiederherstellen" klicken. (Für den Abschluss dieses Vorgangs ist ein Neustart erforderlich, wodurch die hohe Verfügbarkeit wieder aktiviert wird.)
5. Warten Sie, bis Appliance B neu gestartet ist. Es wird die primäre.
6. Appliance A neu starten.
7. Melden Sie sich an der Benutzeroberfläche von Appliance A an, und aktivieren Sie die Hochverfügbarkeit auf der Registerkarte Konfiguration: Erweiterte Bereitstellungen: Hohe Verfügbarkeit (hohe Verfügbarkeit) erneut. Die Appliance erhält ihre Parameter von der primären.

8. Schließen Sie das Netzkabel an, das in Schritt 2 entfernt wurde.

Beide Appliances werden nun wiederhergestellt und synchronisiert.

## Problembehandlung bei Hochverfügbarkeitspaaren

April 19, 2021

Wenn die Appliances einen Fehler melden, den Hochverfügbarkeitsmodus zu betreten, wird auch die Ursache in der Fehlermeldung angezeigt. Einige Probleme, die den Hochverfügbarkeitsmodus beeinträchtigen können, sind:

- Die andere Appliance wird nicht ausgeführt.
- Die Hochverfügbarkeitsparameter der beiden Appliances sind nicht identisch.
- Auf den beiden Appliances wird nicht dieselbe Softwareversion ausgeführt.
- Die beiden Appliances haben nicht die gleiche Modellnummer.
- Eine falsche oder unvollständige Verkabelung zwischen den Appliances lässt den Heartbeat für hohe Verfügbarkeit zwischen ihnen nicht passieren.
- Die SSL-Zertifikate für hohe Verfügbarkeit/Gruppenmodus-SSL-Zertifikate auf einer oder beiden Appliances sind beschädigt oder fehlen.

## Zwei-Box-Modus

April 19, 2021

Der Zwei-Box-Modus ist eine WCCP-Einarm-basierte Bereitstellung, bei der die SD-WAN SE-Appliance als WCCP-Router fungiert und die SDWAN-WANOP (4000/5000) Appliances als WCCP-Clients fungieren und dabei helfen, WCCP-Konvergenz zu etablieren. Auf diese Weise werden alle virtuellen Pfad-/Intranet-Service-orientierten TCP-Pakete, die die SD-WAN SE Appliance erreichen, zur Optimierung weitergeleitet, indem sie sowohl SD-WAN SE als auch WANOP Vorteile für den Kundenverkehr bieten.

Der Zwei-Box-Modus wird nur bei den folgenden Appliance-Modellen unterstützt:

- SD-WAN SE-Appliances —4000, 4100 und 5100
- SD-WANOP-Geräte —4000, 4100, 5000 und 5100

**Hinweis**

Auf Hochverfügbarkeits- und WCCP-Bereitstellungsmodi kann nicht zugegriffen werden, wenn der Zwei-Box-Modus aktiviert ist. Diese Bereitstellungsmodi sind jedoch für den Benutzer zur Verwaltung verfügbar.

**Wichtig**

- Obwohl die Legacy-WCCP-Bereitstellung deaktiviert ist, wenn der Zwei-Box-Modus aktiviert ist, kann die Konvergenz der Dienstgruppen nur auf der WCCP-Überwachungsseite überprüft werden. Es gibt keine separate GUI-Seite unter dem Monitoring-Abschnitt für den Zwei-Box-Modus.
- Wenn der WCCP-Prozess, der auf der Standard Edition-Appliance ausgeführt wird, mehrmals innerhalb eines kurzen Zeitraums neu gestartet wird, z. B. dreimal in einer Minute, wird die Servicegruppe automatisch heruntergefahren. Um die WCCP-Konvergenz auf der WANOP-Appliance abrufen zu können, aktivieren Sie in diesem Szenario die WCCP-Funktion in der Web-GUI der WANOP-Appliance erneut.
- Wenn sich die WCCP-Konfiguration oder die WAN-Optimierung im Zusammenhang mit der Konfiguration auf der Standard Edition-Appliance ändert, wird die externe WANOP-Appliance neu gestartet. Wenn Sie beispielsweise das Kontrollkästchen WCCP in der Schnittstellengruppe des Konfigurationseditors, gefolgt vom Change Management-Prozess, aktivieren/deaktivieren, startet auch die WANOP-Appliance neu.

**Hinweis**

Beachten Sie auch die folgenden Punkte, die bei der Implementierung des Zwei-Box-Modus zu beachten sind:

- Wenn eine Routingdomäne aus dem Konfigurationseditor zur WANOP-Appliance ausgewählt ist, sollte sie der Schnittstellengruppe hinzugefügt werden, für die WCCP aktiviert ist.
- Der Datenverkehr derselben Routingdomäne sollte auch auf der Partnerseite ausgewählt werden. Beispiel: **MCN > Branch01**, um die Vorteile der WAN-Optimierung zu beobachten.
- Wenn eine Routingdomäne in der Schnittstellengruppe ausgewählt ist, für die WCCP aktiviert ist, sollte eine andere Schnittstellengruppe, die die überbrückten Schnittstellen enthält, dieselbe Routingdomäne konfiguriert sein. Nur wenn die WCCP-aktivierte Schnittstellengruppe die Routingdomäne konfiguriert hat, reicht es nicht aus, den End-to-End-Datenverkehr mit WAN-Optimierungsvorteilen zu übertragen.

## Citrix SD-WAN Standard Edition

So konfigurieren Sie die Lösung im Zwei-Box-Modus in der Standard Edition-Appliance am DC- oder Zweigstandort:

1. Wechseln Sie in der SD-WAN SE-Webverwaltungsschnittstelle zu **Konfiguration > Virtuelles WAN > Konfigurations-Editor**. Öffnen Sie ein vorhandenes Konfigurationspaket oder erstellen Sie ein Paket.
2. Wechseln Sie im ausgewählten Konfigurationspaket zur Registerkarte **Erweitert**, um die Konfigurationsdetails anzuzeigen.
3. Öffnen Sie **Globale** Einstellungen, und erweitern Sie **Routingdomänen, um anzuzeigen, dass das Kontrollkästchen An WANOP umleiten** aktiviert ist.
4. Erweitern Sie DC, um **WCCP** für die **virtuelle Schnittstelle** unter **Schnittstellengruppeneinstellungen** zu aktivieren, die anzeigen, für welche virtuelle Netzwerkschnittstelle die Appliance aktiviert ist.
5. Erweitern Sie **Sites+ Hinzufügen**, um die Einstellungen der Zweigroutingdomäne und der Schnittstellengruppeneinstellungen anzuzeigen. Unter dem Zweigstandort ist das Kontrollkästchen **An WANOP umleiten** für Routingdomänen aktiviert.

### Hinweis

Der WCCP-Listener sollte nur für die virtuellen Netzwerkschnittstellen aktiviert werden, für die nur EINE Ethernet-Schnittstelle konfiguriert ist. Aktivieren Sie den WCCP-Listener nicht auf einem BRIDGED-Paar. Es soll auf der ONE-ARM-Schnittstelle zwischen den SD-WAN SE und SD-WAN WANOP-Einheiten aktiviert werden.

## Citrix SD-WAN WANOP-Konfiguration

So konfigurieren Sie den Zwei-Box-Bereitstellungsmodus in der Web-GUI der SD-WAN WANOP Appliance:

1. Wechseln Sie in der SD-WAN WANOP-Webverwaltungsschnittstelle zu **Konfiguration > Appliance-Einstellungen > Erweiterte Bereitstellungen > Zwei-Box-Lösung**.
2. Klicken Sie auf das Symbol **Bearbeiten**, um die beiden Einstellungen für den Boxmodus zu bearbeiten. Der Informationsdialog zu **Cache-IPs** wird angezeigt. Klicken Sie auf **OK**.
3. Aktivieren Sie das **Kontrollkästchen Zwei Kästchen aktiviert**.
4. Geben Sie die **Peer-IP** ein. Peer IP ist die IP-Adresse der SD-WAN Standard Edition Appliance.
5. Geben Sie die Benutzeranmeldeinformationen ein, und klicken Sie auf **Übernehmen**.

## Konfiguration und Verwaltbarkeit im Zwei-Box-Modus

Im Folgenden sind einige der beiden Boxmoduskonfigurations- und Verwaltbarkeitspunkte aufgeführt, die für die Bereitstellung in Betracht gezogen werden sollten:

- SD-WAN WANOP Konfigurationen, die unten erwähnt werden, können vom SD-WAN SE Konfigurationseditor als einheitlichen Bereich konfiguriert werden
  - SERVICE CLASS
  - APPLICATION CLASSIFIER
  - FEATURES
  - SYSTEM TUNING

## Überwachen

Sie können den SD-WANOP-Datenverkehr direkt über die Seite Überwachung der Web-Benutzeroberfläche der SD-WAN SE Appliance überwachen. Auf diese Weise können sowohl die SDWAN-SE als auch die SDWAN-WO Appliances in einem einzigen Bereich überwacht werden, während der Datenverkehr verarbeitet wird. Sie können die Verbindungsdetails, Details zu sicheren Partnern usw. unter dem Knoten WAN-Optimierung in der SDWAN-SE-Benutzeroberfläche anzeigen.

## Konfiguration

Sie können APPFLOW direkt über die SDWAN-SE-**Konfigurationsseite** unter **APPFLOW**-Knoten konfigurieren. Dadurch kann SDWAN-SE als ein einziger Bereich für die Konfiguration von APPFLOW und anderen Datenverarbeitungskonfigurationsattributen wie Service Class, Application Classifiers fungieren. Die Konfiguration auf der SDWAN-SE spiegelt die SDWAN-WO-Konfiguration wider, wodurch eine nahtlose APPFLOW Funktionalität unterstützt wird.

SD-WAN WANOP, die bereits von Citrix Application Delivery Management (ADM) erkannt wurde, sollte isoliert und nicht mit Citrix ADM konfiguriert werden, bis dieser Modus ausgeschaltet ist. Dies liegt daran, dass die Konfiguration von WANOP für die Datenverarbeitung von der SD-WAN SE-Appliance im Zwei-Box-Modus verwaltet wird.

Erweiterte Optimierungen oder Secure Acceleration sollten direkt auf der SDWAN-SE-Appliance konfiguriert werden, wie wir es auf der SDWAN-WO Appliance konfigurieren würden. Dies hilft, einen einzelnen Bereich der Konfiguration von Konfigurationen wie Domain Join oder Secure Acceleration/SSL-Profilerstellung für erweiterte Optimierungen oder SSL-Proxy aufrechtzuerhalten.

- Die Lizenzierung sollte für jede SD-WAN SE und SD-WAN WANOP Appliances separat verwaltet werden.
- Software-Upgrade sollte für jede SD-WAN SE und SD-WAN WANOP Appliances mit den entsprechenden Softwarepaketen separat verwaltet werden. Zum Beispiel tar.gz für SD-WAN SE und Upgrade für SD-WAN WANOP.
- Die Datenpfadintegration sollte zwischen SD-WAN SE und externen WANOP-Appliances über den WCCP-Bereitstellungsmodus konfiguriert werden.
  - Auf Datenpfad-Ebene werden sowohl WCCP- als auch Virtual WAN-Funktionen durch Datenpfadintegration zwischen WANOP und SE extern im Einarmmodus angeboten, um Optimierungsvorteile zu erzielen.

## Einheitliche Konfiguration und Überwachung

Wenn Sie den Zwei-Box-Modus mit SD-WAN SE und SDWANOP-Appliances aktivieren, können Sie die Konfiguration in der SD-WAN SE-Appliance ähnlich anzeigen, wie Sie zwei Box-Konfigurationen mit der SD-WAN-EE-Appliance anzeigen können.

1. Gehen Sie zu **Konfiguration > Virtuelles WAN > WAN-Optimierung**
2. Appflow-Knoten unter **Konfiguration > Appliance-Einstellungen**
3. WAN-Optimierungsknoten unter Konfiguration.

Diese Informationen werden von der SD-WAN WANOP-Appliance umgeleitet, die sich im Zwei-Box-Modus mit der SD-WAN SE-Appliance befindet.

Konfigurationen im Zusammenhang mit WANOP, wie SSL Acceleration und AppFlow können nun von der SD-WAN SE Web-GUI durchgeführt werden.

Verkehrsbezogene Statistiken wie Verbindungen, Komprimierung, CIFS/SMB, ICA Advanced, MAPI und Partner können jetzt von der SD-WAN SE-Web-GUI unter **Überwachung > WAN-Optimierung** ähnlich der SD-WAN Premium Edition-Appliance aus überwacht werden.

## Änderung der Verwaltungs-IP-Adresse für die SD-WAN WANOP Appliance im Zwei-Box-Modus

So ändern Sie die Verwaltungs-IP-Adresse der SDWAN-WANOP-Appliance im Zwei-Box-Modus:

1. Führen Sie den Befehl *clear\_wo\_sync* auf der SD-WAN SE-Appliance aus. Es stellt sicher, dass die SD-WAN WANOP IP-Adressinformationen für die GUI-Umleitung gelöscht werden.



2. Deaktivieren und aktivieren Sie die Konfiguration des Zwei-Box-Modus auf der SD-WAN WANOP-Appliance. Die neue IP-Adresse (geänderte IP) der SD-WAN WANOP Appliance wird an SD-WAN SE gesendet. Die neue geänderte IP-Adresse wird in den URL-Umleitungsseiten angezeigt.

Die Verwaltungs-IP-Adresse wird für die Konfiguration der Peer-IP-Adresse verwendet.

## **Deaktivieren Sie den Zwei-Box-Modus auf der SD-WAN WANOP-Appliance**

So deaktivieren oder entkoppeln Sie die SD-WAN WANOP- und SD-WAN SE-Geräte aus dem Zwei-Box-Modus:

1. Deaktivieren Sie den Zwei-Box-Modus von der SD-WAN WANOP-Appliance.
2. Es wird erwartet, dass die SD-WAN WANOP-Appliance zwei Box-Mode-Seiten in der Web-GUI SD-WAN SE angezeigt wird. Um diese Seiten zu löschen, führen Sie den Befehl `clear_wo_syncaus`.

## **FAQ**

April 19, 2021

- [Beschleunigung](#)
- [Komprimierung](#)
- [CIFS und MAPI](#)
- [RPC über HTTP](#)
- [SCPS](#)
- [Sicheres Peering](#)
- [SSL-Beschleunigung](#)
- [Citrixsd-WAN WANOP Einsteckbar](#)
- [Traffic Shaping](#)
- [Upgrade](#)
- [Video-Caching](#)
- [Office 365](#)

## Beschleunigung

April 19, 2021

### **Verwendet die Beschleunigung einen Tunnel?**

Nein, die Beschleunigung ist transparent und verwendet dieselben IP-Adressen und Portnummern wie die ursprüngliche Verbindung. Dadurch können Ihre aktuellen Überwachungsmethoden weiterhin normal funktionieren.

### **Wie ändert die Beschleunigung den Paketstrom?**

Bei nicht komprimierten Verbindungen fügt die Beschleunigung dem TCP-Header des Pakets Optionen hinzu, lässt jedoch die Paketnutzlast intakt. Diese Optionen ermöglichen es den Citrix SD-WAN WANOP-Geräten an jedem Ende der Verbindung, miteinander zu kommunizieren. Darüber hinaus wird die TCP-Sequenznummer angepasst, um zu verhindern, dass Routingprobleme oder Appliance-Fehler beschleunigte Pakete und nicht beschleunigte Pakete in derselben Verbindung mischen.

Bei komprimierten Verbindungen wird natürlich die Nutzlast komprimiert und der Ausgang des Kompressors wird in Full-Size-Pakete akkumuliert. Das Ergebnis ist, dass beispielsweise die 3:1-Komprimierung dazu führt, dass ein Drittel so viele Pakete übertragen werden, anstatt die gleiche Anzahl von Paketen, die jeweils auf ein Drittel reduziert werden. Die Komprimierung verwendet auch Citrix SD-WAN WANOP TCP-Header-Optionen und die Anpassung der Sequenznummer.

### **Was sind die grundlegenden Anforderungen der Beschleunigung?**

Die Beschleunigung erfordert ein Citrix SD-WAN WANOP-Gerät an beiden Enden der Verbindung, die Verbindung muss das TCP-Protokoll verwenden und alle Pakete für die Verbindung müssen beide Citrix SD-WAN WANOP-Geräte durchlaufen.

## CIFS und MAPI

April 19, 2021

### **Welche Voraussetzungen müssen vor der Konfiguration von MAPI und Signed SMB auf einer Citrix SD-WAN WANOP-Appliance erforderlich sein?**

Sie müssen die folgenden Bedingungen erfüllen, bevor Sie MAPI und Signed SMB auf einer Citrix SD-WAN WANOP-Appliance konfigurieren:

- Die Option Secure Peer sollte sowohl auf der Client- als auch auf der serverseitigen Appliance auf True festgelegt sein.

- Ein Delegatbenutzer muss der Appliance im Datenzentrum hinzugefügt werden und sein Status sollte "Erfolg" sein.
- Die Rechenzentrumsseitige Appliance muss erfolgreich der Domäne beitreten.
- Die auf der serverseitigen Appliance konfigurierte DNS-IP-Adresse muss erreichbar sein.

Weitere Informationen finden Sie unter [Konfigurieren einer Citrix SD-WAN WANOP-Appliance zur Optimierung des sicheren Windows-Datenverkehrs](#).

### **Was muss ich auf dem Domänencontroller für einen delegierten Benutzer konfigurieren?**

Sie müssen einen Benutzer auf dem Domänencontroller erstellen, bevor Sie die Delegierung für den Benutzer auf einer Citrix SD-WAN WANOP-Appliance konfigurieren.

### **Muss ich etwas auf dem DNS-Server konfigurieren?**

Ja. Auf dem DNS-Server müssen Sie Forward- und Reverse-Lookups für alle IP-Adresse der Domänencontroller konfigurieren.

### **Was muss ich überprüfen, bevor ich die Citrix SD-WAN WANOP-Appliance dazu bringe, der Domäne beizutreten?**

Bevor die Appliance der Domäne beitreten soll, überprüfen Sie Folgendes:

- IP-Adressen, die für primäre oder sekundäre DNS-Server konfiguriert sind, sollten erreichbar sein.
- Domain sollte erreichbar sein.
- Gelöste Domänen-IP-Adressen sollten erreichbar sein.
- Optional sollte der Status des Dienstprogramms vor Domain-Join Check bestehen.

### **Wie kann ich überprüfen, ob die Citrix SD-WAN WANOP Appliance bereit ist, einen Benutzer als Delegiertenbenutzer hinzuzufügen?**

Sie können den Benutzer mithilfe des Dienstprogramms Delegaten prüfen auf der Windows-Domänenseite überprüfen. Wenn der Status für alle Parameter keine Fehlermeldungen enthält, kann die Appliance den Benutzer als delegierten Benutzer hinzufügen.

Wenn das Dienstprogramm Fehler anzeigt, müssen Sie diese beheben, bevor Sie einen Benutzer als delegierten Benutzer hinzufügen. Sie können auf das Protokoll verweisen, um die Testergebnisse zu verstehen.

### **Gibt es Anforderungen für die Länge des Hostnamens und des Hostnamens der serverseitigen Citrix SD-WAN WANOP Appliance?**

Stellen Sie auf der Serverseite Citrix SD-WAN WANOP Appliance sicher, dass der Hostname im Netzwerk eindeutig ist. Darüber hinaus darf die Länge des Hostnamens nicht mehr als 15 Zeichen betragen.

**Kann ich die unidirektionale Vertrauensstellung in der Domäne konfigurieren?**

Nein. Der Client und der Server müssen die Mitglieder einer Domäne sein, die bidirektionales Vertrauen in die Domäne der serverseitigen Citrix SD-WAN WANOP-Appliance hat. Die Appliance unterstützt keine unidirektionale Vertrauensstellung.

**Kann ich den Macintosh Outlook-Client verwenden und die Beschleunigungsvorteile der Citrix SD-WAN WANOP Appliance erhalten?**

Nein. Macintosh Outlook verwendet MAPI nicht als Kommunikationsprotokoll. Daher können Sie nicht Macintosh Outlook in diesem Setup verwenden.

**Muss ich die Zweigseite der Citrix SD-WAN WANOP-Appliance der Domäne beitreten lassen, um verschlüsseltes MAPI zu beschleunigen?**

Nein. Sie müssen nicht dazu führen, dass die Citrix SD-WAN WANOP-Appliance auf der Zweigseite der Domäne beitrifft, um verschlüsselte MAPI zu beschleunigen.

**Kann ich eine Citrix SD-WAN WANOP 2000-Appliance mit Windows-Server auf Rechenzentrumsseite für verschlüsseltes MAPI konfigurieren?**

Ja. Sie können eine Citrix SD-WAN WANOP 2000 Appliance mit Windows-Server auf Rechenzentrumsseite für verschlüsseltes MAPI konfigurieren.

**Wenn ich eine Citrix SD-WAN WANOP-Appliance zum Beitritt zu einer Domäne bereitstelle und ein mit einer anderen Zeitzone konfigurierter NTP-Server im Netzwerk synchronisiert, synchronisiert die Appliance die Zeit mit dem Domänencontroller oder dem NTP-Server?**

Wenn Sie die Citrix SD-WAN WANOP-Appliance dazu bringen, einer Domäne beizutreten, synchronisiert die Appliance ihre Zeit immer mit dem Domänencontroller und nicht mit dem NTP-Server.

**Wie lang ist die Standarddauer auf der Citrix SD-WAN WANOP-Appliance, um die schwarz aufgelistete Verbindung zu löschen?**

Standardmäßig werden die Verbindungen auf der Sperrliste in 900 Sekunden gelöscht.

**Welche Outlook-Authentifizierungsmechanismen werden auf einer Citrix SD-WAN WANOP-Appliance unterstützt?**

Ab Version 6.2.4 unterstützt die Appliance Negotiate (Standard) und NTLM v2 Outlook-Authentifizierung, Kerberos-Authentifizierung wird jedoch nicht unterstützt. Version 6.2.3 und frühere Versionen unterstützen jedoch nur die Outlook-Authentifizierung aushandeln.

**Unterstützt Citrix SD-WAN WANOP Outlook Anywhere, RPC über HTTPS?**

Ja, ab Version 7.3.

## Komprimierung

April 19, 2021

### Was ist der Vorteil von Citrix SD-WAN WANOP Compression?

Während der grundlegende Mechanismus der Komprimierung darin besteht, Datenströme zu verkleinern, besteht der Vorteil darin, die Dinge schneller zu machen. Eine kleinere Datei (oder eine kleinere Transaktion) benötigt weniger Zeit für die Übertragung. Größe spielt keine Rolle: Der Punkt der Komprimierung ist Geschwindigkeit.

### Wie wird der Kompressionsvorteil gemessen?

Es gibt zwei Möglichkeiten, den Kompressionsvorteil zu messen: Zeit und Kompressionsverhältnis. Die beiden sind verwandt, wenn die WAN-Verbindung der dominante Engpass ist. Da der Citrix SD-WAN WANOP-Kompressor sehr schnell ist und Daten in Echtzeit komprimiert, wird eine Datei, die um 5:1 komprimiert, in einem Fünftel der Zeit überträgt. Dies gilt bis zu einem sekundären Engpass. Wenn der Client beispielsweise zu langsam ist, um eine Übertragung mit voller Geschwindigkeit zu verarbeiten, liefert ein Kompressionsverhältnis von 5:1 weniger als eine Geschwindigkeit von 5:1.

### Wie funktioniert die Komprimierung?

Die Komprimierungs-Engine speichert Daten, die zuvor über die Verbindung übertragen wurden, wobei die neueren Daten im Speicher und eine viel größere Menge auf der Festplatte gespeichert sind. Wenn eine zuvor übertragene Zeichenfolge erneut auftritt, wird sie durch einen Verweis auf die vorherige Kopie ersetzt. Diese Referenz wird über das WAN anstelle der tatsächlichen Zeichenfolge gesendet, und die Appliance am anderen Ende sucht die Referenz und kopiert sie in den Ausgabe-Stream.

### Was ist das maximal erreichbare Komprimierungsverhältnis?

Das maximal erreichbare Komprimierungsverhältnis bei einer Citrix SD-WAN WANOP-Appliance beträgt ungefähr 10.000:1.

### Was ist das erwartete Komprimierungsverhältnis?

Das Gesamtkomprimierungsverhältnis ist der Durchschnitt aller Versuche, die Datenströme auf der Verknüpfung zu komprimieren. Einige komprimieren besser als andere, und einige komprimieren überhaupt nicht. Die Appliance verwendet Service-Klassen, um zu verhindern, dass offensichtlich nicht komprimierbare Ströme an den Kompressor gesendet werden. Die Auswirkungen der Komprimierung auf verschiedene Datentypen variieren wie folgt:

Einmalige komprimierte oder verschlüsselte Daten —Streams, die nie wieder zu sehen sind und bereits komprimiert oder verschlüsselt wurden, wie verschlüsselte SSH-Tunnel und Echtzeit-Videokameraüberwachung —werden nicht komprimiert, da ihre Datenströme nie doppelt so groß sind.

Komprimierte binäre Daten oder verschlüsselte Daten, die mehr als einmal gesehen werden, komprimieren extrem gut bei der zweiten und nachfolgenden Übertragung, mit Komprimierungsverhältnissen im Bereich von Hunderten bis Tausenden zu eins bei diesen späteren Übertragungen. Bei der ersten Übertragung komprimieren sie nicht. Das durchschnittliche Komprimierungsverhältnis für solche Daten hängt davon ab, wie häufig Daten mehrmals angezeigt werden. Während einzelne Übertragungen manchmal Komprimierungsverhältnisse über 1,000:1 zeigen, liegen Durchschnittswerte für die komprimierten binären Daten auf den Verbindungsmittelwerten zwischen 1,5:1 und 5:1 bei den meisten Links, wobei bei einigen Links Durchschnittswerte über 10:1 liegen, abhängig von der Art des Datenverkehrs.

Textströme und unkomprimierte/unverschlüsselte Binärdaten komprimieren auch beim ersten Durchgang. Textströme komprimieren sich gut, da selbst nicht verwandte Texte viele Teilzeichenfolgen gemeinsam haben. Dies gilt für Dokumente, Quellcode, HTML-Seiten usw. Erstpasskompression in der Größenordnung von 1,5:1 bis 4:1 sind üblich. Im zweiten und nachfolgenden Durchgang komprimieren sie fast ebenso wie komprimierte Binärdaten (100:1 oder mehr). Unkomprimierte Binärdaten sind variabel, komprimiert aber oft besser als Text. Beispiele für unkomprimierte Binärdaten sind CD-Images, ausführbare Dateien sowie unkomprimierte Bild-, Audio- und Videoformate. Auf dem zweiten und nachfolgenden Durchgang komprimieren sie sowohl etwa als auch komprimierte Binärdaten.

Citrix Virtual Apps and Desktops-Daten werden besonders bei Dateiübertragungen, Druckerausgabe und Video komprimiert, sofern zuvor dieselben Datenströme den Link durchquert haben. Aufgrund des Protokoll-Overhead beträgt die Spitzenkomprimierung ungefähr 40:1, und die durchschnittliche Komprimierung liegt wahrscheinlich in der Nähe von 3:1. Interaktive Datenströme wie Bildschirmaktualisierungen) liefern Komprimierungsergebnisse in der Größenordnung von 2:1.

### **Was ist der Unterschied zwischen Caching und Komprimierung?**

Caching speichert ganze benannte Objekte auf der clientseitigen Appliance. Der Name kann ein Pfad und Dateiname im Fall von Dateisystem-Caching oder eine URL im Falle von Web-Caching sein. Wenn Sie ein identisches Objekt mit einem anderen Namen übertragen, bietet der Cache keinen Nutzen. Wenn Sie ein Objekt mit dem gleichen Namen wie ein zwischengespeichertes Objekt übertragen, jedoch mit geringfügigen inhaltlichen Unterschieden, bietet der Cache keinen Nutzen. Wenn das Objekt aus dem Cache bereitgestellt werden kann, wird es nicht vom Server abgerufen.

Die Komprimierung hingegen hat kein Konzept von Objektnamen und hat Vorteile, wenn eine Zeichenfolge in der Übertragung mit einer Zeichenfolge übereinstimmt, die sich bereits im Komprimierungsverlauf befindet. Wenn Sie eine Datei herunterladen, 1% ihres Inhalts ändern und die neue Datei hochladen, können Sie beim Upload eine 99:1 Komprimierung erzielen. Wenn Sie eine Datei herunterladen und dann in ein anderes Verzeichnis auf der Remote-Site hochladen, erreichen Sie möglicherweise auch ein hohes Komprimierungsverhältnis. Die Komprimierung erfordert keine Dateisperre und leidet nicht unter Staleness. Das Objekt wird immer vom Server abgerufen und ist somit immer byte-für-Byte-korrekt.

## RPC über HTTPS

April 19, 2021

### **Ist es zwingend erforderlich, eine Dienstklasse zu erstellen, um RPC über HTTPS-Verbindungen zu beschleunigen?**

Das Erstellen einer neuen Serviceklasse ist eine optionale Aufgabe. Sie können eine vorhandene HTTPS-Dienstklasse verwenden. Um jedoch Berichte speziell für RPC-über-HTTPS-Verbindungen zu erstellen, müssen Sie eine neue Dienstklasse erstellen und das SSL-Profil daran binden. Wenn Sie keine Dienstklasse für RPC-über-HTTPS-Verbindungen erstellen möchten, können Sie das von Ihnen erstellte SSL-Profil an die Web-Service-Klasse (Privat-Secure) binden.

### **Ich habe keine Dienstklasse für die RPC-über-HTTPS-Anwendungen erstellt. Wie wirkt sich dies auf die Berichterstellung der RPC-über-HTTPS-Verbindungen aus?**

Wenn Sie die Appliance auf Version 7.3 aktualisieren, gehören die erstellten RPC-über-HTTPS-Anwendungen keiner Dienstklasse an. Daher werden alle RPC-über-HTTPS-Verbindungen in den Berichten als TCP Andere Verbindungen aufgeführt. Wenn Sie diese Verbindungen als RPC-über-HTTPS-Verbindungen klassifizieren möchten, müssen Sie eine Dienstklasse für diese Anwendungen erstellen.

### **Gibt es eine Standarddienstklasse für RPC über HTTPS auf der Appliance?**

Nein. Die Appliance verfügt nur über Standardanwendungen und nicht über Standarddienstklassen. Sie müssen die Serviceklasse für eine Anwendung erstellen.

### **Bietet die Appliance dem RPC gegenüber HTTPS-Verbindungen irgendwelche SSL-Komprimierungsvorteile?**

Nein. Die Appliance bietet keine SSL-Komprimierungsvorteile für RPC über HTTP-Verbindungen. Komprimierungsvorteile sind nur für die Verschlüsselung und Entschlüsselung von HTTPS-Datenverkehr verfügbar.

### **Optimiert die Appliance ähnlich wie MAPI die Latenz für RPC-über-HTTPS-Verbindungen?**

Nein. Die Appliance optimiert die Latenz für RPC über HTTPS nicht.

### **unterscheidet sich MAPI über HTTP von RPC über HTTPS?**

Ja. MAPI über HTTP ist ein neues Protokoll, das auf Microsoft Exchange Server 2013 SP1 oder höher unterstützt wird.

### **Was ist der Unterschied zwischen den RPC- über HTTPS-Einstellungen auf clientseitigen und serverseitigen Citrix SD-WAN WANOP-Appliances?**

Außer dem Erstellen einer Serviceklasse und dem Hinzufügen von RPC über HTTPS-Anwendungen benötigen Sie keine zusätzliche Konfiguration auf einer clientseitigen Citrix SD-WAN WANOP-Appliance.

### **Was passiert, wenn ich das SSL-Profil im transparenten Proxy-Modus konfiguriere?**

Einige Exchange-Server benötigen TLS-Sitzungsticket-Support. Um Verbindungen zu diesen Servern zu beschleunigen, müssen Sie ein SSL-Profil mit geteiltem Proxy erstellen, da der transparente Proxy-modus TLS-Sitzungstickets nicht unterstützt.

### **Wenn ein Lastausgleichs-Setup für Microsoft Exchange Server verwendet wird, welche Ziel-IP-Adresse sollte ich der Filterregel hinzufügen, wenn eine RPC-über-HTTPS-Dienstklasse erstellt wird?**

Wenn Sie eine Load Balancing-Appliance verwenden, fügen Sie die virtuelle IP-Adresse (VIP) der Filterregel hinzu, wenn Sie eine RPC-über-HTTP-Dienstklasse erstellen.

### **Wie kann ich zwischen MAP- und RPC-über-HTTPS-Datenverkehr auf der Outlook-Seite (MAPI) unterscheiden?**

Sie können den Datenverkehr anhand von Anwendungen unterscheiden, die auf der Seite Outlook (MAPI) angezeigt werden. Beispielsweise werden MAPI und RPC über HTTPS für die folgenden Anwendungen verwendet:

- **MAPI:** MAPI und eMAPI
- **RPC über HTTPS:** HTTP MAPI, HTTP eMAPI, HTTPS MAPI, and HTTPS eMAPI



## SCPS

April 19, 2021

### **Was ist SCPS-Protokoll?**

Space Communications Protocol Standard (SCPS) -Protokoll ist eine Variante des TCP-Protokolls.

### **Was ist die Verwendung des SCPS-Protokolls?**

SCPS-Protokoll wird in der Satellitenkommunikation und ähnlichen Anwendungen verwendet.

### **Wird das SCPS-Protokoll auf einer Citrix SD-WAN WANOP Appliance unterstützt?**

Ja. Die Citrix SD-WAN WANOP-Appliance unterstützt das SCPS-Protokoll und beschleunigt die mit diesem Protokoll übertragene Daten.

### **Kann ich eine SCPS-fähige Appliance mit einer nicht SCPS-fähigen Appliance verwenden?**

Ja. Wenn Sie SCPS-fähige Appliances mit nicht SCPS-fähigen Appliances mischen müssen, stellen Sie sie so bereit, dass keine Abweichungen auftreten. Sie können entweder IP-basierte Dienstklassenregeln verwenden oder die Bereitstellung so anordnen, dass jeder Pfad über passende Appliances verfügt.

### **Was passiert, wenn ich eine SCPS-fähige Appliance an einem Ende ohne SCPS-fähige Appliance am anderen Ende des Linksverwende?**

Wenn für die Appliance an einem Ende der Verbindung SCPS aktiviert ist und eine nicht, leidet die Weiterübertragungsleistung. Diese Bedingung verursacht auch eine Warnung SCPS-Modus Mismatch.

### **Was ist der Unterschied zwischen dem Verhalten einer SCPS-fähigen Appliance und einer Standardeinheit?**

Der Hauptunterschied zwischen einem SCPS-fähigen und dem Standardverhalten der Appliance besteht darin, dass SCPS-Stil selektive negative Bestätigungen (SNACKs) anstelle von standardmäßigen selektiven Bestätigungen (SACKs) verwendet wird.

## Sicheres Peering

April 19, 2021

### **Welche Citrix SD-WAN WANOP-Funktionen erforderten ein sicheres Peering?**

Sie müssen ein sicheres Peering zwischen Citrix SD-WAN WANOP-Appliances an zwei Enden der Verbindung einrichten, wenn Sie eine der folgenden Funktionen verwenden möchten:

- SSL-Komprimierung
- Signierte CIFS-Unterstützung
- Verschlüsselte MAPI-Unterstützung

**Muss ich etwas in Betracht ziehen, bevor ich einen sicheren Tunnel konfiguriere?**

Ja. Sie müssen eine Krypto-Lizenz bestellen und erhalten, bevor Sie einen sicheren Tunnel zwischen den Citrix SD-WAN WANOP-Appliances am Ende der Verbindung konfigurieren können.

**Was passiert, wenn Sie das sichere Peering auf einer Appliance an einem Ende des Links aktivieren?**

Wenn Sie Secure Peering auf einer Citrix SD-WAN WANOP-Appliance an einem Ende der Verbindung aktivieren, erkennt die andere Appliance diese und versucht, einen SSL-Signaltunnel zu öffnen. Wenn sich die beiden Appliances über diesen Tunnel erfolgreich authentifizieren, verfügen die Appliances über eine sichere Peering-Beziehung. Alle beschleunigten Verbindungen zwischen den beiden Appliances werden verschlüsselt, und die Komprimierung ist aktiviert.

**Was passiert, wenn ich das sichere Peering auf der Partner-Appliance nicht aktiviere?**

Wenn eine Appliance sicheres Peering aktiviert hat, werden Verbindungen mit einem Partner, für den es keine sichere Peer-Beziehung aufweist, nicht verschlüsselt oder komprimiert, obwohl die TCP-Durchflusssteuerungsbeschleunigung weiterhin verfügbar ist. Die Komprimierung ist deaktiviert, um sicherzustellen, dass Daten, die im Komprimierungsverlauf von gesicherten Partnern gespeichert sind, nicht mit ungesicherten Partnern geteilt werden können.

**Warum benötige ich ein Keystore-Kennwort?**

Sie benötigen ein Keystore-Kennwort, um auf die Sicherheitsparameter zuzugreifen. Dieses Kennwort unterscheidet sich vom Administratorkennwort und ermöglicht es, die Sicherheitsverwaltung von anderen Aufgaben zu trennen. Wenn das Keystore-Kennwort zurückgesetzt wird, gehen alle vorhandenen verschlüsselten Daten und privaten Schlüssel verloren.

Um Daten zu schützen, selbst wenn die Appliance gestohlen wurde, muss das Schlüsselspeicherkenwort bei jedem Neustart der Appliance erneut eingegeben werden. Bis dies geschehen ist, sind sicheres Peering und Komprimierung deaktiviert.

**Enthält die Citrix SD-WAN WANOP-Appliance, die ich von Citrix erhalten habe, Schlüssel und ein Zertifikat zur Einrichtung eines sicheren Tunnels?**

Nein. Citrix SD-WAN WANOP-Produkte werden ohne die erforderlichen Schlüssel und Zertifikate für den SSL-Signaltunnel ausgeliefert. Sie müssen sie selbst generieren.

## SSL-Beschleunigung

April 19, 2021

### Verwendet die Beschleunigung einen Tunnel?

Nein, die Beschleunigung ist transparent und verwendet dieselben IP-Adressen und Portnummern wie die ursprüngliche Verbindung. Dadurch können Ihre aktuellen Überwachungsmethoden weiterhin normal funktionieren.

### Wie ändert die Beschleunigung den Paketstrom?

Bei nicht komprimierten Verbindungen fügt die Beschleunigung dem TCP-Header des Pakets Optionen hinzu, lässt jedoch die Paketnutzlast intakt. Diese Optionen ermöglichen es den Citrix SD-WAN WANOP-Geräten an jedem Ende der Verbindung, miteinander zu kommunizieren. Darüber hinaus wird die TCP-Sequenznummer angepasst, um zu verhindern, dass Routingprobleme oder Appliance-Fehler beschleunigte Pakete und nicht beschleunigte Pakete in derselben Verbindung mischen.

Bei komprimierten Verbindungen wird natürlich die Nutzlast komprimiert und der Ausgang des Kompressors wird in Full-Size-Pakete akkumuliert. Das Ergebnis ist, dass beispielsweise die 3:1-Komprimierung dazu führt, dass ein Drittel so viele Pakete übertragen werden, anstatt die gleiche Anzahl von Paketen, die jeweils auf ein Drittel reduziert werden. Die Komprimierung verwendet auch Citrix SD-WAN WANOP TCP-Header-Optionen und die Anpassung der Sequenznummer.

### Was sind die grundlegenden Anforderungen der Beschleunigung?

Die Beschleunigung erfordert ein Citrix SD-WAN WANOP-Gerät an beiden Enden der Verbindung, die Verbindung muss das TCP-Protokoll verwenden und alle Pakete für die Verbindung müssen beide Citrix SD-WAN WANOP-Geräte durchlaufen.

## Citrix SD-WAN WANOP-Plug-In

April 19, 2021

### Welche Methoden kann ich verwenden, um das Citrix SD-WAN WANOP-Plug-In auf meinem Computer zu installieren?

Sie können eine der folgenden Methoden verwenden, um das Citrix SD-WAN WANOP-Plug-In auf Ihrem Computer zu installieren:

- Eigenständige Installation: Führen Sie die Microsoft Installer (msi) -Datei aus.
- Automatische Installation: Führen Sie den folgenden Befehl aus:  

```
> msiexec.exe /i Pfad\Citrixsd-WanwanopPluginReleaseEx64- <Release_Nunmer> /qn
```

- Remote-Installation: Installieren Sie das Citrix SD-WAN WANOP-Plug-in remote von Citrix Receiver. Diese Installation erfolgt über den Merchandising-Server.

**Kann ich das Citrix SD-WAN WANOP Plug-in-Installationsprogramm anpassen?**

Ja. Sie können die signalisierende IP-Adresse und die Disc-basierte Komprimierungsgröße (DBC) mit der MSI-Datei für das Citrix SD-WAN WANOP-Plug-In anpassen.

**Was sind die Mindestanforderungen für die Hardware für die Installation des Citrix SD-WAN WANOP Plug-ins?**

Für das Citrix SD-WAN WANOP-Plug-in sollte Ihr Computer die folgenden Anforderungen erfüllen:

- Pentium 4-Klasse CPU
- Mindestens 4 GB RAM
- Mindestens 2 GB freier Festplattenspeicher

**Auf welchen Betriebssystemen kann ich das Citrix SD-WAN WANOP-Plug-In installieren?**

Sie können das Citrix SD-WAN WANOP-Plug-In unter folgenden Betriebssystemen installieren:

---

Betriebssystem	Ausgabe	Version
Windows XP	Wohnsitz, Professionell	32 Bits
Windows Vista	Home Basic, Home Premium, Business, Enterprise und Ultimate	32 Bits
Windows 7	Home Basic, Home Premium, Business, Enterprise und Ultimate	32 Bit, 64 Bit
Windows 8	Professionell, Unternehmen	32-Bit, 64-Bit
Windows 10	Professionell, Unternehmen	32 Bit, 64 Bit

---

**Welche Vorsichtsmaßnahmen sollte ich vor der Installation des Citrix SD-WAN WANOP Plug-Instreffen?**

Bevor Sie das Citrix SD-WAN WANOP-Plug-In auf Ihrem Computer installieren, treffen Sie die folgenden Vorsichtsmaßnahmen:

- Laden Sie je nach Betriebssystemversion entweder die 32-Bit- oder 64-Bit-Citrix SD-WAN WANOP-Installationsversion herunter.
- Sie können das Citrix SD-WAN WANOP-Plug-In nicht auf einem komprimierten Laufwerk oder Ordner installieren.

- Stellen Sie sicher, dass der Computer über ausreichend freien Speicherplatz verfügt.
- Sie können das Citrix SD-WAN WANOP-Plug-in-Release nicht herunterstufen. Wenn Sie eine frühere Citrix SD-WAN WANOP-Version verwenden möchten, müssen Sie die aktuelle Version deinstallieren und dann eine frühere Version installieren.

#### **Welche Citrix SD-WAN WANOP-Appliances unterstützen das Citrix SD-WAN WANOP Plug-in?**

Die folgenden Citrix SD-WAN WANOP-Appliances unterstützen das Citrix SD-WAN WANOP-Plug-in:

- SD-WAN WANOP
- SD-WAN WANOP 2000-Appliance mit Windows Server
- SD-WAN WANOP 3000
- SD-WAN WANOP 4000
- SD-WAN WANOP 5000

#### **Welche Citrix SD-WAN WANOP-Appliances unterstützen das Citrix SD-WAN WANOP Plug-in nicht?**

Die folgenden Citrix SD-WAN WANOP-Appliances unterstützen das Citrix SD-WAN WANOP-Plug-In nicht:

- SD-WAN WANOP 400
- SD-WAN WANOP 700
- SD-WAN WANOP 800
- SD-WAN WANOP 1000 mit Windows Server

#### **Muss ich eine Concurrent (CCU) -Lizenz auf Citrix SD-WAN WANOP 2000, 3000 und VPX Appliances installieren, um das Citrix SD-WAN WANOP-Plug-In verwenden zu können?**

Ja. Sie müssen eine CCU-Lizenz auf Citrix SD-WAN WANOP 2000, 3000 und VPX Appliances installieren, um das Citrix SD-WAN WANOP-Plug-In verwenden zu können.

#### **Muss ich eine CCU-Lizenz auf Citrix SD-WAN WANOP 4000 und 5000 Appliances installieren, um das Citrix SD-WAN WANOP-Plug-in verwenden zu können?**

Nein. Sie müssen keine CCU-Lizenz auf Citrix SD-WAN WANOP 4000 und 5000 Appliances installieren, um das Citrix SD-WAN WANOP-Plug-In verwenden zu können. Die Basislizenz der Appliance reicht aus, damit das Citrix SD-WAN WANOP-Plug-in eine Verbindung mit diesen Appliances herstellen kann.

#### **Was sind die Citrix Empfehlungen für die Beschleunigung von Subnetzen?**

Citrix empfiehlt Folgendes für die Beschleunigung von Subnetzen:

- Verwenden Sie niemals ALL/ALL für die Beschleunigungskonfiguration. Geben Sie die Subnetze auf der Grundlage der Anforderungen an.

- Konfigurieren Sie keine Beschleunigung für die Citrix Gateway VIP-Adresse.

**Wird das Citrix SD-WAN WANOP-Plug-in auf Windows Thin Clients unterstützt?**

Nein. Das Citrix SD-WAN WANOP-Plug-in wird auf Windows Thin Clients nicht unterstützt.

**Welche Releases von Citrix Receiver und Citrix Gateway werden mit dem Citrix SD-WAN WANOP Plug-in unterstützt?**

Das Citrix SD-WAN WANOP Plug-In unterstützt Citrix Receiver 4.1 und Citrix Gateway 10.5 Releases.

**Welche Citrix SD-WAN WANOP-Funktionen werden mit dem Citrix SD-WAN WANOP Plug-in nicht unterstützt?**

Das Citrix SD-WAN WANOP-Plug-In unterstützt die folgenden Citrix SD-WAN WANOP-Funktionen nicht:

- Video-Caching
- Traffic Shaping
- IPv6

**Muss ich Beschleunigungsregeln für eine Citrix SD-WAN WANOP 4000- oder 5000-Appliance konfigurieren, damit das Citrix SD-WAN WANOP Plug-in damit funktioniert?**

Ja. Sie müssen Beschleunigungsregeln auf einer Citrix SD-WAN WANOP 4000- oder 5000-Appliance konfigurieren, damit das Citrix SD-WAN WANOP-Plug-in damit funktioniert.

**Welche Bedeutung hat die Signalkanalquellenfilterung?**

Mithilfe der Signalkanalquellenfilterung können Sie einem bestimmten Subnetz oder einer IP-Adresse die Verbindung mit der Appliance zulassen oder verweigern und Beschleunigungsregeln abrufen. Das verweigernte Quellsubnetz kann keine Signalverbindungen herstellen und den Datenverkehr beschleunigen.

**Was ist die Bedeutung der LAN-Erkennung?**

Wenn Sie die LAN-Erkennung aktivieren, wird die Verkehrsbeschleunigung verhindert, wenn sich das Citrix SD-WAN WANOP-Plug-in und die Appliance im selben LAN befinden. Lokale Beschleunigung ist nicht wünschenswert, da das Anwenden der Bandbreitengrenze der Appliance auf die lokale Verbindung die Geschwindigkeit des lokalen Datenverkehrs verringert.

**Um den Datenverkehr zu beschleunigen, wie hoch ist der empfohlene RTT-Mindestwert zwischen dem Citrix SD-WAN WANOP Plug-In und der Appliance?**

Citrix empfiehlt, einen RTT-Wert zu konfigurieren, der größer ist als jeder RTT (Ping-Zeit) im lokalen LAN, aber kleiner als der RTT für einen Remotebenutzer ist. Der Standardwert von 20 Millisekunden ist für die meisten Netzwerke ausreichend.

### **Welche Bedingungen muss ich bei der Definition von Beschleunigungsregeln für das Citrix SD-WAN WANOP-Plug-in berücksichtigen?**

Berücksichtigen Sie beim Definieren von Beschleunigungsregeln für das Citrix SD-WAN WANOP Plug-in die folgenden Bedingungen:

- Definieren Sie Beschleunigungsregeln für alle Subnetze, die lokal auf der Appliance sind. Diese Subnetze sind die LAN-Subnetze an der Stelle, an der die Appliance installiert ist.
- Wenn Ziel-IP-Adressen vorhanden sind, die nicht Teil des LAN sind, fügen Sie Ausschlussregeln für diese IP-Adressen hinzu. Stellen Sie sicher, dass die Regeln zum Ausschließen von IP-Adressen den Regeln für die Beschleunigung des Datenverkehrs für Subnetze vorausgehen. Dazu gehören Subnetze an Remote-Standorten mit lokalen IP-Adressen.
- Wenn Sie die Appliance im Inlinemodus mit einem VPN installiert haben und sie im transparenten Modus betrieben wird, können Sie die Appliance so konfigurieren, dass der gesamte Unternehmensdatenverkehr beschleunigt wird, nicht nur der Datenverkehr, der von der lokalen Site stammt oder für diesen bestimmt ist. In diesem Fall bestehen die einzigen beschleunigten Verbindungen zwischen dem Citrix SD-WAN WANOP-Plug-In und VPN. Die Beschleunigung des Datenverkehrs zwischen dem Citrix SD-WAN WANOP Plug-in und dem VPN ist optimal.

### **Wo werden die Absturz- und Ablaufverfolgungsdateien des Citrix SD-WAN WANOP-Plug-ins auf dem Computer gespeichert?**

Die Absturz- und Trace-Dateien des Citrix SD-WAN WANOP-Plug-ins werden in den folgenden Ordnern gespeichert:

- Absturzdateien: C:/ProgramFiles/Citrix/Citrix SD-WAN WANOP
- Ablaufverfolgungsdateien: C:/Users/admin/AppData/Local/Temp

### **Wie stellt das Citrix SD-WAN WANOP Plug-in eine Verbindung zu einem Hochverfügbarkeitspaar her?**

Das Citrix SD-WAN WANOP-Plug-In stellt immer eine Verbindung mit derselben Signalisierungs-IP-Adresse her. Die signalgebende IP-Adresse ist nur an die primäre Appliance des Hochverfügbarkeitspaares gebunden, nicht an die sekundäre Appliance. Daher stellt das Citrix SD-WAN WANOP-Plug-In immer eine Verbindung mit der primären Appliance des Hochverfügbarkeitspaares her.

### **Welche Bereitstellungsmodi unterstützt das Citrix SD-WAN WANOP-Plug-In?**

Das Citrix SD-WAN WANOP-Plug-In unterstützt die folgenden Bereitstellungsmodi:

- Inline.
- WCCP:
- Hohe Verfügbarkeit.

- Citrix SD-WAN WANOP-Plugin mit NAT-Bereitstellung.
- Citrix SD-WAN WANOP-Plug-in mit Citrix SD-WAN WANOP-Appliance im WCCP-Modus unter Verwendung von ICA-Proxy.
- Citrix SD-WAN WANOP-Plugin mit Citrix SD-WAN WANOP 4000 oder 5000 Appliance. Bei dieser Bereitstellung ist der Management-Port (0/1) mit dem Verwaltungsnetzwerk verbunden, und die signalisierende IP-Adresse befindet sich in einem anderen Netzwerk.

### Wie fließen Pakete in Transparent- und Redirector-Modi?

Im transparenten Modus ändert die Citrix SD-WAN WANOP-Appliance nicht die Quell-IP-Adresse des Pakets. Im Redirector-Modus unterstützt die Citrix SD-WAN WANOP Appliance Server und ändert die IP-Adresse der Pakete.

#### Hinweis

Citrix empfiehlt den transparenten Modus für die Produktionsbereitstellung.

### Wie kann ich einen sicheren Tunnel zwischen dem Citrix SD-WAN WANOP-Plug-in und der Appliance einrichten?

Gehen Sie folgendermaßen vor, um einen sicheren Tunnel zwischen dem Citrix SD-WAN WANOP-Plug-In und der Appliance einzurichten:

1. Öffnen Sie auf der Benutzeroberfläche des Citrix SD-WAN WANOP-Plug-ins die Registerkarte **Zertifikate**.
2. Wählen Sie die Option **Zertifizierungsstellenzertifikat** aus.
3. Klicken Sie auf **Importieren** und laden Sie das entsprechende CA-Zertifikat hoch.
4. Wählen Sie einen Zertifikatspeicher aus, in dem Sie das Zertifikat speichern möchten.
5. Wählen Sie die Option **Clientzertifikat** aus.
6. Klicken Sie auf **Importieren**.
7. Wählen Sie die entsprechenden Zertifikatsformate aus und laden Sie die entsprechenden Zertifikate hoch.
8. Speichern Sie die Zertifikate in einem Zertifikatspeicher.
9. Wenn der private Schlüssel kennwortgeschützt ist, geben Sie das Kennwort ein, um den privaten Schlüssel zu entschlüsseln.
10. Sie müssen dasselbe CA-Zertifikat und dasselbe Schlüsselpaar auf die Appliance hochladen, um einen sicheren Tunnel einzurichten.

### Wie kann ich überprüfen, ob ein sicherer Tunnel eingerichtet ist?

Gehen Sie folgendermaßen vor, um zu überprüfen, ob ein sicherer Tunnel eingerichtet ist:



1. Der Computer, auf dem Sie das Citrix SD-WAN WANOP-Plug-In installiert haben, führen Sie den folgenden Befehl aus:

> *Telnet localhost 1362*

2. Führen Sie auf der Konsole den folgenden Befehl aus:

> *Showtunnels*

Es folgt Beispielausgabe des Befehls. Wenn die Ausgabe den Text sicher im Abschnitt Verbunden verfügbar enthält, wurde ein sicherer Tunnel eingerichtet. Wenn kein sicherer Tunnel eingerichtet ist, wird im Text *Klartext* angezeigt.

```
1  ```\n2  Showtunnels\n3  Message Tunnels:\n4      Connected Available:\n5      172.16.9.100 auto,secure,client,initiator,configured\n6      CN: mike.199.130\n7\n8\n9  Connected Available : 1\n10 Clients: 1 peers: 0\n11 <!--NeedCopy--> ```\n
```

Weitere Informationen zum Citrix SD-WAN WANOP-Plug-in finden Sie unter [Citrix SD-WAN WANOP Plug-in] (/en-us/citrix-sd-wan-wanop/10-2/wanopt-plugin.html).

## Traffic Shaping

April 19, 2021

### Was ist Citrix SD-WAN WANOP Traffic Shaping?

Citrix SD-WAN WANOP Traffic Shaping verwendet eine Gruppe von Richtlinien, um die Priorität des unterschiedlichen Link-Datenverkehrs festzulegen und Traffic mit einer Rate nahe der Verbindungsgeschwindigkeit auf die Verbindung zu senden. Im Gegensatz zu Beschleunigung, die nur für TCP/IP-Datenverkehr gilt, verarbeitet der Traffic Shaper den gesamten Datenverkehr auf der Verbindung.

### Was ist der Vorteil der Traffic Shaping?

Traffic Shaping verwendet knappe Link-Ressourcen gemäß den von Ihnen festgelegten Richtlinien, so dass Datenverkehr, der als wichtig bekannt ist, mehr Bandbreite erhalten als Datenverkehr, der als unwichtig bekannt ist.

### Wie interagiert der Datenverkehrsformer mit Citrix Virtual Apps and Desktops Datenverkehr?

Das Citrix SD-WAN WANOP-Gerät analysiert den Datenstrom Virtual Apps/Virtual Desktops und ist sich der verschiedenen Arten von Datenverkehr und seinen Prioritäten bewusst, um Datenverkehr mit hoher Priorität zu begünstigen. Es ist das einzige Produkt, das verschlüsselte ICA-Streams priorisieren kann und native Unterstützung für MultiStream ICA bietet, die die Sitzung eines Benutzers in bis zu vier Verbindungen mit unterschiedlichen Prioritäten unterteilt.

### **Was ist gewichtete faire Warteschlange?**

Eine Citrix SD-WAN WANOP-Appliance verwendet gewichtete Fair Queuing, die für jede Verbindung eine separate Warteschlange bietet. Mit Fair Queuing kann eine zu schnelle Verbindung nur ihre eigene Warteschlange überlaufen. Es hat keine Auswirkungen auf andere Verbindungen.

### **Was ist der Unterschied zwischen gewichteter und nicht gewichteter Fair Queuing?**

Die gewichtete faire Warteschlange beinhaltet die Möglichkeit, einigen Traffic eine höhere Priorität (Gewicht) zu geben als andere. Traffic mit einem Gewicht von zwei erhält die doppelte Bandbreite des Traffic mit einem Gewicht von eins. In einer Citrix SD-WAN WANOP-Konfiguration werden die Gewichtungen in Traffic-Shaping-Richtlinien zugewiesen.

### **Was ist eine Linkdefinition?**

Eine Linkdefinition gibt an, welcher Datenverkehr mit der definierten Verbindung verknüpft ist, die maximale Bandbreite für den empfangenen Datenverkehr auf der Verbindung und die maximale Bandbreite für den über die Verbindung gesendeten Datenverkehr. Die Definition identifiziert außerdem den Datenverkehr als ein- oder ausgehender und als WAN-seitiger oder LAN-seitiger Datenverkehr.

### **Welche Vorteile bietet die Link-Definition?**

Verknüpfungsdefinitionen ermöglichen es der Appliance, Überlastung und Verlust Ihrer WAN-Verbindungen zu verhindern und Traffic Shaping durchzuführen. Die Definition identifiziert außerdem den Datenverkehr als ein- oder ausgehender und als WAN-seitiger oder LAN-seitiger Datenverkehr. Der gesamte Datenverkehr, der durch die Appliance fließt, wird mit der Liste der Verknüpfungsdefinitionen verglichen, und die erste übereinstimmende Definition identifiziert den Link, zu dem der Datenverkehr gehört.

### **Ich habe keine Dienstklasse mit Standardrichtlinie konfiguriert. In den Traffic Shaping Berichten wird jedoch ein großer Datenverkehr angezeigt, der durch die Standardrichtlinie dargestellt wird. Habe ich etwas falsch konfiguriert?**

Nein. Es gibt kein Problem mit Ihrer Konfiguration. Traffic Shaping ist nur für die WAN-Verbindung anwendbar. Der Datenverkehr im LAN oder einer anderen Verbindung wird durch die Standardrichtlinie dargestellt.

Betrachten Sie beispielsweise eine Konfiguration, bei der Sie eine Dienstklasse erstellen, z. B. Management\_Service\_Class, die das Verwaltungssubnetz als Ziel-IP-Adresse aufweist, und Sie binden eine benutzerdefinierte Traffic Shaping-Richtlinie an diese Dienstklasse. Wenn in diesem Fall kein Datenverkehr auf WAN vorhanden ist, können Sie feststellen, dass der Verwaltungsdatenverkehr im Service-

Class-Bericht als Management\_Service\_Class klassifiziert wird. Im Bericht Traffic Shaping Policy sind jedoch weiterhin Einträge für die Standardrichtlinie vorhanden, die Sie als benutzerdefinierte Traffic Shaping Policy erwarten.

Im Bericht Traffic Shaping Policy verwendet die Appliance keine benutzerdefinierte Traffic Shaping-Richtlinie für die Management\_Service\_Class-Richtlinie und wendet die Standardrichtlinie an. Um diese Verwirrung zu vermeiden, können Sie die Option Alle anderen deaktivieren oder den LAN-Typ-Link für die Verwaltungsschnittstelle definieren.

## **Upgrade-Prozess (OS)**

April 19, 2021

### **Das neue WANOP OS Kernel-Upgrade wird von welcher SD-WAN-Version unterstützt?**

Citrix SD-WAN Version 10.1 und höher.

### **Wird das neue Betriebssystem auf allen SD-WAN-Plattformen unterstützt?**

Ja. Das Betriebssystem-Upgrade wird auf allen SD-WAN WANOP (VPX, Physical, Cloud) und Premium/Enterprise Edition-Appliances unterstützt.

### **Was sind die WANOP VPX-Profilen (RAM/Disk/vCPU), die mit Release 10.1 unterstützt werden?**

- 6 GB RAM, 100 GB Festplatte und 2 vCPUs
- 6 GB RAM, 250 GB Festplatte und 2 vCPUs
- 8 GB RAM, 500 GB Festplatte und 4 vCPUs
- 16 GB RAM, 500 GB Festplatte und 4 vCPUs

### **Was sind die wichtigsten Unterschiede zwischen WANOP mit Version 10.0 oder niedriger im Vergleich zu 10.1?**

Feature	10.0 oder früher	10.1 oder höher	Anmerkungen
Unterstützung für Video-Caching auf WANOP	unterstützt	Nicht unterstützt	Ohne
Minimale RAM-Anforderung für WANOP VPX	4 GB RAM	6 GB RAM	Ohne
WANOP VPX-Bereitstellungsassistent	unterstützt	Nicht unterstützt	Ohne
Primäre /APA Adapter-Management-IP-Adresse für WANOP VPX	DHCP ist standardmäßig deaktiviert	DHCP ist standardmäßig aktiviert	Ohne
Upgradeunterstützung für vorhandenes WANOP VPX auf Citrix Hypervisor	unterstützt	nicht unterstützt. Frisches SD-WAN 10.1 XVA-Images sollte importiert werden	Ohne
Upgradeunterstützung auf physischen WANOP-Plattformen mit Citrix Hypervisor 6.0 Hypervisor-Version (Plattformen, die mit Werksversionsbasisimage 7.2.2 oder früher ausgeliefert werden, verwenden Citrix Hypervisor Version 6.0) Release 10.1	unterstützt	Sie müssen ein Upgrade Citrix Hypervisor auf Version 6.5 durchführen (mit WANOP Citrix Hypervisor 6.5-Upgradepaket) und dann ein WANOP 10.1-Upgrade durchführen.	Durch Klicken auf "Configuration" wird Citrix Hypervisor-Version angezeigt.

**Das Upgrade von WANOP VPX, das auf dem eigenständigen Citrix Hypervisor ausgeführt wird (mit WO-Build 10.0 oder früher) auf Version 10.1 wird unterstützt, falls nicht, warum?**

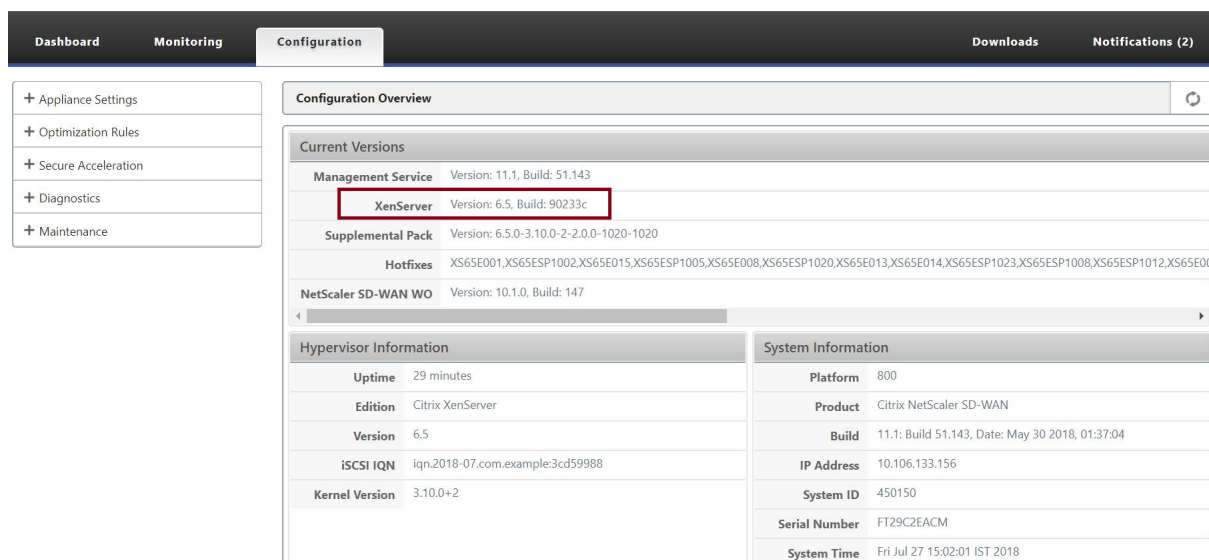
Dieses Upgrade wird aufgrund der PV-zu-HVM-Konvertierung nicht unterstützt. Sie müssen ein neues SD-WAN-Release auf 10.1 Citrix Hypervisor WANOP VPX über das XVA-Image bereitstellen.

## Upgrade von WANOP VPX läuft auf eigenständigen ESXi/Hyper-V (mit WO Build 10.0 oder früher) auf 10.1 Version wird unterstützt, Wenn nicht, warum?

Dieses Upgrade wird unterstützt. Bitte beachten Sie vor dem Upgrade die Änderungen der neuen RAM-Ressourcenanforderungen.

## Upgrade von WANOP auf physische Appliance (mit WANOP Build 10.0 oder früher) auf 10.1 Version wird unterstützt, Wenn nicht, warum?

Dieses Upgrade wird unterstützt. Voraussetzung für dieses Upgrade ist, dass der Host-Citrix Hypervisor (auf einem physischen SD-WAN-Gerät) Citrix Hypervisor Version 6.2 / 6.5 oder höher hat. Dies kann über die Registerkarte **Konfiguration** überprüft werden.



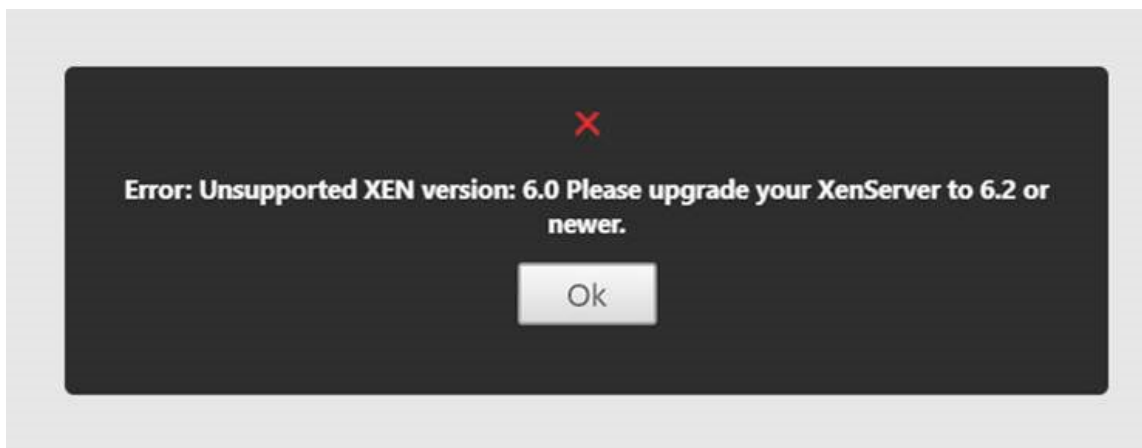
The screenshot displays the 'Configuration Overview' page in the Citrix SD-WAN WANOP interface. The page is divided into several sections:

- Current Versions:**
  - Management Service: Version: 11.1, Build: 51.143
  - XenServer: Version: 6.5, Build: 90233c** (highlighted with a red box)
  - Supplemental Pack: Version: 6.5.0-3.10.0-2-2.0.0-1020-1020
  - Hotfixes: XS65E001,XS65ESP1002,XS65E015,XS65ESP1005,XS65E008,XS65ESP1020,XS65E013,XS65E014,XS65ESP1023,XS65ESP1008,XS65ESP1012,XS65E00
  - NetScaler SD-WAN WO: Version: 10.1.0, Build: 147
- Hypervisor Information:**
  - Uptime: 29 minutes
  - Edition: Citrix XenServer
  - Version: 6.5
  - iSCSI IQN: iqn.2018-07.com.example:3cd59988
  - Kernel Version: 3.10.0+2
- System Information:**
  - Platform: 800
  - Product: Citrix NetScaler SD-WAN
  - Build: 11.1: Build 51.143, Date: May 30 2018, 01:37:04
  - IP Address: 10.106.133.156
  - System ID: 450150
  - Serial Number: FT29C2EACM
  - System Time: Fri Jul 27 15:02:01 IST 2018

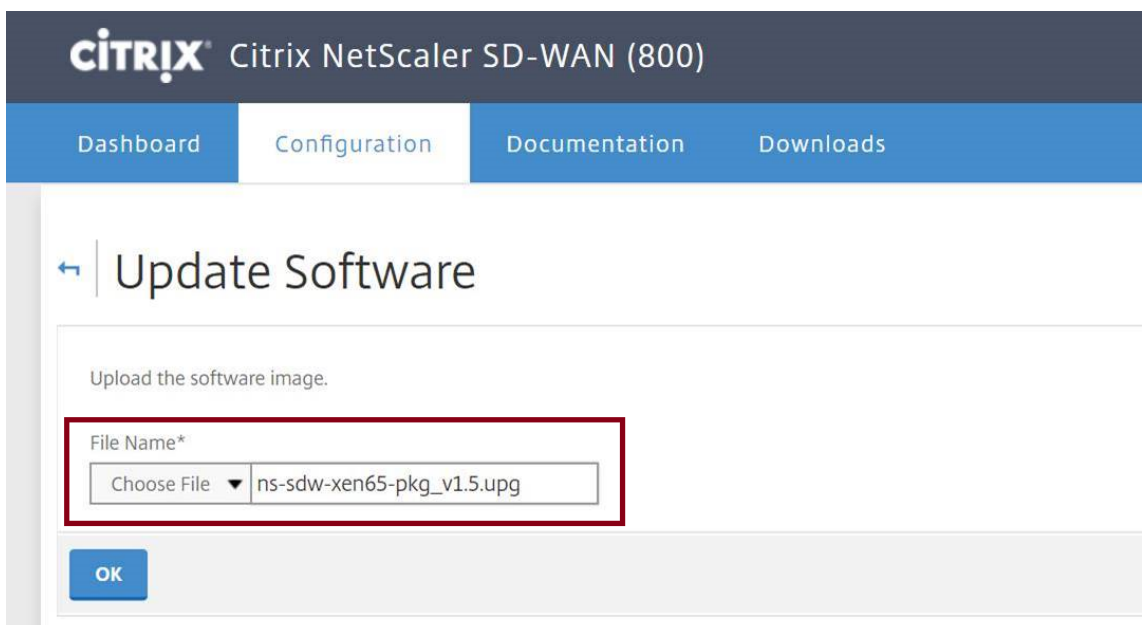
## Was muss der Benutzer ausführen, wenn das physische WANOP-Gerät nicht mit Citrix Hypervisor 6.2/6.5 oder höher ausgeführt wird?

Führen Sie ein Upgrade Citrix Hypervisor aus, bevor Sie die SD-WAN WO-Version aktualisieren. In diesem Anwendungsfall könnte beispielsweise ein Upgrade der SD-WAN 800-WANOP-Plattform mit Version 7.2.2 geplant werden (eine Version mit Citrix Hypervisor 6.0).

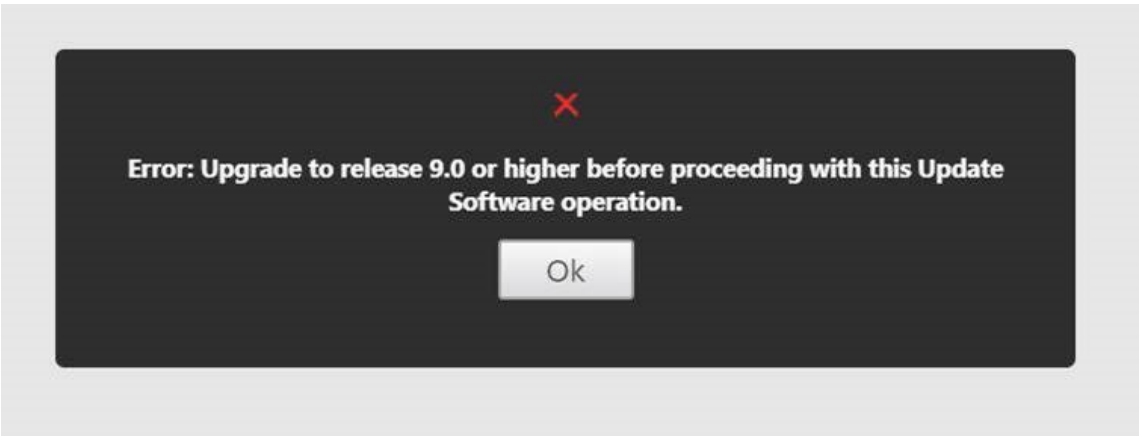
1. Beim Upgrade dieser Appliance auf Version SD-WAN 10.1 tritt die folgende Fehlermeldung auf.



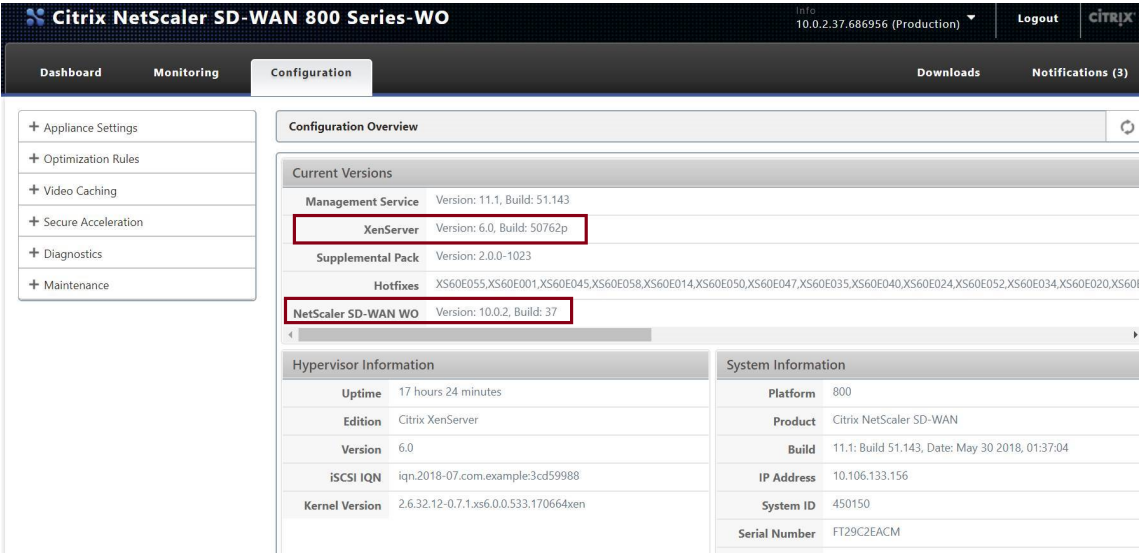
2. Führen Sie Citrix Hypervisor mit “ns-sdw-xen65-pkg\_v1.5.upg” ein Upgrade auf 6.5 durch (diese Datei kann von Citrix-Downloadwebsite heruntergeladen werden).



3. Wenn SD-WAN WO die Version 9.0 oder höher nicht hat, wird kein Upgrade auf Citrix Hypervisor 6.5 durchführen. Die folgende Fehlermeldung wird angezeigt.



4. Nehmen wir an, der Benutzer hat die WO-Version jetzt auf 10.0.2 aktualisiert.



5. Führen Sie nun das Upgrade Citrix Hypervisor mit “ns-sdw-xen65-pkg\_v1.5.upg” auf 6.5 durch.



Upgrade in progress...

1/1

Upgrading XEN...

Time remaining 20 minutes

Upgrade successfully completed.

Ok

Citrix NetScaler SD-WAN 800 Series-WO

10.0.2.37:686956 (Production)

Logout

CITRIX

Dashboard

Monitoring

Configuration

Downloads

Notifications (2)

+ Appliance Settings

+ Optimization Rules

+ Video Caching

+ Secure Acceleration

+ Diagnostics

+ Maintenance

Configuration Overview

Current Versions

Management Service	Version: 11.1, Build: 51.143
XenServer	Version: 6.5, Build: 90233c
Supplemental Pack	Version: 6.5.0-3.10.0-2-2.0.0-1020-1020
Hotfixes	XS65E001,XS65ESP1002,XS65E015,XS65ESP1005,XS65E008,XS65ESP1020,XS65E013,XS65E014,XS65ESP1023,XS65ESP1008,XS65ESP1012,XS65
NetScaler SD-WAN WO	Version: 10.0.2, Build: 37

Hypervisor Information

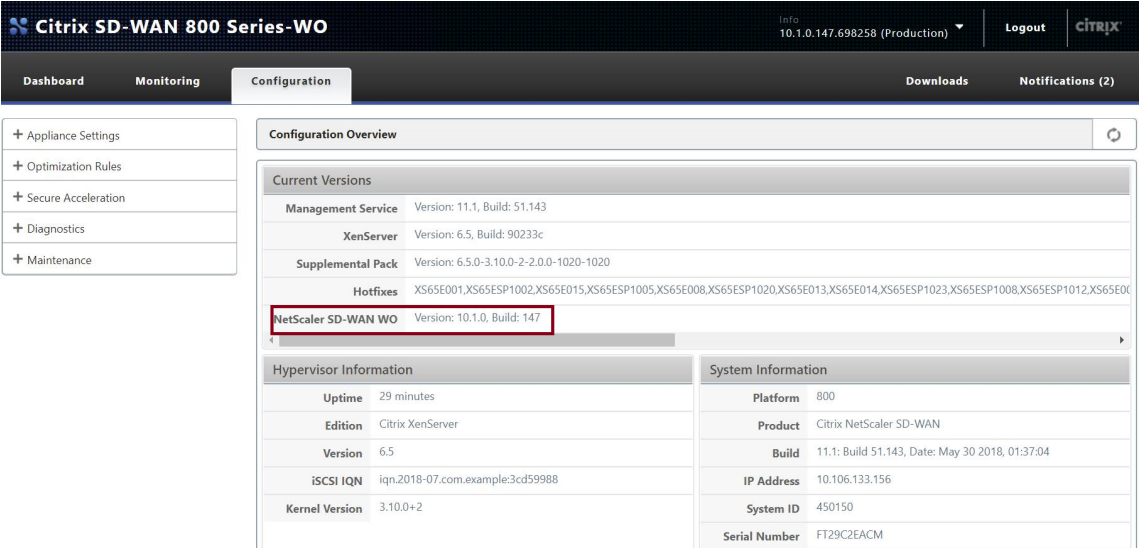
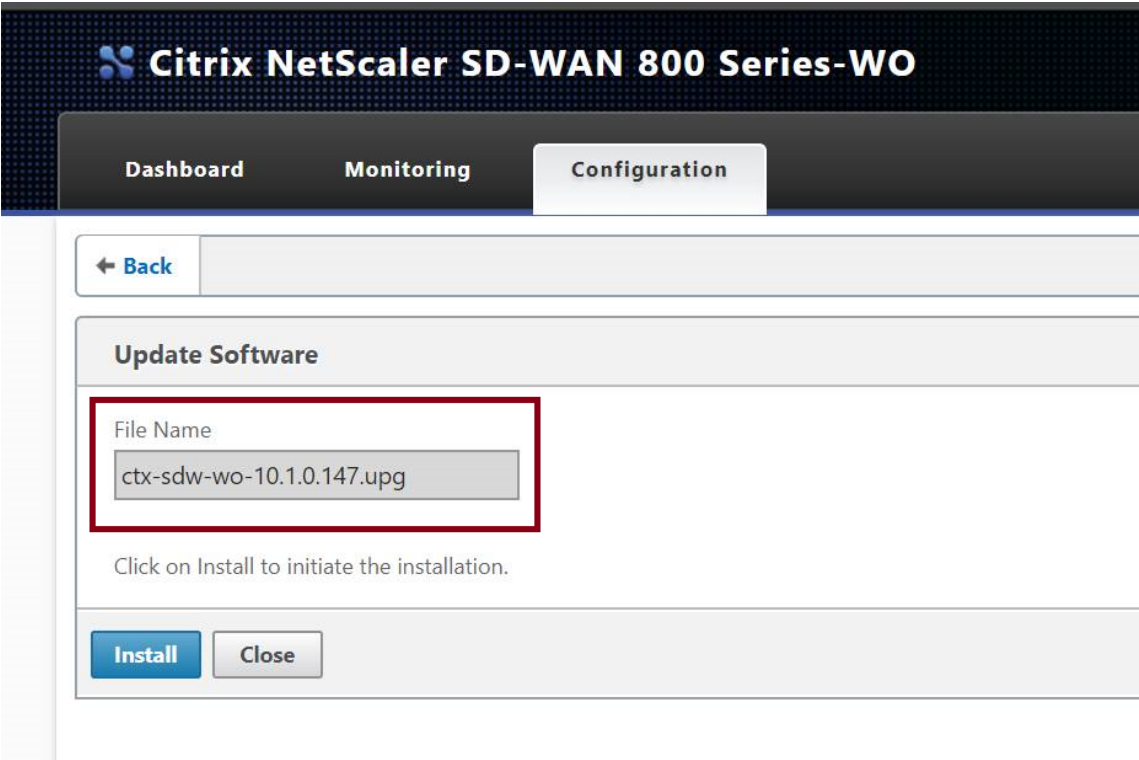
Uptime	5 minutes
Edition	Citrix XenServer
Version	6.5
iSCSI IQN	iqn.2018-07.com.example:3cd59988
Kernel Version	3.10.0+2

System Information

Platform	800
Product	Citrix NetScaler SD-WAN
Build	11.1: Build 51.143, Date: May 30 2018, 01:37:04
IP Address	10.106.133.156
System ID	450150
Serial Number	FT29C2EACM
System Time	Fri Jul 27 14:38:00 IST 2018

6. Aktualisieren Sie jetzt SD-WAN auf Version 10.1.





**Client zu Server ICMP Ping funktioniert einwandfrei, aber TCP-Datenverkehr geht nicht über die WANOP VPX-Appliance (Deaktivierung der WANOP-Datenverarbeitung funktioniert einwandfrei)?**

Überprüfen Sie die Firewall-Einstellungen auf Client, Server und Router.  
Wenn WANOP VPX oder Client/Server als VM gehostet werden, stellen Sie sicher, dass die Prüfsumme auf der Endhost-VM deaktiviert ist.

```
1 Beispiel für Linux-Befehle:  
2 ethtool -K eth0 tx off  
3 ethtool -K eth0 rx off  
4 ethtool --offload eth0 tx off  
5 ethtool --offload eth0 rx off
```

Aktivieren Sie den Parameter `Checksum.SendForceSW` auf beiden WO VPXs sollte ON sein.

```
1 Beispiel:  
2 Checksum.SendForceSW on
```

## **Gibt es Änderungen am SDWAN SE/EE/WO Appliance-Upgrade-Prozess aufgrund des neuen WO OS Kernel?**

Nr.

## **Video-Caching**

April 19, 2021

### **Wie unterscheidet sich das Video-Caching von der Datenträgerbasierten Komprimierung?**

Beim Caching wird eine lokale Kopie des zwischengespeicherten Objekts von der lokalen Appliance bereitgestellt, ohne es erneut vom Remoteserver herunterzuladen. Das Caching erfordert keine Appliance an beiden Enden des Links, nur am lokalen Ende. Bei Komprimierung wird eine Remote-Kopie des Objekts vom Remoteserver bereitgestellt. Die Remote-Appliance (serverseitig) komprimiert sie, verringert ihre Größe und erhöht damit ihre Übertragungsgeschwindigkeit, und die lokale (clientseitige) Appliance dekomprimiert sie.

Die Komprimierung funktioniert sowohl bei modifizierten als auch bei unveränderten Objekten. Wenn sich eine Datei auf dem Server um 1% ändert, erreicht die nächste Übertragung eine Komprimierung von bis zu 99:1.

Das Caching funktioniert nur bei unveränderten Objekten. Wenn sich eine Datei auf dem Server um 1% ändert, muss die neue Version vollständig heruntergeladen werden. Caching und Komprimierung sind komplementäre Technologien, da alles, was nicht zwischengespeichert wird, komprimiert wird, was die Vorteile beider ermöglicht.

### **Kann ich den gesamten Speicher der Appliance zwischen dem Video-Cache und anderen Citrix SD-WAN WANOP-Funktionen partitionieren?**

Nein. Die erforderliche Cache-Partition und der erforderliche Speicher sind nicht konfigurierbar.

### **Was sind die unterstützten Videocontainer-Formate?**

Video-Caching ist unabhängig vom Codec-Format und unterstützt alle gängigen Container-Formate.

### **Kann ich Caching für interne und externe Enterprise-Videos auf meinen eigenen Websites aktivieren?**

Ja. Wenn der Zugriff auf diese Videos über HTTP erfolgt, können Sie diese Websites für das Caching konfigurieren.

### **Kann ich die maximale Größe für ein zwischengespeichertes Objekt konfigurieren?**

Ja. Ein Objekt, das größer als der von Ihnen konfigurierte Grenzwert ist, wird nicht zwischengespeichert. Um dieses Limit festzulegen, navigieren Sie zu **Konfiguration > Optimierungsregeln > Video-Caching** und wählen Sie den Wert aus den verfügbaren Limits aus.

### **Wie verbessert das Video-Caching die Benutzererfahrung?**

Caching verbessert die Benutzererfahrung für Videos, die mehr als einmal angezeigt werden, insbesondere bei langsameren Links. Der erste Betrachter eines bestimmten Videostreams profitiert nicht von der Video-Caching-Funktion, aber nachfolgende Ansichten werden mit der LAN-Geschwindigkeit von der Citrix SD-WAN WANOP-Appliance bereitgestellt, mit dem zusätzlichen Vorteil einer reduzierten WAN-Nutzung.

Wenn ein zweiter Benutzer dasselbe Video anfordert, während es noch für den ersten Benutzer gestreamt wird, erhält der zweite Benutzer die zwischengespeicherte Kopie.

Im Gegensatz zum normalen Citrix SD-WAN WANOP-TCP-Betrieb, bei dem die Appliance die ursprünglichen Quell- und Ziel-IP-Adressen beibehält, ersetzt die Appliance die Quelladresse des Clients durch die IP-Adresse, die der beschleunigten Brücke zugewiesen ist, sodass der gesamte HTTP-Datenverkehr, der durch die Appliance geleitet wird, von der Appliance selbst.

### **Welche Citrix SD-WAN WANOP-Appliances unterstützen Video Caching?**

Die folgenden Appliances unterstützen die Video-Caching-Funktion:

- SD-WAN WANOP 800 Appliance mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 1000 Appliance mit Windows Server, mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 2000 Appliance mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 2000 Appliance mit Windows Server, mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 3000 Appliance mit allen Bandbreitenlizenzenmodellen.

### **Welche Bereitstellungsmodi werden für das Video-Caching auf einer Citrix SD-WAN WANOP-Appliance unterstützt?**

- Unterstützte Bereitstellung - Inline Virtual Inline, VLAN und WCCP

- Nicht unterstützte Funktionen - Citrix SD-WAN WANOP Hochverfügbarkeit, Gruppenmodi und Daisy Chaining

### **Welche Dateierweiterungen werden für Video-Caching unterstützt?**

Der Videodateiname muss eine der folgenden Erweiterungen haben: .3gp, .avi, .dat, .divx, .dix, .dv-avi, .flv, .fvm, .h264, .hdmov, .m15, .m1v, .m21, .m2a, .m2v, .m4e, .m4v, .m75, .moov, .mov, .movie, .mp21, .mp2v, .mp4, .mp4v, .mpe, .mpeg, .mpeg4, .mpg, .mpg2, .mpv, .mts, .ogg, .ogv, .qt, .qtm, .ra, .rm, .ram, .rmd, .rms, .rmvb, .rp, .rv, .swf, .ts, .vfw, .vob, .webm, .wm, .wma, .wmv, and .wtv.

### **Kann ich die Video-Caching-Funktion auf einer nicht unterstützten Citrix SD-WAN WANOP-Plattform aktivieren?**

Nein. Die Video-Caching-Funktion kann nicht auf nicht unterstützten Plattformen verwendet werden.

### **Was sind die Mindestkonfiguration und andere Voraussetzungen für die Aktivierung der Video-Caching-Funktion?**

Um die Video-Caching-Funktion zu aktivieren, müssen Sie:

- Weisen Sie der APA-Schnittstelle und, falls vorhanden, der APB-Schnittstelle eine gültige IP-Adresse und ein Gateway zu.
- Konfigurieren Sie auf der Appliance einen gültigen DNS-Server, der auf [www.citrix.com](http://www.citrix.com) aufgelöst werden kann.
- Mindestens eine Anwendung in der Liste Ausgewählte Video-Caching-Anwendungen.
- Prüfen Sie die Warnungen von Citrix SD-WAN WANOP GUI über vorhandene Konfigurationsalarme.

### **Kann das Citrix SD-WAN WANOP-Plug-In die Video-Caching-Funktion verwenden?**

Nein. Sie können die Video-Caching-Funktion nicht mit dem Citrix SD-WAN WANOP-Plug-In verwenden.

### **Was sind die unterstützten Browser und Geräte?**

Video-Caching unterstützt die Browser Internet Explorer, Firefox und Chrome. Videos können auf Windows 7 oder 8, Apple iPad und Android iOS-Geräten angezeigt werden.

### **Unterstützt die Citrix SD-WAN WANOP-Appliance Video-Caching für alle Video-Websites?**

Nein. Die Videowebsite ist verfügbar und in der Liste Unterstützte Anwendungen auf der Konfigurationsseite Video Caching hinzugefügt. Standardmäßig sind die unterstützten Anwendungen YouTube, Vimeo, Youku, Dailymotion und Metacafe. Sie können andere Websites hinzufügen, indem Sie ihre IP-Adressen angeben, wenn sie keine Caching-Vermeidungsmechanismen verwenden, z. B. das Hinzufügen von zufälligen Zeichen zu URLs.

**Wird die SNMP-Überwachung für Video-Caching unterstützt?**

Ja. Sie können SNMP-MIBs verwenden, um bestimmte Videozischenspeicheraufgaben zu überwachen.

**Wird Video-Caching für Nicht-HTTP-Datenverkehr unterstützt?**

Nein. Video-Caching wird nicht für Nicht-HTTP-Datenverkehr wie HTTPS, RTSP und RTMP unterstützt.

**Kann ich Video-Caching mit HTTP-Datenverkehr verwenden, der an einen anderen Port als Port 80 gesendet wird?**

Ja. Für die Videozischenspeicherung können Sie der Appliance benutzerdefinierte Ports hinzufügen. Um benutzerdefinierte Ports für die Videozischenspeicherung hinzuzufügen, navigieren Sie zur Seite **Konfiguration > Optimierungsregeln > Videozischenspeicherung** und klicken Sie auf der Registerkarte **Einstellungen auf den Link Globale Einstellungen**.

**Kann Citrix SD-WAN WANOP-Komprimierung (mit einer HTTP-Service-Class-Richtlinie) für Video-Caching verwendet werden?**

Ja. Wenn die zwischengespeicherten Objekte sowohl im Citrix SD-WAN WANOP-Komprimierungsverlauf als auch im Video-Cache vorhanden sind, wird der Inhalt bei einem Cache-Treffer aus dem Cache bereitgestellt und bei einem Cache-Miss vom Server abgerufen (und komprimiert).

**Erfordert eine vorhandene HTTP-Anwendung, die IP-Adresskonfiguration erfordert, wenn ein transparenter Proxy vorhanden ist, Änderungen?**

Ja. Citrix SD-WAN WANOP führt transparente HTTP-Proxying-Aktionen durch, bei denen es die Quell-IP-Adresse des Pakets ersetzt. Wenn die vorhandene HTTP-Anwendung bestimmte Richtlinien aufweist (z. B. bestimmte IP-Adressen oder Proxy-Mechanismen blockieren), müssen diese Richtlinien geändert werden.

**Was sind die Systemspeicher- und Verbindungsgrenzen für die HTTP-Proxy-Verbindung?**

Um die Grenzwerte zu bestimmen, überprüfen Sie die Diagramme und Statistiken auf der Debug-Seite Video Caching (support.html). Stellen Sie außerdem sicher, dass der Befehl VideoCaching.cmd stats info die folgenden Informationen anzeigt.

	SD-WAN WANOP 800	SD-WAN 1000 mit Widows Server	SD-WAN 2000 mit Widows Server	SD-WAN 2000	SD-WAN 3000
——	——	——	——	——	——
Datenträger	25 GB	25 GB	50 GB	50 GB	99 DE
RAM	375 MB	375 MB	700 MB	700 MB	1024 MB
Höchstwert für HTTP-Verbindungen insgesamt	1000	1000	1500	1500	3000
Maximale HTTP-Schreibgrenze	200	200	300		
300 | 600 |

Nachdem die oben genannten HTTP-Verbindungsgrenzen erreicht wurden, werden neue Verbindungen umgangen.

#### **Hinweis**

Stellen Sie sicher, dass Sie die oben genannte Konfiguration nicht ändern.

#### **Enthält die Überwachungsseite für Video-Caching nur Videoverkehr?**

Ja. Nicht-Video-HTTP-Datenverkehr (obwohl er vom Proxy abgefangen wird), ist nicht in der Video-Caching-GUI-Statistik enthalten.

#### **Muss ich sowohl ap- als auch aPb-Schnittstellen mit einer gültigen IP-Adresse auf einer Citrix SD-WAN WANOP-Appliance konfigurieren?**

Nein. Sie müssen den beiden Schnittstellen keine gültige IP-Adresse zuweisen. HTTP-Pakete, die von der APA-Schnittstelle empfangen werden, verwenden als Proxy die APA-IP-Adresse, und HTTP-Pakete, die von der APB-Schnittstelle empfangen werden, die APB-IP-Adresse.

Wenn Sie keine IP-Adresse für eine Schnittstelle konfigurieren, erhalten die auf dieser Schnittstelle empfangenen HTTP-Pakete keinen Caching-Vorteil.

#### **Was ist die Mindest- und Höchstgrenze für die Größe einer Videodatei, die zwischengespeichert werden kann?**

- Minimum: 100 KB
- Maximal: 300 MB
- Standard: 100 MB

#### **Wie wird der Video-Caching-Datenträger gelöscht?**

Cache-Objekte werden gemäß dem Algorithmus Least Recently Used gelöscht.

#### **Was passiert, wenn ich die Citrix SD-WAN WANOP-Appliance von Version 6.x auf 7.y upgrade und das Video-Caching aktiviert ist?**

Die vorhandene Citrix SD-WAN WANOP DBC-Historie geht verloren und eine separate Partition für das Video-Caching wird erstellt.

#### **Was passiert, wenn ich die Citrix SD-WAN WANOP-Appliance von Release 7.y auf 6.x herunterstufte und das Video-Caching aktiviert ist?**

Die Geschichte von Citrix SD-WAN WANOP DBC und Video Caching bleibt erhalten. Die Video-Caching-Funktion ist jedoch ab Version 6.x nicht verfügbar.

#### **Was passiert, wenn ich die Citrix SD-WAN WANOP-Appliance von Release 7.x auf 7.y aktualisiere und das Video-Caching aktiviert ist?**

Die Geschichte des Citrix SD-WAN WANOP DBC- und Video-Caching bleibt erhalten.

**Ich habe ein einziges Netzwerk in Zweigstellen, das sowohl ein Management als auch den Datenverkehr teilt. Wie kann ich das Video-Caching in diesem Netzwerk konfigurieren?**

Wenn Sie über ein einzelnes Netzwerk für Verwaltung und Datenverkehr verfügen, empfiehlt Citrix, die primäre IP-Adresse der LAN-Seite des Ports für beschleunigte Bridge-Ports hinzuzufügen.

**Wie hoch ist die maximale Anzahl von Vorbevölkerungsaufgaben, die ich gleichzeitig ausführen kann?**

Eins. Wenn Sie versuchen, mehrere Vorbevölkerungsaufgaben gleichzeitig zu starten, erstellt die Appliance eine Warteschlange mit Aufgaben auf einer ersten Basis.

**Wie hoch ist die maximale Anzahl von Videoquellen, die ich auf der Appliance konfigurieren kann?**

100

**Wie hoch ist die maximale Anzahl von Vorbevölkerungseinträgen, die ich zur Appliance hinzufügen kann?**

50

**Wie hoch ist die maximale Anzahl von Videodateien, die aus einem Verzeichnis aufgelisteten Ordner heruntergeladen und zwischengespeichert werden?**

300

**Hat das von der Vorbevölkerungsfunktion initiierte Videodownload und -zwischenspeicherung die Vorteile der datenträgerbasierten Komprimierung (DBC)?**

Ja. Da die Videodatei zwischengespeichert ist, wird der Versuch, auf das Video zuzugreifen, aus dem Cache bereitgestellt.

## Office 365-Beschleunigung

April 19, 2021

### 1. Warum analysieren wir das SAN?

Es ist mühsam, mehrere Profile für FQDNS für jede der Domänen zu erstellen, um dies zu überwinden, analysieren wir das SAN von den Zertifikaten.

### 2. Was ist eine Ausschlussliste?

Eine Fehler- oder Warnmeldung wird angezeigt Wenn der Browser oder die App das CA-Zertifikat nicht enthält, wird die IP-Adresse des Clients in solchen Fällen nach einigen Versuchen, eine Verbindung vom Browser/App herzustellen (2-3 Mal), zu einer Ausschlussliste hinzugefügt. Beim

nächsten Versuch wird die Verbindung nicht SSL-Proxy durchgeführt und die Seite wird ohne Fehler oder Warnung geladen. Die Client-IP-Adresse bleibt 48 Stunden lang in der Ausschlussliste. Die Ausschlussliste wird nur für geteilten Proxy beibehalten.

3. Wo soll nach Office 365-Beschleunigungsverbindungsinformationen gesucht werden?

Navigieren Sie zu **Monitoring > Connections > Accelerated Connections** und suchen Sie nach dem SSL-Proxystatus. Um Verbindungsdetails zu erhalten, klicken Sie auf das Symbol Details.

Action	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)	SSL Proxy
Details	172.16.139.236 : 49713	13.107.6.156 : 443	1m 0s	0m 55s	15.42 KB	1.9 to 1 (Disk)	51.1	True
Details	172.16.139.236 : 49719	111.221.111.196 : 443	0m 57s	0m 56s	7.41 KB	2.8 to 1 (Disk)	65.4	True
Details	172.16.139.236 : 49717	23.101.222.248 : 443	1m 0s	0m 58s	21.18 KB	1.1 to 1 (Disk)	8.4	True

4. Was passiert, wenn die Option Liste ausschließen nicht standardmäßig als Teil der SSL-Profilkonfiguration aktiviert ist?

Wenn der Browser oder die App das Zertifizierungsstellenzertifikat nicht enthält, wird ein Fehler oder eine Warnung angezeigt, und die Verbindungen von diesem Client oder der App werden blockiert. Um solche Probleme zu vermeiden, wählen Sie **Liste ausschließen** als Teil der SSL-Profilkonfiguration.

5. Was passiert, wenn die erforderlichen SANs nicht Teil des konfigurierten/erstellten Proxy-Zertifikats sind?

Die Verbindungen werden nicht SSL-Proxy durchgeführt und es gibt keine Beschleunigungsvorteile für Nicht-Proxy-SSL-Verbindungen.

6. Was passiert, wenn der Client nicht Teil der Domäne ist oder wenn der Client nicht über das Stammzertifikat der Domäne verfügt?

Die Verbindungen werden blockiert, wenn die Ausschlussliste nicht aktiviert ist.

7. Was passiert, wenn Citrix SD-WAN WANOP auf der Rechenzentrumsseite keine Root- oder Zwischenzertifizierungsstellen hat?

Die Verbindungen werden blockiert oder die Office 365-Anwendungsseiten, für die die fehlenden Stamm- oder Zwischenzertifizierungsstellen erforderlich sind, werden teilweise geladen. Um die Blockierung der Verbindungen aufzuheben oder diese Seiten vollständig zu laden, fügen Sie entweder die entsprechenden Zertifizierungsstellenzertifikate hinzu oder deaktivieren Sie das SSL-Profil für die Beschleunigung.



8. Wie kann man wissen, welche Clients von der Beschleunigung ausgeschlossen sind?

Ausgeschlossene Clientinformationen können aus Protokollen oder mithilfe des CLI-Befehls `show ssl-exclude -list` bekannt sein.

9. Was tun, wenn Kunden ausgeschlossen sind?

Standardmäßig werden die Ausschlusslisteninformationen von der Appliance nach 48 Stunden gelöscht. Der Benutzer kann die Informationen der Ausschlussliste zwangsweise löschen, indem er CLI-Befehle `clear ssl-exclude-list -/ <all>` verwenden `<Client_IP>`.

10. Wie kann man wissen, für welche SSL-Verbindungen (SNIs) kein Proxy verwendet wird?

In den Protokollen oder mit dem CLI-Befehl `show ssl-non-proxied-sni` können Sie die Liste der nicht über Proxy-Proxy-Proxys erfahrenen SNIs erfahren.

11. Wie lösche ich Nicht-Proxy-SNIs?

Verwenden Sie den CLI-Befehl `clear ssl-non-proxied-sni - <all>/<server name identifier>`.

12. Was ist die Standardzeit für Client im Ausschlusszustand?

Der Client bleibt 48 Stunden lang im Ausschlusszustand.

13. Können mehrere Profile für eine bestimmte Serviceklasse angewendet werden?

Ja, wir können Service-Klassen mit mehreren SSL-Profilen anwenden.

Navigieren Sie dazu auf Ihrer Virtual WAN-Appliance zu **Konfiguration > Service Class > Web (Internet-Secure) > Bearbeiten > Bearbeiten** (Anwendung) und fügen Sie die verfügbaren Profile hinzu.

14. Wie überprüfen Sie den Grund für nicht proxyierte Verbindungen?

Überprüfen Sie die TCP-Verbindungsseite. Weitere Informationen finden Sie in den Protokollen. Gehen Sie folgendermaßen vor, um die nicht-proxy Verbindungsprobleme zu debuggen.

- a) Wenn das Protokoll keine gültige Konfiguration anzeigt -  
Legen Sie die gültige Konfiguration fest. Weitere Informationen zum Konfigurieren der Office 365-Funktion finden Sie unter [Office 365-Beschleunigung](#).
- b) Wenn das Protokoll zeigt, dass die Zertifizierungsüberprüfung fehlgeschlagen ist - Fügen Sie der Citrix SD-WAN WANOP-Appliance im Rechenzentrum gültige CA-Zertifikate hinzu.
- c) `<Client\_IP\ >` wenn das Protokoll anzeigt, dass der Client ausgeschlossen ist - Informationen über ausgeschlossene Clients können mit dem CLI-Befehl `*clear ssl-exclude-list - \ <all\ > *` von der Appliance gelöscht werden.

## Zusätzliche Hinweise

- Bei der Protokollierung auf dem OneDrive-Client wird manchmal eine Warnmeldung „unechte Warnung“ angezeigt. Dies ist ein bekanntes Problem von Microsoft (<https://support.microsoft.com/en-us/kb/3097938>) und nicht spezifisch für die Citrix SD-WAN WANOP-Appliance.
- Für die von Office 365 umgeleiteten Seiten wird empfohlen, ein separates Proxy-Zertifikat zu erstellen, das SAN-Liste enthält, die dem Zertifikat der umgeleiteten Seiten entspricht. Erstellen Sie ein anderes Profil mit diesem Proxyzertifikat und wenden Sie sich für die Dienstklasse an. Fügen Sie außerdem die relevante CA in der Citrix SD-WAN WANOP-Appliance hinzu.
- Manchmal zeigt der Browser nicht die richtigen CA-Zertifikate an, in solchen Fällen verwenden Sie Wireshark oder OpenSSL, um die Stamm- und Intermediate-CA-Namen zu erhalten und die Zertifikate von 'authentischer' Quelle zu erhalten (zum Beispiel Windows SSL Store).
- Ein Unterschied im Browserverhalten kann beim Zugriff auf Office 365-Anwendungen von verschiedenen Browsern aus beobachtet werden, die keine erforderlichen Zertifikate haben und die Option Liste ausschließen deaktiviert ist.
- Wenn Office 365-Verbindungen SSL-Proxy (d. h. SSL-Proxy auf True festgelegt) und im Browser Office 365-Zertifikat anstelle des Proxy-Zertifikats angezeigt wird, wird empfohlen, den Browser im kognitiven Modus zu öffnen und das Verhalten zu überprüfen oder den Cache zu löschen und dann das Verhalten erneut zu überprüfen.
- Microsoft Office 365 umfasst viele Komponenten und Anwendungen wie OneDrive, Outlook, SharePoint, Word, PPT, Excel, OneNote. Alle diese Anwendungen wurden getestet und sind bekannt, dass sie problemlos funktionieren. Es wird erwartet, dass auch andere Anwendungen problemlos funktionieren. Dieser Status kann sich jedoch im Laufe der Zeit ändern und es können unbekannte Probleme auftreten.

## Komprimierung

April 19, 2021

Citrix SD-WAN WANOP-Komprimierung nutzt bahnbrechende Technologie, um eine transparente Multi-Level-Komprimierung bereitzustellen. Es ist wahre Komprimierung, die auf beliebige Byte-Streams wirkt. Es ist nicht anwendungsbewusst, ist gleichgültig gegenüber Verbindungsgrenzen und kann eine Zeichenfolge beim zweiten Mal in den Daten optimal komprimieren. Die Citrix SD-WAN WANOP-Komprimierung funktioniert mit jeder Verbindungsgeschwindigkeit.

Der Kompressionsmotor ist sehr schnell, so dass sich der Beschleunigungsfaktor für die Komprimierung dem Komprimierungsverhältnis nähert. Beispielsweise kann eine Massenübertragung,

die eine 1,5 Mbit/s T1-Verbindung monopolisiert und ein Komprimierungsverhältnis von 100:1 erreicht, ein Geschwindigkeitsverhältnis von fast 100x oder 150 Mbit/s liefern, vorausgesetzt, die WAN-Bandbreite ist der einzige Engpass in der Übertragung.

Im Gegensatz zu den meisten Komprimierungsmethoden wird der Citrix SD-WAN WANOP-Komprimierungsverlauf zwischen allen Verbindungen geteilt, die zwischen denselben beiden Appliances bestehen. Daten, die Stunden, Tage oder sogar Wochen früher über Verbindung A gesendet werden, können später über Verbindung B referenziert werden und erhalten den vollen Vorteil der Komprimierung. Die resultierende Leistung ist viel höher als mit herkömmlichen Methoden erreicht werden kann.

Die Komprimierung kann sowohl die Festplatte als auch den Arbeitsspeicher der Appliance verwenden, wodurch der Komprimierungsverlauf bis zu Terabyte bereitgestellt wird.

## **So funktioniert die Komprimierung**

Alle Komprimierungsalgorithmen scannen die zu komprimierenden Daten und suchen nach Datenzeichenfolgen, die mit zuvor gesendeten Zeichenfolgen übereinstimmen. Wenn keine solchen Übereinstimmungen gefunden werden, werden die Literaldaten gesendet. Wenn eine Übereinstimmung gefunden wird, werden die übereinstimmenden Daten durch einen Zeiger auf das vorherige Vorkommen ersetzt. In einer sehr großen übereinstimmenden Zeichenfolge können Megabyte oder sogar Gigabyte Daten durch einen Zeiger dargestellt werden, der nur wenige Bytes enthält, und nur diese wenigen Bytes müssen über den Link gesendet werden.

Komprimierungs-Engines sind durch die Größe ihres Komprimierungsverlaufs begrenzt. Traditionelle Komprimierungsalgorithmen wie LZS und ZLIB verwenden Komprimierungsprotokolle von 64 KB oder weniger. Citrix SD-WAN WANOP-Appliances behalten mindestens 100 GB Komprimierungsverlauf bei. Mit mehr als einer Million Mal so viel Komprimierungsverlauf herkömmlicher Algorithmen findet der Citrix SD-WAN WANOP-Algorithmus mehr Übereinstimmungen und längere Übereinstimmungen, was zu überlegenen Komprimierungsverhältnissen führt.

Der Citrix SD-WAN WANOP-Komprimierungsalgorithmus ist sehr schnell, sodass selbst die Einstiegsgeräte ein 100-Mbit/s-LAN mit dem Ausgang des Kompressors sättigen können. Die leistungstärksten Modelle bieten einen Durchsatz von über 1 Gbit/s.

Nur Nutzlastdaten werden komprimiert. Header werden jedoch indirekt komprimiert. Wenn eine Verbindung beispielsweise 4:1-Komprimierung erreicht, wird nur ein Ausgabepaket in voller Größe für alle vier Eingabepakete in voller Größe gesendet. Somit wird auch die Menge der Header-Daten um 4:1 reduziert.

### **Komprimierung als Allzweckoptimierung:**

Die Citrix SD-WAN WANOP-Komprimierung ist anwendungsunabhängig: Sie kann Daten aus jeder nicht verschlüsselten TCP-Verbindung komprimieren.

Im Gegensatz zu Caching ist die Komprimierungsleistung angesichts der sich ändernden Daten robust. Durch das Ändern eines einzelnen Bytes einer Datei wird die gesamte Kopie im Cache ungültig. Durch die Komprimierung werden beim Ändern eines einzelnen Bytes in der Mitte einer Datei nur zwei große Übereinstimmungen erstellt, die durch ein einzelnes Byte nicht übereinstimmender Daten getrennt sind, und die resultierende Übertragungszeit ist nur etwas größer als zuvor. Daher verschlechtert sich das Komprimierungsverhältnis im Verhältnis der Menge der Änderungen. Wenn Sie eine Datei herunterladen, 1% davon ändern und erneut hochladen, erwarten Sie beim Upload ein Kompressionsverhältnis von 99:1.

Ein weiterer Vorteil einer großen Komprimierungsgeschichte besteht darin, dass vorkomprimierte Daten problemlos mit der Citrix SD-WAN WANOP-Technologie komprimiert werden. Ein JPEG-Bild oder ein YouTube-Video beispielsweise ist vorkomprimiert, sodass beim ersten Senden über den Link nur wenig zusätzliche Komprimierung möglich ist. Aber wenn es wieder gesendet wird, wird die gesamte Übertragung auf nur eine Handvoll Bytes reduziert, auch wenn sie von verschiedenen Benutzern oder mit unterschiedlichen Protokollen gesendet wird, wie zum Beispiel per FTP das erste Mal und HTTP das nächste Mal.




In der Praxis hängt die Komprimierungsleistung davon ab, wie viel der Daten, die die Verknüpfung durchlaufen, mit den Daten übereinstimmt, die zuvor die Verknüpfung durchlaufen haben. Die Menge variiert von Anwendung zu Anwendung, von Tag zu Tag und sogar von Moment zu Moment. Wenn Sie sich eine Liste aktiver beschleunigter Verbindungen ansehen, erwarten Sie Verhältnisse zwischen 1:1 und 10.000:1.

Monitoring > Optimization > Connections > Accelerated Connections

Accelerated Connections

Unaccelerated Connections

Action ▾

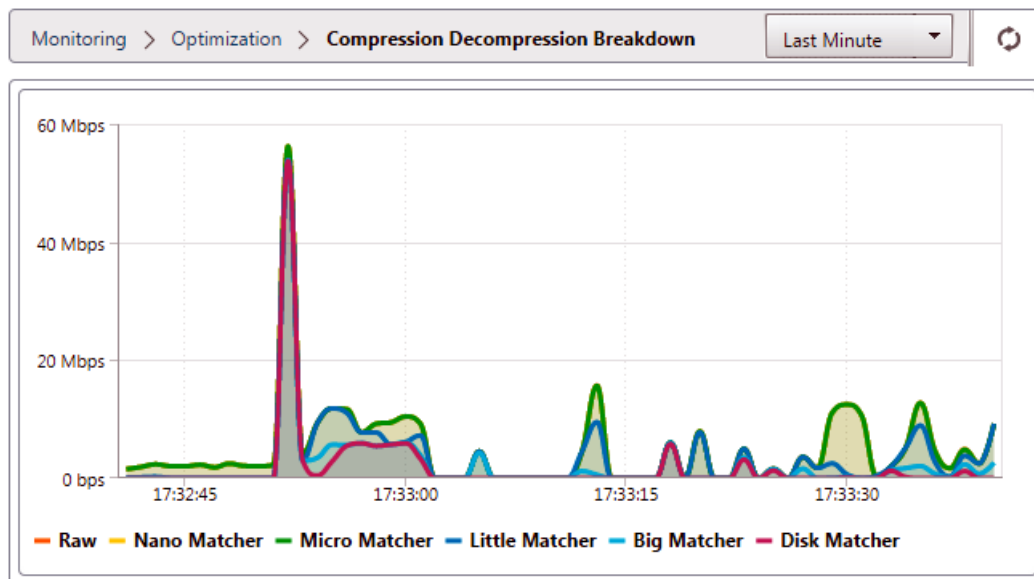
Details	Initiator	Responder	Duration	Idle	Bytes Transferred ↑	Compression Ratio/Type
	172.16.0.1 : 55222	172.16.0.71 : 3120	0m 43s	0m 13s	7.39 MB	969.0 to 1 (Disk)
	172.16.0.52 : 58730	208.85.46.23 : 80	1m 41s	1m 37s	1.70 MB	97.9 to 1 (Disk)
	172.16.0.34 : 51869	173.194.33.142 : 443	1m 7s	0m 3s	913.82 KB	N/A (None)

## Verschlüsselte Protokolle komprimieren:

Viele Verbindungen mit schlechter Komprimierungsleistung tun dies, weil sie verschlüsselt sind. Verschlüsselter Datenverkehr ist normalerweise nicht komprimierbar, aber Citrix SD-WAN WANOP-Appliances können verschlüsselte Verbindungen komprimieren, wenn die Appliances der Sicherheitsinfrastruktur beitreten. Citrix SD-WAN WANOP-Appliances treten der Sicherheitsinfrastruktur automatisch mit Citrix Citrix Virtual Apps and Desktops bei und können der Sicherheitsinfrastruktur von SSL-, Windows-Dateisystem- (CIFS/SMB) und Outlook/Exchange (MAPI) Servern mit manueller Konfiguration beitreten.

**Adaptive, Null-Konfigurationsoperation:**

Um den unterschiedlichen Anforderungen des unterschiedlichen Datenverkehrs gerecht zu werden, verwenden Citrix SD-WAN WANOP-Appliances nicht eine, sondern fünf Kompressions-Engines, sodass die Anforderungen von allem, vom massivsten Massentransfer bis zum aktuellsten interaktiven Datenverkehr, problemlos berücksichtigt werden können. Die Komprimierungseengine wird dynamisch auf die sich ändernden Anforderungen einzelner Verbindungen abgestimmt, so dass die Komprimierung automatisch optimiert wird. Ein zusätzlicher Vorteil ist, dass die Komprimierungseengine keine Konfiguration erfordert.

**Speicherbasierte Komprimierung**

Die meisten Komprimierungseengine verwenden RAM, um ihren Komprimierungsverlauf zu speichern. Dies wird als speicherbasierte Komprimierung bezeichnet. Einige Appliances widmen diesen Komprimierungseengine Gigabytes an Speicher. Die speicherbasierte Komprimierung hat eine geringe Latenz und wird oft automatisch für interaktive Aufgaben wie Virtual Apps/Virtual Desktops-Datenverkehr ausgewählt.

**Festplattenbasierte Komprimierung**

Die festplattenbasierte Komprimierungseengine verwendet überall zwischen zehn Gigabyte und Terabyte Speicher, um den Komprimierungsverlauf zu speichern und so mehr und bessere Komprimierungsübereinstimmungen zu ermöglichen. Die festplattenbasierte Komprimierungseengine ist sehr schnell, weist aber manchmal eine höhere Latenz als die speicherbasierten Engines auf und wird häufig automatisch für Massenübertragungen ausgewählt.

## Aktivieren oder Deaktivieren der Komprimierung

Die Komprimierung ist auf der Seite Konfiguration:

Service-Klassen pro Service-Klasse aktiviert. Diese Seite enthält ein Pulldownmenü für jede Serviceklasse mit den folgenden Optionen:

- **Datenträger**, was bedeutet, dass sowohl die festplattenbasierte als auch die speicherbasierte Komprimierung aktiviert sind. Diese Option sollte ausgewählt werden, es sei denn, Sie haben einen bestimmten Grund für die Deaktivierung.
- **Speicher**, was bedeutet, dass die speicherbasierte Komprimierung aktiviert ist, aber die festplattenbasierte Komprimierung nicht ist. Diese Einstellung wird selten verwendet, da die Appliance automatisch Speicher oder Datenträger auswählt, wenn beide Komprimierungsarten aktiviert sind.
- **Nur Flow-Control**, die die Komprimierung deaktiviert, aber die Beschleunigung der Durchflussregelung ermöglicht. Wählen Sie diese Option für Dienste, die immer verschlüsselt sind, und für den FTP-Steuerkanal.
- **Keine**, was bedeutet, dass Komprimierung und Durchflusssteuerung beide deaktiviert sind.

Weitere Informationen finden Sie unter [Serviceklassen](#).

## Messen der festplattenbasierten Kompressionsleistung

Auf der Registerkarte Komprimierungsstatus der Seite

Berichte: Komprimierung wird die Systemkomprimierungsleistung angezeigt, seit das System gestartet wurde oder die Schaltfläche Löschen zum Zurücksetzen der Statistiken verwendet wurde. Die Komprimierung für einzelne Verbindungen wird in den Verbindungsabschlussmeldungen im Systemprotokoll gemeldet.

Die Komprimierungsleistung variiert mit einer Reihe von Faktoren, einschließlich der Redundanz im Datenstrom und in geringerem Maße der Struktur des Datenprotokolls.

Einige Anwendungen, wie FTP, senden reine Datenströme; die TCP-Verbindungsnutzlast ist immer Byte für Byte identisch mit der ursprünglichen Datendatei. Andere, wie CIFS oder NFS, senden keine reinen Datenströme, sondern mischen Befehle, Metadaten und Daten in demselben Stream. Die Komprimierungs-Engine unterscheidet die Dateidaten, indem die Verbindungsnutzlast in Echtzeit analysiert wird. Solche Datenströme können problemlos Komprimierungsverhältnisse zwischen 100:1 und 10.000:1 im zweiten Durchgang erzeugen.

Durchschnittliche Komprimierungsverhältnisse für den Link hängen von der relativen Prävalenz von langen Übereinstimmungen, kurzen Übereinstimmungen und keine Übereinstimmungen ab. Dieses Verhältnis ist vom Verkehr abhängig und ist in der Praxis schwer vorherzusagen.

Die Testergebnisse zeigen den Effekt der Multi-Level-Komprimierung als Ganzes, wobei jeweils speicherbasierte und festplattenbasierte Komprimierung ihren Beitrag leisten.

Die maximale Komprimierungsleistung wird erst erreicht, wenn der für die festplattenbasierte Komprimierung verfügbare Speicherplatz gefüllt ist, wodurch eine maximale Menge früherer Daten mit neuen Daten übereinstimmt. In einer perfekten Welt würde das Testen erst abgeschlossen, wenn die Festplatten der Appliance nicht nur gefüllt, sondern mindestens einmal gefüllt und überschrieben wurden, um sicherzustellen, dass der stationäre Betrieb erreicht wurde. Allerdings haben nur wenige Administratoren so viele repräsentative Daten zur Verfügung.

Eine weitere Schwierigkeit bei Leistungstests besteht darin, dass die Beschleunigung oft schwache Verbindungen im Netzwerk offenlegt, typischerweise in der Leistung des Clients, des Servers oder des LAN, und diese manchmal als enttäuschende Beschleunigungsleistung falsch diagnostiziert werden.

Sie können Iperf oder FTP für Vor- und Ersttests verwenden. Iperf ist nützlich für Vorversuche. Es ist extrem komprimierbar (auch auf dem ersten Durchgang) und verbraucht relativ wenig CPU und keine Festplattenressourcen auf den beiden Endpunktsystemen. Komprimierte Leistung mit Iperf sollte über eine T1-Verbindung mehr als 200 Mbit/s senden, wenn die LANs auf beiden Seiten Gigabit-Ethernet verwenden, oder etwas weniger als 100 Mbit/s, wenn sich Fast-Ethernet-Geräte in den LAN-Pfaden zwischen Endpunkten und Appliances befinden.

Iperf ist auf den Appliances (im Menü „Diagnostics“) vorinstalliert und ist bei erhältlich <http://iperf.sourceforge.net/>. Idealerweise sollte es von den Endpunktsystemen installiert und ausgeführt werden, damit das Netzwerk von Ende zu Ende getestet wird, nicht nur von Appliance zu Appliance.

FTP ist nützlich für realistischere Tests als mit Iperf möglich. FTP ist einfach und vertraut, und seine Ergebnisse sind leicht zu interpretieren. Second-Pass-Leistung sollte ungefähr die gleiche wie bei Iperf sein. Wenn nicht, ist der Grenzfaktor wahrscheinlich das Festplattensubsystem auf einem der Endpunktsysteme.

#### **So testen Sie das festplattenbasierte Komprimierungssystem:**

1. Übertragen Sie einen Datenstrom mit mehreren Gigabyte zwischen zwei Appliances mit aktivierter festplattenbasierter Komprimierung. Beachten Sie die Komprimierung, die während dieser Übertragung erreicht wurde. Abhängig von der Art der Daten kann im ersten Durchgang eine beträchtliche Komprimierung gesehen werden.
2. Übertragen Sie denselben Datenstrom ein zweites Mal und notieren Sie sich den Effekt auf die Komprimierung.

#### **Kompressionsberichte in Premium Edition**

Die Citrix SD-WAN Premium (Enterprise) Edition verfügt nicht über eine Ansicht zum Anzeigen von Komprimierungsberichten auf Protokoll- oder Anwendungsbasis über WANOP-Dienstklassen, die

über die Protokoll- oder Anwendungszuordnung verfügen. Wenn Sie eine Premium (Enterprise) Edition-Appliance verwenden, ist der einzige für die Komprimierung verfügbare Bericht ein Komprimierungsbericht auf Verbindungsebene, der keinen Einblick in das Ausmaß gibt, in dem ein Protokoll optimiert oder komprimiert wurde. Komprimierungsberichte sind in der WAN-Optimierungs-GUI verfügbar, die eine Aufschlüsselung aller eindeutigen Protokolle anzeigt und wie Berichte über einen bestimmten Zeitraum optimiert wurden.

In der Benutzeroberfläche der Citrix SD-WAN Premium (Enterprise) Edition-Appliance für WAN-Optimierung wurden die folgenden Widgets unter dem WAN-Optimierungs-Dashboard hinzugefügt.

- Konsolidiertes Komprimierungsverhältnis —der gesamte Datenverkehr, der über die WANOP-Appliance und die Gesamtzahl der beschleunigten und nicht beschleunigten Verbindungen. Auf diese Weise können Sie den gesamten Datenverkehr überwachen, der von LAN zu WAN übertragen wird.
- Kompressionsverhältnis - Top 10 Service-Klassen.
- Aggregierter Link-Durchsatz —LAN und WAN.

**Konsolidiertes Komprimierungsverhältnis:**

Dieser Bericht zeigt das konsolidierte Komprimierungsverhältnis für den gesamten an WANOP übertragenen Datenverkehr sowie die Gesamtzahl der beschleunigten und nicht beschleunigten Verbindungen an. Außerdem wird die Betriebszeit des WANOP-Dienstes in der Appliance angezeigt.

Monitoring > WAN Optimization > Dashboard				
Up Time	Compression Ratio	Accelerated Connections	Unaccelerated Connections	
1 hr 17 min	12,283 to 1 (91.859%)	12	2	

**Aggregierter Verbindungsdurchsatz:**

Dieser Bericht zeigt den gesamten Datenverkehr, der an WANOP übertragen wird, und den gesamten Datenverkehr, der mit Unterbrechungen in Kategorien optimierter und nicht optimierter Daten an beiden Enden überträgt.



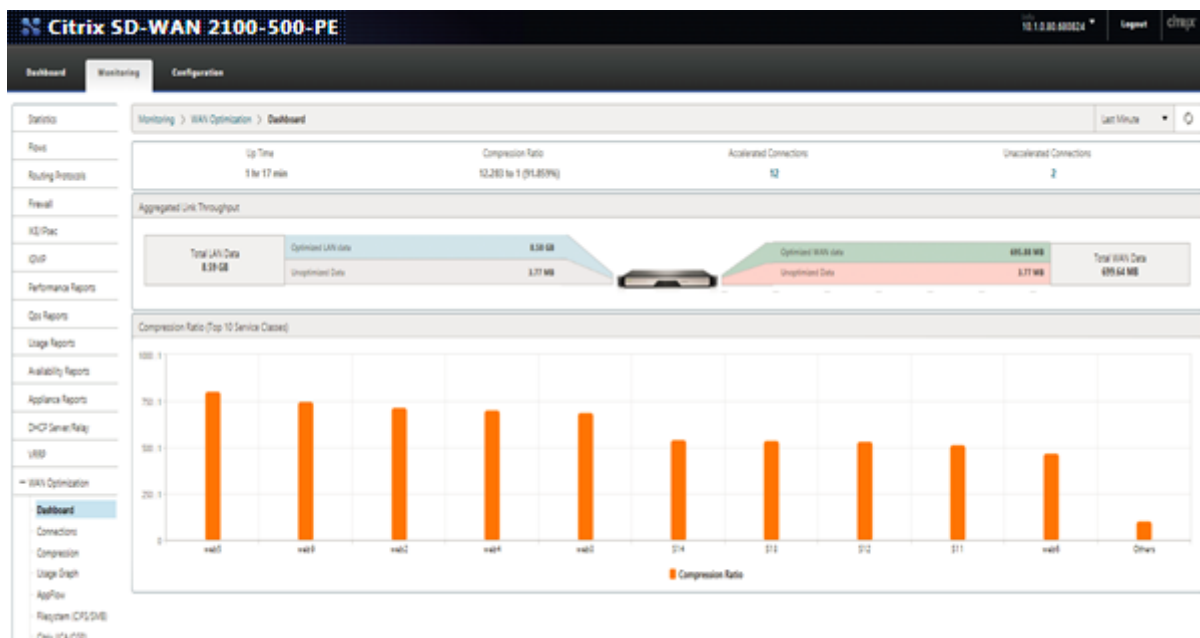
**Komprimierungsverhältnis (Top 10 Serviceklassen):**

In der Benutzeroberfläche der Citrix SD-WAN Appliance können Sie die Verbindungsdetails und das Komprimierungsverhältnis (pro Service-Class-Dashboard) überprüfen, indem Sie zu **Überwachung > WAN-Optimierung** navigieren. Diese Option wählt automatisch den Dashboard-Knoten aus und bietet eine Übersicht in Form von Dashboard.

Das Diagramm zeigt die zehn wichtigsten Werte des Komprimierungsverhältnisses für Verkehr, kategorisiert nach Serviceklassen.



Es wird ein zusätzlicher Balken Andere angezeigt, der neben den Top 10 Serviceklassen Komprimierungsverhältnisberichten für alle anderen beschleunigten Verbindungen, die Teil des Systems sind, das Komprimierungsverhältnis anzeigt.



## HTTP-Beschleunigung

April 19, 2021

Der Citrix SD-WAN WANOP-Beschleuniger verwendet eine Vielzahl von Zero-Config-Optimierungen, um den HTTP-Verkehr zu beschleunigen. Dies wiederum beschleunigt Webseiten und andere Anwendungen, die das HTTP-Protokoll verwenden (Datei-Downloads, Video-Streaming, automatische Updates usw.).

Optimierungen, die HTTP beschleunigen, umfassen Komprimierung, Traffic Shaping, Flow Control und Caching.

## Komprimierung

HTTP ist eine ideale Anwendung für Citrix SD-WAN WANOP Multi-Level-Komprimierung.

Statische Inhalte, einschließlich Standard-HTML-Seiten, Bilder, Videos und Binärdateien, erhalten variable Mengen an Erstpasse-Komprimierung, in der Regel 1:1 für vorkomprimierte Binärinhalte und 2:1 oder mehr für textbasierte Inhalte. Beginnend mit dem zweiten Mal, dass das Objekt gesehen wird, liefern die beiden größten Komprimierungsmodule (speicherbasierte Komprimierung und

festplattenbasierte Komprimierung) extrem hohe Komprimierungsverhältnisse, wobei größere Objekte Komprimierungsverhältnisse von 1, 000:1 oder mehr erhalten. Bei solch hohen Komprimierungsverhältnissen ist die WAN-Verbindung nicht mehr der Grenzfaktor, und der Server, der Client oder das LAN wird zum Engpass.

Das Gerät schaltet dynamisch zwischen Kompressoren um maximale Leistung zu erzielen. Beispielsweise verwendet die Appliance einen kleineren Kompressor im HTTP-Header und einen größeren Kompressor im HTTP-Körper.

Dynamische Inhalte, einschließlich HTTP-Header und dynamisch generierte Seiten —Seiten, die nie doppelt gleich sind, aber Ähnlichkeiten zueinander aufweisen —werden von den drei Komprimierungsmodule komprimiert, die kleinere Übereinstimmungen bewältigen. Wenn eine Seite zum ersten Mal gesehen wird, ist die Komprimierung gut. Wenn eine Variante auf einer vorherigen Seite angezeigt wird, ist die Komprimierung besser.

## **Traffic Shaping**

HTTP besteht aus einer Mischung aus interaktivem und Massenverkehr. Der Datenverkehr jedes Benutzers ist eine Mischung aus beiden, und manchmal enthält die gleiche Verbindung eine Mischung aus beiden. Der Traffic Shaper stellt nahtlos und dynamisch sicher, dass jede HTTP-Verbindung ihren fairen Anteil an der Verbindungsbandbreite erhält. Dadurch wird verhindert, dass Massenübertragungen die Verbindung auf Kosten interaktiver Benutzer monopolisiert und gleichzeitig sichergestellt, dass Massenübertragungen jede Bandbreite erhalten, die interaktive Verbindungen nicht verwenden.

## **Durchflussregelung**

Erweiterte Weiterübertragungsalgorithmen und andere Optimierungen auf TCP-Level behalten die Reaktionsfähigkeit und halten Übertragungsraten angesichts von Latenz und Verlust aufrecht.

## **Video-Caching**

HTTP-Caching für Videodateien wurde in Version 7.0 eingeführt. Caching beinhaltet das Speichern von HTTP-Objekten im lokalen Speicher und die Bereitstellung für lokale Clients, ohne sie vom Server neu zu laden.

Was ist der Unterschied zwischen Caching und Komprimierung? Während das Caching eine Beschleunigung bietet, die der Komprimierung ähnelt, sind die beiden Methoden unterschiedlich und machen sie komplementär.

- Durch die Komprimierung werden Übertragungen vom Remoteserver beschleunigt, und diese höhere Datenrate kann den Server höher belasten, wenn keine Komprimierung vorhanden ist. Caching verhindert Übertragungen vom Server und reduziert die Belastung des Servers.
- Die Komprimierung funktioniert auf jedem Datenstrom. Dies ähnelt einer vorherigen Übertragung. Wenn Sie den Namen einer Datei auf dem Remote-Server ändern und erneut übertragen, funktioniert die Komprimierung perfekt. Caching funktioniert nur, wenn das vom Client angeforderte Objekt und das Objekt auf dem Datenträger als identisch sind. Wenn Sie den Namen einer Datei auf dem Remoteserver ändern und erneut übertragen, wird die zwischengespeicherte Kopie nicht verwendet.
- Komprimierte Daten können nicht schneller bereitgestellt werden, als der Server sie senden kann. Im Cache gespeicherte Daten sind nur von der Geschwindigkeit der clientseitigen Appli-ance abhängig.
- Die Komprimierung ist CPU-intensiv, die Zwischenspeicherung ist nicht möglich.

## Funktionsweise von HTML5

April 19, 2021

HTML5 verwendet HTTP, ein Request/Response-Protokoll für die Kommunikation zwischen Clients und Servern. Ein Client initiiert eine TCP-Verbindung und sendet HTTP-Anforderungen an den Server. Der Server antwortet auf diese Anforderungen, indem er Zugriffsrechte für die verfügbaren Ressourcen erteilt. Nachdem Client und Server eine Verbindung hergestellt haben, enthalten die zwischen ihnen ausgetauschten Nachrichten nur WebSocket-Header und nicht HTTP-Header.

Die Infrastruktur von HTML5 besteht aus WebSockets, die die vorhandene HTTP-Infrastruktur weiter nutzen, um einen einfachen Mechanismus für die Kommunikation zwischen einem Client und einem Webserver bereitzustellen. In der Regel implementieren Sie das WebSocket-Protokoll in einem Browser und Webservern. Sie können dieses Protokoll jedoch mit jeder Client- oder Serveranwendung verwenden.

Wenn ein Client versucht, eine Verbindung mit WebSockets herzustellen, behandeln Webserver den WebSocket-Handshake als Aktualisierungsanforderung, und der Server wechselt zum WebSocket-Protokoll. Das WebSocket-Protokoll ermöglicht eine häufige Interaktion zwischen dem Browser und den Webservern. Daher können Sie dieses Protokoll für Live-Updates wie Aktienindizes und Score-Karten und sogar Live-Spiele verwenden. Dies ist aufgrund einer standardisierten Möglichkeit möglich, dass der Server unerwünschte Antworten an den Client senden kann, während eine offene Verbindung für die bidirektionale fortlaufende Kommunikation zwischen dem Client-Browser und dem Server aufrechterhalten wird.

**Hinweis**

Sie können diesen Effekt auch auf nicht standardisierte Weise erreichen, indem Sie verschiedene andere Technologien wie Comet verwenden. Weitere Informationen über Comet finden Sie unter [http://en.wikipedia.org/wiki/Comet\\_\(programming\)](http://en.wikipedia.org/wiki/Comet_(programming)).

Das WebSocket-Protokoll kommuniziert über TCP-Ports 80 und 443. Dies erleichtert die Kommunikation in Umgebungen, in denen Firewalls verwendet werden, um nicht-webbasierte Internetverbindungen zu blockieren. Darüber hinaus verfügt WebSocket über einen eigenen Fragmentierungsmechanismus. Eine WebSocket-Nachricht kann als mehrere WebSocket-Frames gesendet werden.

**Hinweis**

Sie können WebSocket nicht verwenden, wenn die Webanwendungen auf den Servern es nicht unterstützen.

**Wie HTML5 eine WebSocket-Sitzung einrichtet**

Ein Browser, der HTML5 unterstützt, verwendet JavaScript-APIs, um die folgenden Aufgaben auszuführen:

- Öffnen Sie eine WebSocket-Verbindung.
- Kommunizieren Sie über die WebSocket-Verbindung.
- Schließen Sie die WebSocket-Verbindungen.

Um eine WebSocket-Verbindung zu öffnen, sendet der Browser eine HTTP-Upgrade-Nachricht an den Server, um zum WebSocket-Protokoll zu wechseln. Der Server akzeptiert diese Anforderung entweder oder lehnt sie ab. Im Folgenden finden Sie Ausschnitte einer Beispiel-Clientanforderung und Serverantwort:

- Beispiel-Clientanforderung

```
GET /HTTP/1.1 Upgrade: websocket Sec-websocket-
protocol: <List of protocols that the client supports over this
websocket session, such as an application level protocol, for
example ICA.> Sec-websocket-extensions: <List of extensions
client wants applied to this session, such as compression.> Sec-
WebSocket-version: <Version of websocket protocol that the client
intends to use.> <!--NeedCopy-->
```

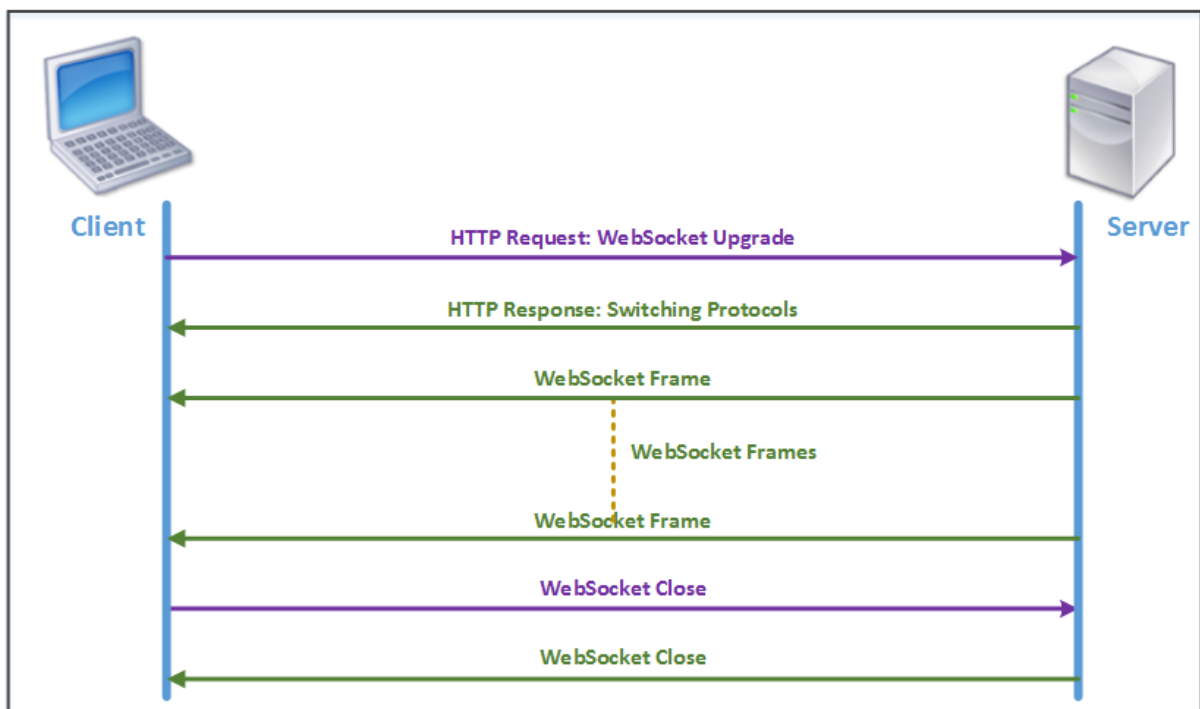
- Beispiel-Server-Antwort

```

pre codeblock HTTP/1.1 101 Switching Protocols Upgrade: websocket
  Connection: Upgrade Sec-WebSocket-Protocol: <One from the list
  of protocols in the client request.> Sec-WebSocket-extensions:
  <List of extensions server accepts for session.> Sec-WebSocket-
  version: <Version of websocket protocol that the server supports
  .> <!--NeedCopy-->

```

Die folgende Abbildung zeigt die Reihenfolge der Nachrichten, die zwischen einem Client und einem Server ausgetauscht werden:



Während einer HTML5-Verbindung werden die folgenden Meldungen zwischen dem Client und dem Server ausgetauscht:

- Client sendet eine HTTP-Anforderung zum Upgrade von WebSocket.
- Server reagiert auf die Clientanforderung und wechselt zum WebSocket-Protokoll.
- Server sendet WebSocket-Frames an den Client.
- Client sendet eine Anforderung, den WebSocket zu schließen.
- Der Server schließt den WebSocket.

## IPv6 (Internet Protocol Version 6) Beschleunigung

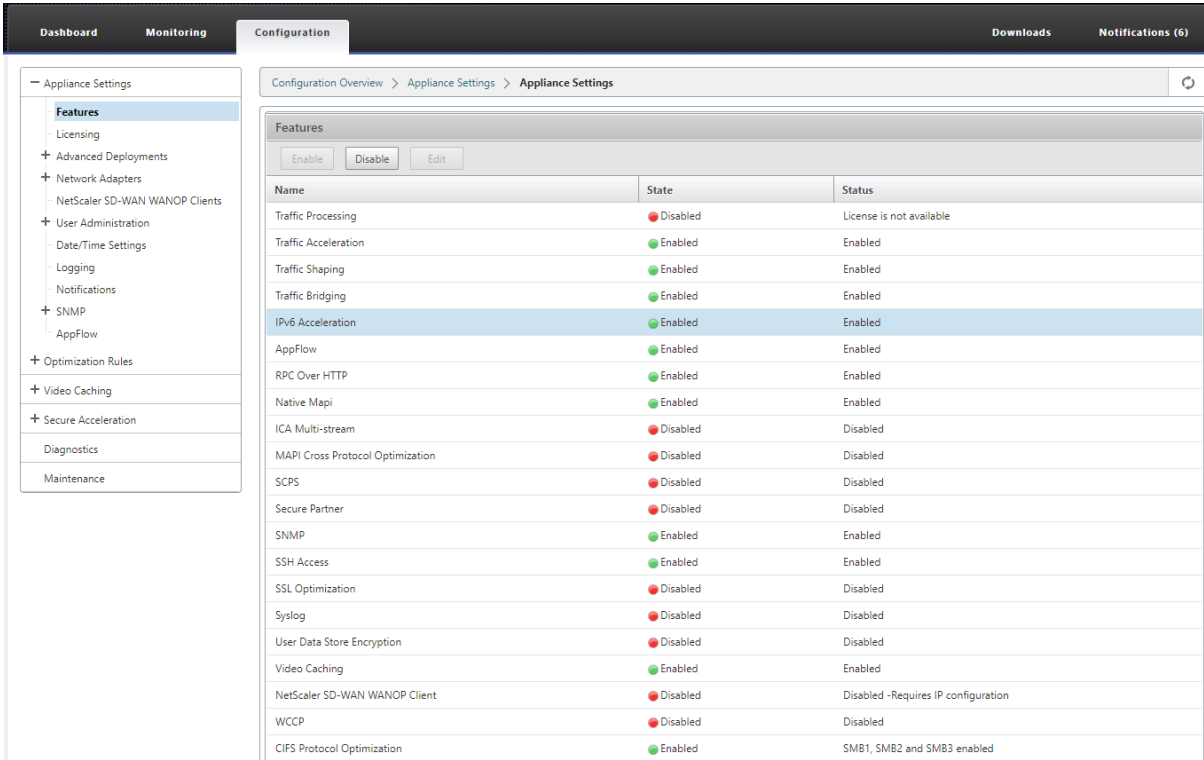
April 19, 2021

Wenn Sie über ein Gerät eine Internetverbindung herstellen, wird dem Gerät eine IP-Adresse zugewiesen. Die IP-Adresse identifiziert die Appliance und zeigt ihren Standort an. Die Anzahl der Geräte, die mit dem Internet verbunden sind, nimmt rapide zu. Daher ist es schwierig, die Anforderung für die IP-Adressen mit der vorhandenen Version von Internet Protocol (IP), IPv4, zu verwalten, die 32-Bit-Adressen verwendet. Mit IPv4 können den Geräten, die mit dem Internet verbunden sind, ca. 4,3 Milliarden Adressen zugewiesen werden.

IPv6 behebt dieses Problem, indem 128-Bit-Adressen und ein Hexadezimallabel verwendet werden, um die Netzwerkschnittstellen von Geräten in einem IPv6-Netzwerk zu identifizieren. Da IPv6 weit mehr IP-Adressen unterstützt als IPv4, werden Organisationen und Anwendungen schrittweise Unterstützung für das IPv6-Protokoll eingeführt.

Die Protokolle IPv4 und IPv6 sind nicht interoperabel, was den Übergang erschwert. Um den zunehmenden IPv6-Verkehr von verschiedenen Anwendungen zu beschleunigen, die von der Citrix SD-WAN WANOP-Appliance unterstützt werden, können Sie die IPv6-Beschleunigungsfunktion aktivieren.

Standardmäßig ist IPv6 auf der Appliance deaktiviert. Um die IPv6-Beschleunigung auf einer Citrix SD-WAN WANOP-Appliance zu aktivieren, navigieren Sie zur Seite **Konfiguration > Appliance-Einstellungen > Feature** und aktivieren Sie die **IPv6-Beschleunigungsfunktion**.



The screenshot shows the Citrix SD-WAN WANOP Configuration interface. The left sidebar lists various settings categories, with 'Features' selected. The main panel displays a table of features and their status.

Name	State	Status
Traffic Processing	Disabled	License is not available
Traffic Acceleration	Enabled	Enabled
Traffic Shaping	Enabled	Enabled
Traffic Bridging	Enabled	Enabled
<b>IPv6 Acceleration</b>	<b>Enabled</b>	<b>Enabled</b>
AppFlow	Enabled	Enabled
RPC Over HTTP	Enabled	Enabled
Native Mapi	Enabled	Enabled
ICA Multi-stream	Disabled	Disabled
MAPI Cross Protocol Optimization	Disabled	Disabled
SCPS	Disabled	Disabled
Secure Partner	Disabled	Disabled
SNMP	Enabled	Enabled
SSH Access	Enabled	Enabled
SSL Optimization	Disabled	Disabled
Syslog	Disabled	Disabled
User Data Store Encryption	Disabled	Disabled
Video Caching	Enabled	Enabled
NetScaler SD-WAN WANOP Client	Disabled	Disabled - Requires IP configuration
WCCP	Disabled	Disabled
CIFS Protocol Optimization	Enabled	SMB1, SMB2 and SMB3 enabled

Überprüfen von IPv6-Verbindungen

Nachdem die IPv6-Beschleunigung auf der Appliance aktiviert wurde, beschleunigt die Appliance den Datenverkehr für die Anwendungen mithilfe des IPv6-Protokolls. Um sicherzustellen, dass die Appliance den IPv6-Datenverkehr beschleunigt, können Sie solche Verbindungen auf der Appliance überwachen.

Um die IPv6-Verbindungen zu überwachen, navigieren Sie zur Registerkarte Überwachung. Auf der Seite „**Verbindungen**“ der Registerkarte „**Überwachung**“ werden Statistiken zu IPv6-Protokollen im Zusammenhang mit dem Verkehr angezeigt:

**Verbindungen:** Auf der Seite Verbindungen werden Details aller Verbindungen aufgeführt, die mit der Appliance hergestellt wurden. Diese Seite besteht aus zwei Registerkarten: Beschleunigte Verbindungen und nicht beschleunigte Verbindungen. Auf der Registerkarte Beschleunigte Verbindungen werden alle Verbindungen aufgeführt, die die Appliance beschleunigt. Sie können IPv6-Datenverkehr auf dieser Registerkarte identifizieren, indem Sie auf die Spalte Initiator und Responder jedes Eintrags verweisen. Wenn diese Spalten hexadezimale IP-Adresswerte enthalten, stellt der Eintrag eine IPv6-Verbindung dar, wie im folgenden Screenshot gezeigt.

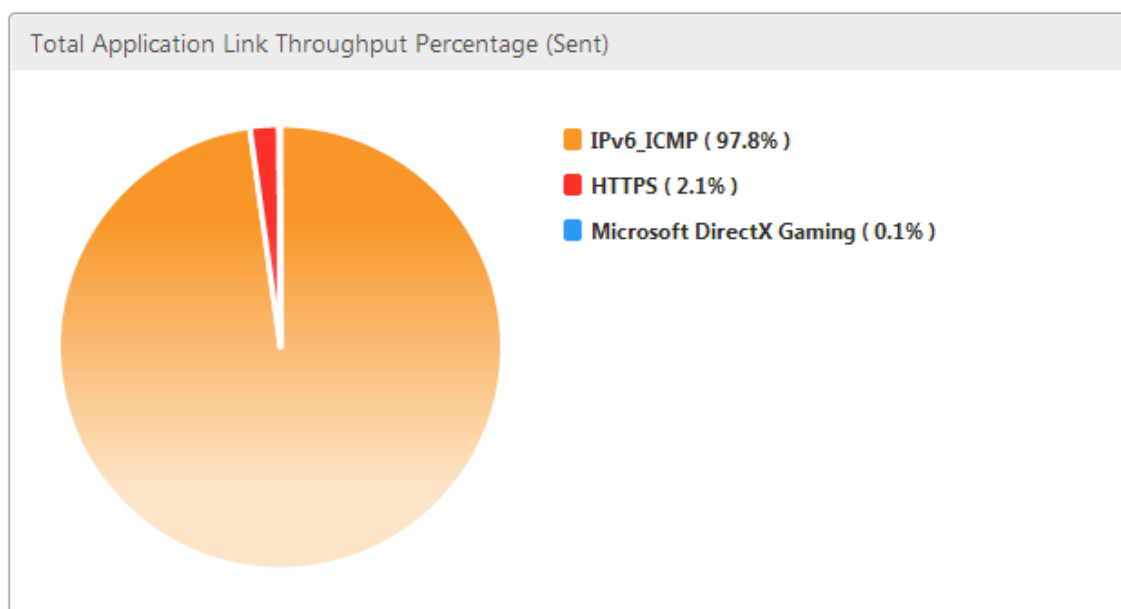
Accelerated Connections											
Unaccelerated Connections											
Action	Details	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	SSL Proxy	Service Class	State	Partner Unit
		2000:10:60730	4000:10:5001	6m 33s	0m 0s	34.29 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60717	4000:10:5001	6m 33s	0m 0s	34.27 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60725	4000:10:5001	6m 33s	0m 0s	33.63 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		192.168.1.10:39688	172.16.1.10:5001	2m 19s	0m 0s	26.03 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		192.168.1.10:39689	172.16.1.10:5001	2m 19s	0m 0s	25.79 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60718	4000:10:5001	6m 33s	0m 0s	31.32 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60722	4000:10:5001	6m 33s	0m 0s	31.07 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60728	4000:10:5001	6m 33s	0m 0s	30.92 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60720	4000:10:5001	6m 33s	0m 0s	30.55 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60715	4000:10:5001	6m 33s	0m 0s	30.29 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60727	4000:10:5001	6m 33s	0m 0s	29.36 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60721	4000:10:5001	6m 33s	0m 0s	26.23 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60713	4000:10:5001	6m 33s	0m 0s	24.67 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60714	4000:10:5001	6m 33s	0m 0s	23.58 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60726	4000:10:5001	6m 33s	0m 0s	23.08 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60711	4000:10:5001	6m 33s	0m 0s	22.99 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60729	4000:10:5001	6m 33s	0m 0s	22.95 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60723	4000:10:5001	6m 33s	0m 0s	22.71 MB	N/A (None)	False	Iperf	Open	10.105.145.125
		2000:10:60712	4000:10:5001	6m 33s	0m 0s	22.55 MB	N/A (None)	False	Iperf	Open	10.105.145.125

IPv6-Verbindungen, die nicht beschleunigt werden, werden auf der Registerkarte Nicht beschleunigte Verbindungen aufgeführt. Wenn Sie diese Verbindungen beschleunigen möchten, müssen Sie möglicherweise die Anwendungsparameter auf der Appliance beheben und optimieren. Wie auf der Registerkarte **Beschleunigte Verbindungen** können Sie die IPv6-Verbindungen auf dieser Registerkarte identifizieren, indem Sie auf die Spalten **Initiator** und **Responder** jedes Eintrags verweisen.

**Top-Anwendungen:** Die Seite „Top-Anwendungen“ bietet Granularität in dem Zeitrahmen, den Sie

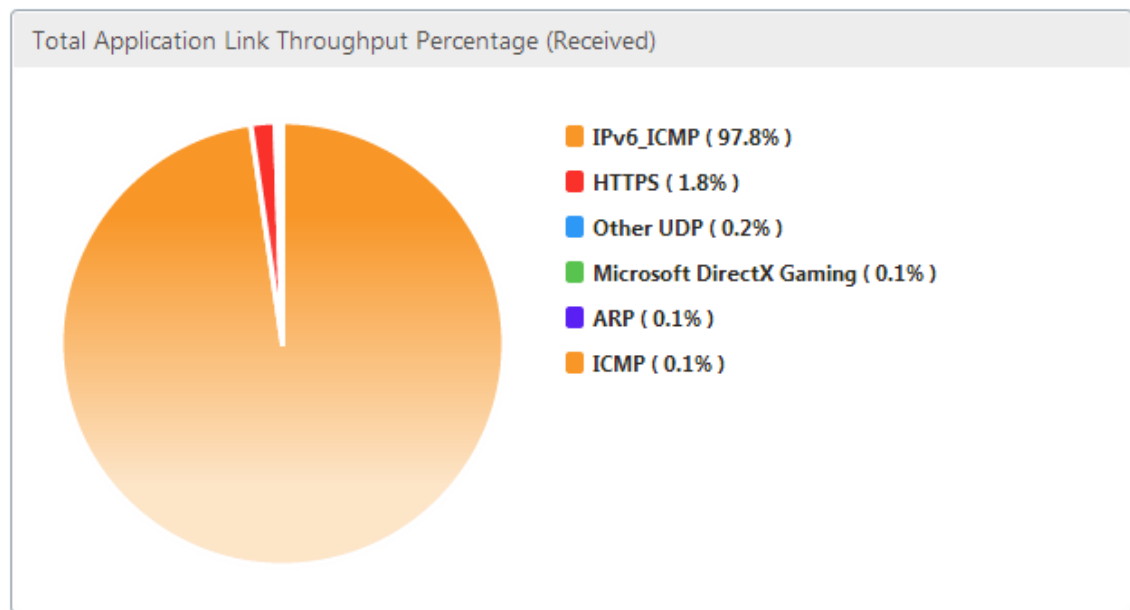
verwenden können, um den Traffic-Durchsatz verschiedener Anwendungen, die von der Citrix SD-WAN Appliance bedient werden, grafisch darzustellen. Standardmäßig wird der Datendurchsatz in letzter Minute angezeigt. Sie können den Zeitrahmen jedoch ändern, indem Sie Last Minute, Last Hour, Last Day, Last Week oder Last Month aus der Liste auf der Titelleiste der Seite auswählen. Diese Seite enthält drei Registerkarten: **Diagramme für Top-Anwendungen, Seit letztem Neustart und Aktive Anwendungen (seit letztem Neustart)**. Die Registerkarte Top Applications Diagramme enthält die folgenden Statistiken:

- **Prozentsatz des Gesamtdurchsatzes für Anwendungsverknüpfungen (gesandt):** Dies ist ein Kreisdiagramm, das den Prozentsatz des Datenverkehrs darstellt, den die Appliance an jede Anwendung gesendet hat. Wenn die Appliance einen erheblichen Prozentsatz des Datenverkehrs für eine Anwendung mit dem IPv6-Protokoll gesendet hat, wird der Prozentsatz des Datenverkehrs in diesem Diagramm dargestellt.

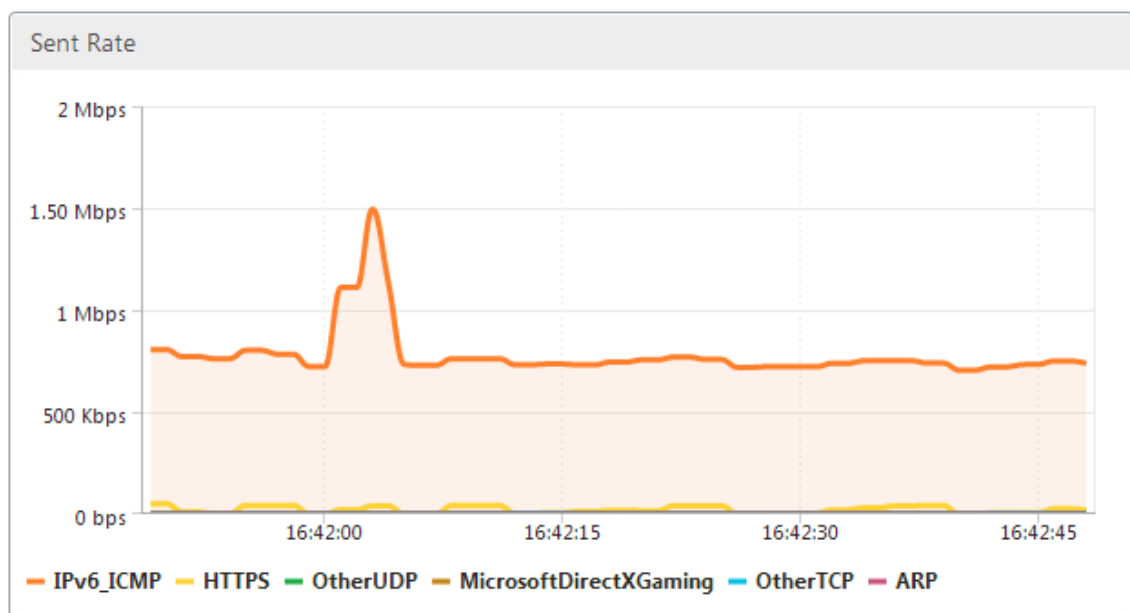


- **Prozentsatz des Gesamtdurchsatzes für Anwendungsverknüpfungen (Empfang):** Dies ist ein Kreisdiagramm, das den Prozentsatz des Datenverkehrs darstellt, den die Appliance von jeder Anwendung erhalten hat. Wenn die Appliance einen signifikanten Prozentsatz des Datenverkehrs von einer Anwendung unter Verwendung des IPv6-Protokolls erhalten hat, zeigt das Diagramm den Prozentsatz des Datenverkehrs an, der von der Anwendung generiert wird.

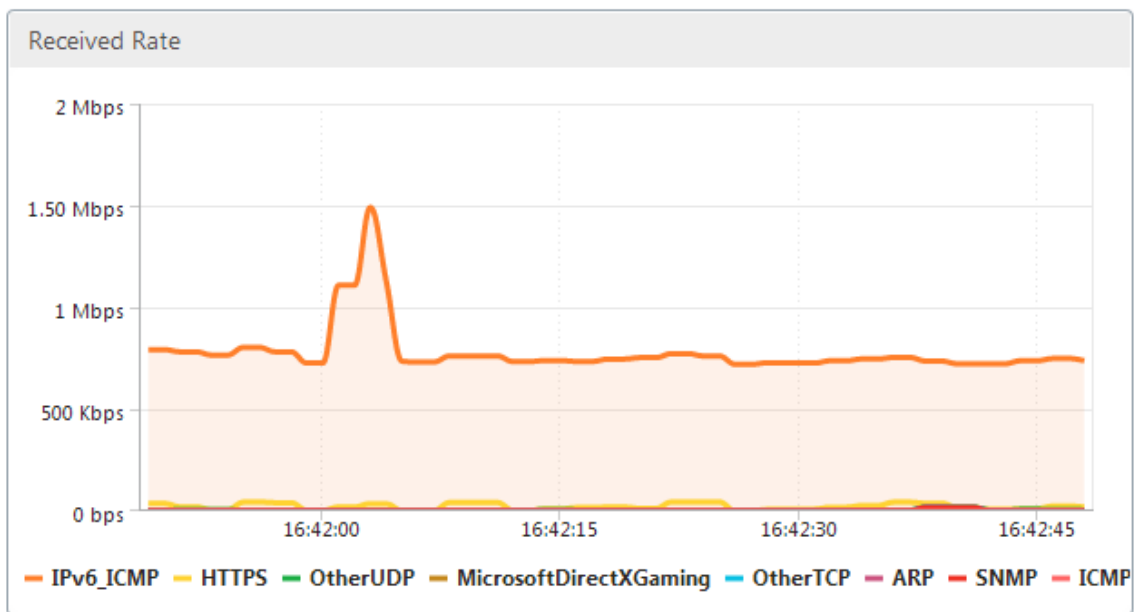




- **Gesendete Rate:** Dies ist ein gestapeltes Diagramm mit Datenreihen, das die Rate in Bits pro Sekunde darstellt, mit der die Appliance Datenverkehr an jede Anwendung gesendet hat. Wenn die Appliance Daten über das IPv6-Protokoll an eine Anwendung gesendet hat, wird in diesem Diagramm auch eine Reihe dargestellt, die jede Anwendung unter Verwendung des IPv6-Protokolls darstellt.



- **Empfangene Rate:** Dies ist ein gestapeltes Diagramm mit Datenreihen, das die Rate in Bits pro Sekunde darstellt, mit der die Appliance Datenverkehr von jeder Anwendung empfangen hat. Wenn die Appliance Daten von einer Anwendung empfangen hat, die das IPv6-Protokoll verwendet, wird in diesem Diagramm auch eine Reihe dargestellt, die jede Anwendung unter Verwendung des IPv6-Protokolls darstellt.



- **Tabelle Top Applications:** Dies ist eine Tabelle mit Statistiken für jede Anwendung. In der Tabelle sind alle Anwendungen aufgeführt, für die die Appliance Datenverkehr bedient hat, sowie gesendete und empfangene Raten in Bit pro Sekunde, gesendete und empfangene Bytes, Prozentsatz des Datenverkehrs für die Anwendung und die Rate, mit der die Appliance den Datenverkehr für die Anwendung bedient hat. Wenn die Appliance Datenverkehr für eine Anwendung unter Verwendung des IPv6-Protokolls bereitgestellt hat, wird die Anwendung zusammen mit ihren Statistiken in dieser Tabelle aufgeführt.

Top Applications						
Application	Sent Rate (bps)	Received Rate (bps)	Total Bytes Sent	Total Bytes Received	Total %	Order
IPv6_ICMP	719.56 K	719.56 K	5.4 M	5.4 M	98.3	1
HTTPS	10.57 K	9.64 K	79.3 K	72.35 K	1.38	2
Microsoft DirectX Gaming	416	416	3.14 K	3.14 K	0.06	4
Other TCP	312	312	2.35 K	2.35 K	0.04	5
Other UDP	128	1.7 K	984	12.73 K	0.12	3
ARP	24	488	232	3.66 K	0.04	6
SNMP	0	496	0	3.76 K	0.03	7
ICMP	0	376	0	2.84 K	0.03	8

- **Anwendungsgruppen:** Dies ist eine Tabelle mit Statistiken für jede Anwendung, zusammen mit der Anwendungsgruppe und der übergeordneten Anwendung, falls vorhanden. Die Tabelle listet die für die Anwendung gesendeten und empfangenen Bytes auf. Jede Anwendung sowie ihre Anwendungsgruppe und übergeordnete Anwendung werden als Hyperlinks angezeigt. Wenn Sie auf den Hyperlink klicken, werden detaillierte Details der Statistiken für den Link angezeigt, auf den Sie geklickt haben. Wenn die Appliance Datenverkehr für eine Anwendung unter Verwendung des IPv6-Protokolls bereitgestellt hat, wird die Anwendung zusammen mit ihren Statistiken in dieser Tabelle aufgeführt.

Application Groups				
Application	Application Group	Parent Application	Bytes Sent	Bytes Received
IPv6_ICMP	IP Protocols	IPv6	5.4 M	5.4 M
HTTPS	Web, Security Protocols	TCP	79.3 K	72.35 K
Microsoft DirectX Gaming	Games	TCP	3.14 K	3.14 K
Other TCP	N/A	N/A	2.35 K	2.35 K
Other UDP	N/A	N/A	984	12.73 K
ARP	Legacy Or Non-IP	N/A	232	3.66 K
SNMP	Network Management, Infrastructure	UDP	0	3.76 K
ICMP	Infrastructure, IP Protocols	IPv6	0	2.84 K

Die Registerkarte **Seit dem letzten Neustart** enthält Statistiken über den Anwendungsdatenverkehr seit dem Neustart der Appliance. Die Registerkarte enthält die Diagramme Gesamter Anwendungsverknüpfungsdurchsatz (gesandt) und Gesamtprozentsatz für Anwendungsverknüpfungen (empfangene) sowie Tabellen Top Applications and Application Groups, in denen Statistiken dargestellt werden, die der Registerkarte Top Applications Diagramme ähneln, jedoch mit Daten seit dem Neustart der Appliance enthalten. Die Registerkarte **Aktive Anwendungen (seit letztem Neustart)** enthält eine Tabelle mit allen aktiven Anwendungen seit dem Neustart der Appliance. Diese Tabelle enthält Details zur gesendeten und empfangenen Rate, Summe gesendeter und empfangener Bytes und Gesamtanzahl der gesendeten und empfangenen Pakete für die Anwendungen.

## Verknüpfungsdefinitionen

April 19, 2021

Verknüpfungsdefinitionen ermöglichen es der Appliance, Überlastung und Verlust Ihrer WAN-Verbindungen zu verhindern und Traffic Shaping durchzuführen. Eine Linkdefinition gibt an, welcher Datenverkehr mit der definierten Verbindung verknüpft ist, die maximale Bandbreite für den empfangenen Datenverkehr auf der Verbindung und die maximale Bandbreite für den über die Verbindung gesendeten Datenverkehr. Die Definition identifiziert außerdem den Datenverkehr als ein- oder ausgehender und als WAN-seitiger oder LAN-seitiger Datenverkehr. Der gesamte Datenverkehr, der durch die Appliance fließt, wird mit der Liste der Verknüpfungsdefinitionen verglichen, und die erste übereinstimmende Definition identifiziert den Link, zu dem der Datenverkehr gehört.

Durch Ausführen des Schnellinstallationsvorgangs passen Sie die Standardverknüpfungsdefinitionen der Appliance an. Anschließend haben Sie die Verbindung der Appliance zum WAN und deren Verknüpfung zum LAN definiert. Für eine einfache Inline-Bereitstellung ist keine weitere Konfiguration der Verknüpfungsdefinitionen erforderlich. Andere Bereitstellungstypen erfordern eine zusätzliche Konfiguration von Verknüpfungsdefinitionen.

Jeder Link hat zwei Bandbreitengrenzen, die die Sendegeschwindigkeit und die Empfangsgeschwindigkeit darstellen. Nur wenn die Verbindungsgeschwindigkeit bekannt ist, kann die

Appliance Datenverkehr mit genau der richtigen Geschwindigkeit in die Verbindung injizieren, wodurch Staus und Paketverlust vermieden werden, die sich aus dem Versuch ergeben, zu viel zu senden, oder der Verlust der Leistung, der durch zu wenig gesendet wird. Wenn die Appliance zwischen einem schnellen LAN und einem langsameren WAN platziert und als *virtuelles Gateway* fungiert, kann der Datenverkehr schneller empfangen, als das WAN ihn akzeptieren kann, wodurch ein Rückstand des Datenverkehrs entsteht. Das Vorhandensein dieses Rückzugs ermöglicht es der Appliance, das Paket auszuwählen, das als nächstes gesendet werden soll, und diese Wahl wiederum ermöglicht die Gestaltung des Datenverkehrs. Es sei denn, es gibt Pakete aus mehreren Streams zur Auswahl, es gibt keine Möglichkeit, einen Stream gegenüber dem anderen zu bevorzugen. Traffic Shaping hängt daher von der Existenz des virtuellen Gateway ab und setzt Bandbreitengrenzen korrekt ein.

#### **Hinweis**

Verknüpfungsdefinitionen gelten normalerweise für Verbindungen mit dem beschleunigten Paar von Bridge-Ports. Die beiden Motherboard-Ports, Primary und Aux1, können auch als Links definiert werden. Dies dient jedoch selten jedem Zweck, da sie für die Verwaltung und als Back-Channel für Hochverfügbarkeits- und Gruppenmodi verwendet werden, nicht für WAN-Datenverkehr.

#### **Wichtig**

Wichtig: Für Linkdefinitionszwecke ist ein *Linke* keine physische Verbindung mit eigener Bandbreitenkapazität. Es ist in der Regel ein Kabel, das das Gebäude verlässt. Beachten Sie die folgenden Punkte:

- Ein VLAN ist keine Verbindung.
- Ein virtueller Link ist kein Link.
- Ein Tunnel ist keine Verbindung.

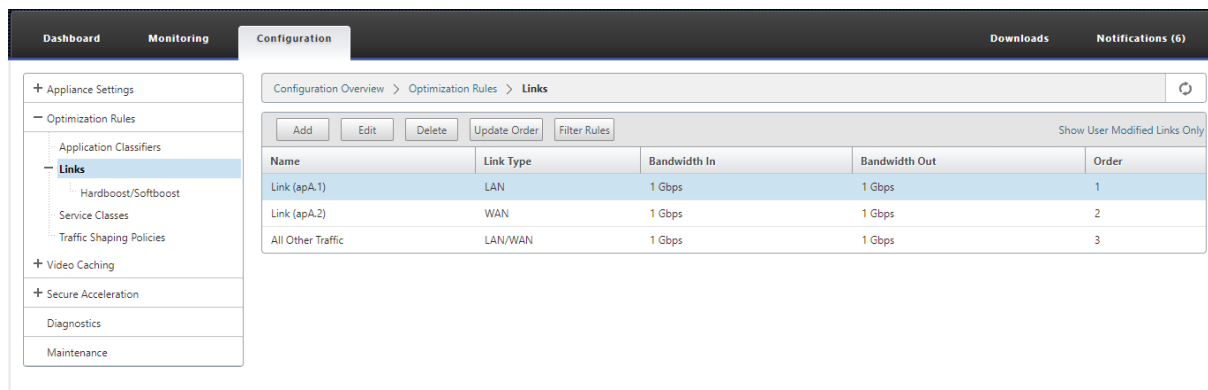
## **Standardverknüpfungsdefinitionen**

Navigieren Sie zu **Konfiguration > Optimierungsregeln > Links**, um die aktuell definierten Links anzuzeigen. Die folgenden Links sind standardmäßig definiert.

1. **APA.1**, einer der beiden Ports auf der beschleunigten Brücke.
2. **APA.2**, der andere Port auf der beschleunigten Brücke.
3. Wenn das System über zwei beschleunigte Brücken verfügt, gibt es auch APB.1 und APB.2.
4. All Other Traffic, der keine echte Verbindung ist, sondern ein Catch-all für Traffic ist, der nicht mit den tatsächlichen Linkdefinitionen übereinstimmt.

Die Reihenfolge, in der die Links auf dieser Seite angezeigt werden, ist signifikant. Wenn Sie entscheiden, zu welcher Verknüpfung ein Paket gehört, testet die Appliance die Links in der Reihenfolge, und

der erste passende Link wird ausgewählt. Dies bedeutet, dass überlappende Definitionen zulässig sind, und die letzte Definition in der Verknüpfung kann mit dem gesamten Datenverkehr übereinstimmen, der als Standardlink dient. Um die Reihenfolge zu ändern, klicken Sie auf **Bestellung aktualisieren**.



## Verwalten von Verknüpfungsdefinitionen in Traffic Shaping

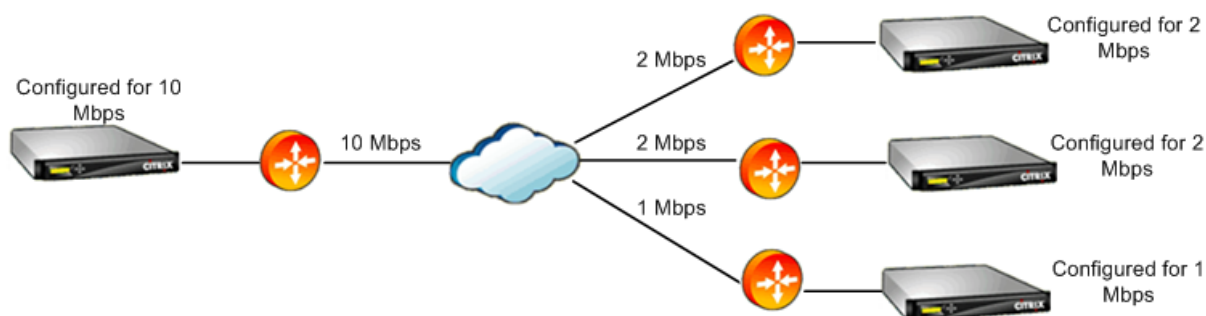
April 19, 2021

Um einen Link zu verwalten, benötigt der Traffic Shaper die folgenden Informationen:

- Die Geschwindigkeit des Links in der Sende- und Empfangsanweisung.
- Ob es sich bei der Verbindung um eine WAN-Verbindung oder ein LAN-Netzwerk handelt.
- Eine Möglichkeit, den Linkverkehr von anderen Traffic zu unterscheiden.
- Die Richtung, in der der Verkehr über die Verbindung fließt.

**Verbindungsgeschwindigkeit**—Die *Verbindungsgeschwindigkeit* bezieht sich immer auf die Geschwindigkeit der physischen Verbindung. Im Falle einer WAN-Verbindung ist es die Geschwindigkeit des WAN-Segments, die mit der Citrix SD-WAN WANOP-Appliance im Gebäude endet. Die Geschwindigkeit des anderen Endes der Verbindung wird nicht berücksichtigt. Die folgende Abbildung zeigt beispielsweise ein Netzwerk von vier Appliances. Jede Appliance hat ihre eingehenden und ausgehenden Bandbreiten auf 95% der Geschwindigkeit ihres eigenen lokalen WAN-Segments, ohne Rücksicht auf die Geschwindigkeit der entfernten Endpunkte.

Abbildung 1. Lokale Bandbreitenbegrenzungen verfolgen lokale Verbindungsgeschwindigkeiten



Der Grund für die Festlegung der Bandbreitengrenzen auf 95% der Verbindungsgeschwindigkeit anstelle von 100% besteht darin, Link-Overhead zu ermöglichen (nur wenige Links können Daten bei 100% ihrer veröffentlichten Geschwindigkeiten tragen) und sicherzustellen, dass die Appliance etwas langsamer ist als die Verbindung, so dass es zu einem leichten Engpass wird. Traffic Shaping ist nur wirksam, wenn der Traffic Shaper der Engpass in der Verbindung ist.

**Unterschiedliche Arten von Datenverkehr unterscheiden**—In jeder Verbindungsdefinition müssen Sie angeben, ob die Definition für eine WAN-Verbindung oder ein LAN-Netzwerk gilt.

Der Traffic Shaper muss wissen, ob ein Paket auf dem WAN unterwegs ist und wenn ja, in welche Richtung. So geben Sie diese Informationen an:

- Bei einfachen Inline-Bereitstellungen erklären Sie, dass ein Port der beschleunigten Bridge zur WAN-Verbindung gehört und der andere Port zum LAN gehört.
- In anderen Bereitstellungsmodi untersucht die Appliance IP-Adressen, MAC-Adressen, VLANs oder WCCP-Dienstgruppen. (Beachten Sie, dass das Testen für WCCP-Dienstgruppen noch nicht unterstützt wird.)
- Wenn ein Standort über mehrere WANs verfügt, müssen die lokalen Verknüpfungsdefinitionen Regeln enthalten, die es der Appliance ermöglichen, den Datenverkehr von verschiedenen WANs zu unterscheiden.

## Konfigurieren von Verknüpfungsdefinitionen

April 19, 2021

Link-Definitionen sind in einer geordneten Liste angeordnet, ein Eintrag pro Link, der von oben nach unten für jedes Paket getestet wird, das die Appliance betreten oder verlässt. Die erste passende Definition bestimmt, zu welcher Verknüpfung das Paket gehört. Innerhalb jeder Linkdefinition befindet sich eine geordnete Liste von Regeln, die ebenfalls von oben nach unten getestet wird. Jedes Paket wird mit diesen Regeln verglichen, und wenn es mit einer von ihnen übereinstimmt, gilt das Paket als über diesen Link unterwegs.

Innerhalb einer einzigen Regel werden die Felder mit einem logischen UND verbunden, so dass alle angegebenen Werte übereinstimmen müssen. Alle Felder sind standardmäßig auf Beliebig, ein Platzhaltereintrag, der immer übereinstimmt. Wenn ein Feld aus einer Liste besteht, z. B. einer Liste von IP-Subnetzen, werden die Listeneinträge mit einem logischen ODER verbunden. Das heißt, wenn ein Element übereinstimmt, wird die Liste als Ganzes als Übereinstimmung betrachtet.

Links können auf dem Ethernet-Adapter basieren, der dem Datenverkehr zugeordnet ist, den Quell- und Ziel-IP-Adressen, dem VLAN-Tag, der WCCP-Dienstgruppe (nur für WCCP-GRE) sowie der Quell- und Ziel-Ethernet-MAC-Adresse. Bei einer einfachen Inline-Bereitstellung werden möglicherweise nur die LAN-seitigen und WAN-seitigen beschleunigten Bridge-Ports (APA.1 und APA.2) identifiziert, während eine komplexe Rechenzentrumsbereitstellung die meisten der bereitgestellten Optionen verwenden muss, um Datenverkehr zu disambiguieren.

Die Definition eines Links in Bezug auf seine IP-Adressen ist möglich, außer wenn redundante Links verwendet werden. Da ein gegebenes Paket entweder einen Link in einer Active-Standby oder eine Active-Active-Active-Dual-Link-Bereitstellung übergehen kann, muss eine andere Methode verwendet werden, um zu bestimmen, welche Verbindung das Paket verwendet. Wenn zwei Brücken verwendet werden, kann der Datenverkehr für eine Verbindung über APA und die andere über aPb gehen, und die Links können in Bezug auf Adapter definiert werden. Wenn die beiden Links von verschiedenen Routern bedient werden, können die MAC-Adressen der Router verwendet werden, um den Datenverkehr auseinander zu bringen. Wenn alles andere fehlschlägt, kann WCCP-GRE verwendet werden, und der Router kann für jede WAN-Verbindung eine andere Servicegruppe verwenden, sodass die Citrix SD-WAN WANOP-Einheit den Verbindungsverkehr nach Servicegruppe unterscheiden kann.

Citrix empfiehlt portbasierte Verknüpfungsdefinitionen für einfache Inline-Bereitstellungen und IP-basierte Verknüpfungsdefinitionen für alle anderen Bereitstellungen.

So konfigurieren Sie Verknüpfungsdefinitionen:

1. Navigieren Sie zu **Konfiguration > Optimierungsregeln > Links**, und klicken Sie auf **Hinzufügen**.

Dashboard Monitoring **Configuration** Downloads Notifications (6)

← Back

**Create Links**

Name\*  
WAN-side link

Link Type\*  
WAN

Bandwidth In\*  
67 mbps

Bandwidth Out\*  
950 mbps

Filter Rules

Add Edit Delete

Adapter	Source IP Address	Dest IP Address	VLAN	WCCP Service Group	Source MAC Address	Destination MAC Address
apA.1	Any	Any	Any	Any	Any	Any

Create Close

2. Geben Sie Werte für die folgenden Parameter ein:

- **Name:** Ein beschreibender Name des Links, der auch beschreiben kann, ob es sich um einen LAN-seitigen oder einen WAN-seitigen Link handelt.
- **Link-Typ:** Der Link-Typ, entweder LAN oder WAN.
- **Bandwidth In:** Das eingehende Bandbreitenlimit.
- **Bandbreitenausgang:** Die ausgehende Bandbreitengrenze.

3. Klicken Sie im Abschnitt **Filterregeln** auf **Hinzufügen**, und geben Sie Werte für die folgenden Parameter ein:

- **Adapter:** Dies gibt eine Liste von Adaptern (Ethernet-Ports) an. Wenn Verbindungen über Ethernet-Adapter identifiziert werden können, vereinfacht dies die Konfiguration.
- **Quell-IP-Adresse:** Die Quell-IP-Regeln werden für Pakete berücksichtigt, die in die Einheit eingehen (Pakete, die die Einheit verlassen, werden ignoriert). Auf diesen Paketen werden die Regeln im Feld Src IP mit dem Feld Quelladresse im IP-Header verglichen. Die Regel gibt eine Liste von IP-Adressen oder Subnetzen an. Negative Übereinstimmungen wie "Exclude 10.0.0.1" werden ebenfalls unterstützt.
- **Ziel-IP-Adresse:** Die Ziel-IP-Regeln werden für Pakete berücksichtigt, die die Einheit verlassen (Pakete, die die Einheit eingehen, werden ignoriert). Auf diesen Paketen werden die Regeln im Feld Dst IP mit dem Feld Zieladresse im IP-Header verglichen. Die Regel gibt eine Liste von IP-Adressen oder Subnetzen an. Negative Übereinstimmungen wie "Exclude 10.0.0.1" werden ebenfalls unterstützt.
- **VLAN:** Die VLAN-Regeln werden auf die VLAN-Header von Paketen angewendet, die in die Einheit eingehen oder sie verlassen.



- **WCCP-Dienstgruppe:** Die WCCP-Dienstgruppenregeln werden auf GRE-gekapselte WCCP-Pakete angewendet, die das Gerät ein- oder verlassen. (Dies funktioniert nicht mit L2 WCCP.)
- **Quell-MAC-Adresse:** Die Quell-MAC-Adresse wird als Filterkriterium verwendet.
- **Ziel-MAC-Adresse:** Die Ziel-MAC-Adresse, die als Dilter-Kriterien verwendet wird.

#### 4. Klicken Sie auf **Erstellen**.

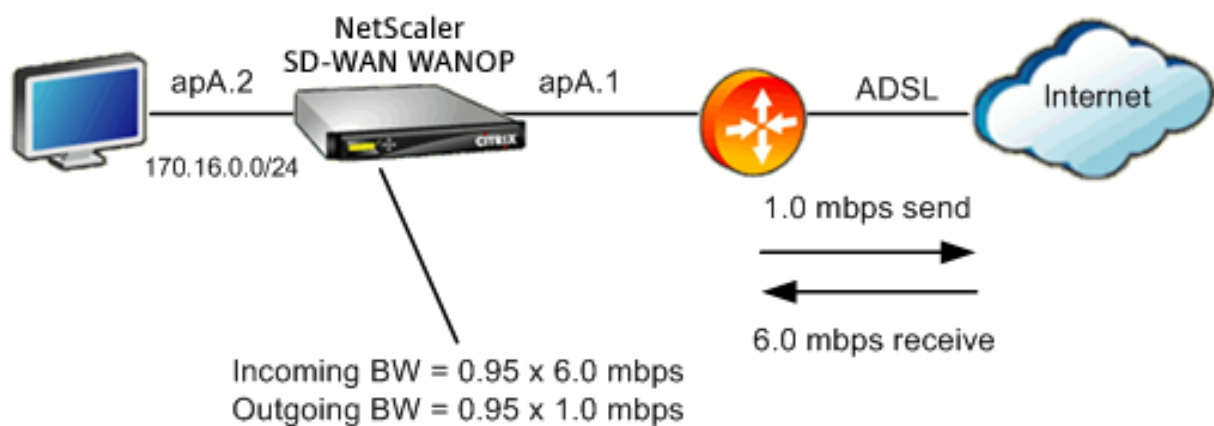
Der Traffic-Klassifikator verwendet die Felder Src IP und Dst IP auf spezialisierte Weise (das gleiche gilt für Src MAC und Dst MAC):

- Das Feld Src wird nur bei Paketen untersucht, die in die Appliance eingegeben werden.
- Die Dst wird nur bei Paketen untersucht, die die Appliance verlassen.

## Inline-Links

Die meisten Citrix SD-WAN WANOP-Appliances verwenden eine einfache Inline-Bereitstellung, bei der jede beschleunigte Bridge nur eine WAN-Verbindung bedient. Dies ist der einfachste Modus zu konfigurieren.

### Einfacher Inline-Link



In der obigen Abbildung wird der gesamte Verkehr, der durch die beschleunigte Brücke führt, als WAN-Datenverkehr angenommen. Der Link ist ein ADSL-Link mit unterschiedlichen Send- und Empfangsgeschwindigkeiten (6,0 Mbit/s nach unten, 1,0 Mbit/s höher). Das WAN ist mit dem beschleunigten Bridge-Port APA.1 verbunden, und das LAN ist mit dem beschleunigten Bridge-Port APA.2 verbunden.

Die Aufgaben zum Definieren des WAN-seitigen Links (APA.1) sind:

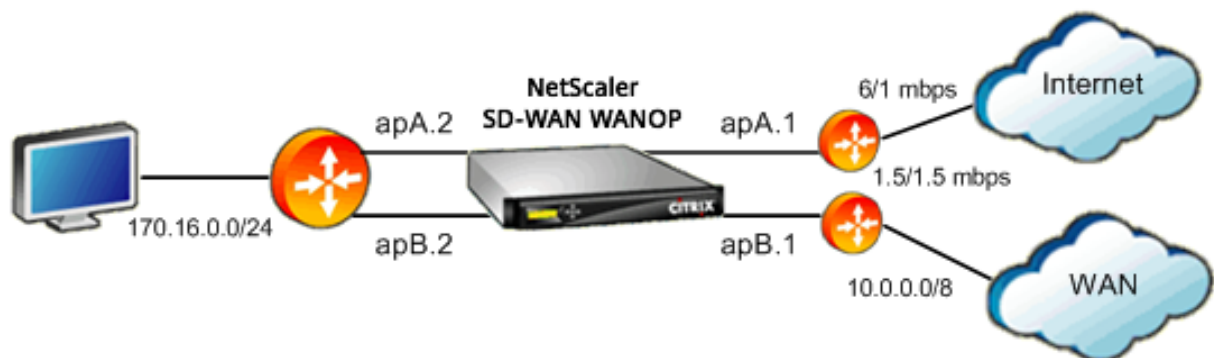
1. Geben Sie dem WAN einen beschreibenden Namen, z. B. WAN an HQ (APA.1).

2. Setzen Sie den Typ auf WAN.
3. Legen Sie die Grenzwerte für eingehende und ausgehende Bandbreite auf 95% der nominalen Verbindungsgeschwindigkeit fest.
4. Stellen Sie sicher, dass eine Regel definiert wurde, die den WAN-Ethernet-Adapter angibt, der in diesem Beispiel APA ist.
5. Klicken Sie auf Erstellen.

Die Aufgaben für die LAN-seitige Verbindung (APA.2) sind ähnlich:

1. Geben Sie ihm einen beschreibenden Namen, z. B. Lokales LAN (APA.2).
2. Setzen Sie den Typ auf LAN.
3. Setzen Sie die Grenzwerte für eingehende und ausgehende Bandbreite auf 95% der nominalen Ethernet-Geschwindigkeit (95 Mbit/s oder 950 Mbit/s).
4. Stellen Sie sicher, dass eine Regel vorhanden ist, die den LAN-Ethernet-Adapter angibt, die in diesem Beispiel APA.2 lautet.
5. Klicken Sie auf Erstellen.

### Inline-Bereitstellung mit zwei Brücken



Die Konfiguration ähnelt der einfachen Inline-Link-Konfiguration, aber die Site verfügt über einen zweiten Link, eine T1-Verbindung zum Unternehmens-WAN, zusätzlich zum ADSL-Internetlink. Die Citrix SD-WAN WANOP-Appliance verfügt über zwei beschleunigte Bridges, eine für jede WAN-Verbindung.

Die Konfiguration ist fast so einfach wie das Single-Bridge-Gehäuse, mit den folgenden zusätzlichen Schritten:

1. Bearbeiten Sie einen zweiten WAN-Link auf aPb, der in diesem Fall apB.1 ist. Setzen Sie den Typ auf WAN. Legen Sie die Verbindungsbandbreite auf 95% der 1,5 Mbit/s T1-Geschwindigkeit fest, und geben Sie der Verbindung einen neuen Namen an, z. B. WAN an HQ.

2. Fügen Sie der Definition LAN eine Regel hinzu, die APB.2 angibt, und löschen Sie die Standardverknüpfungsdefinition für APB.2. (Alternativ können Sie die Standardverknüpfungsdefinition für APB.2 bearbeiten, um sie als LAN-Verbindung anzugeben, wie es für APA.2 getan wurde.)

## Nicht-Inline-Links

Verwenden Sie für andere als einfache Inline-Bereitstellungen (die nur ein WAN pro beschleunigter Bridge bedienen) IP-Subnetze anstelle von Bridge-Ports, um LAN-Datenverkehr vom WAN-Datenverkehr zu unterscheiden. Dieser Ansatz ist für Einarm-Bereitstellungen unerlässlich, die nur einen einzigen Bridge-Port verwenden. IP-Subnetze sind manchmal auch für Inline-Bereitstellungen nützlich, insbesondere wenn die Appliance mehr als ein WAN bedient. Für einfache Inline-Bereitstellungen sind jedoch portbasierte Links einfacher zu definieren.

Der Traffic Classifier wendet eine spezielle Konvention an, wenn die Src IP und Dst IP untersucht wird:

- Das Feld Src IP wird nur in Paketen untersucht, die in die Appliance eingehen.
- Das Feld Dst IP wird nur in Paketen untersucht, die die Appliance verlassen.

Diese Konvention kann manchmal verwirrend sein, aber sie erlaubt es, die Richtung der Paketreise implizit als Teil der Definition zu betrachten.

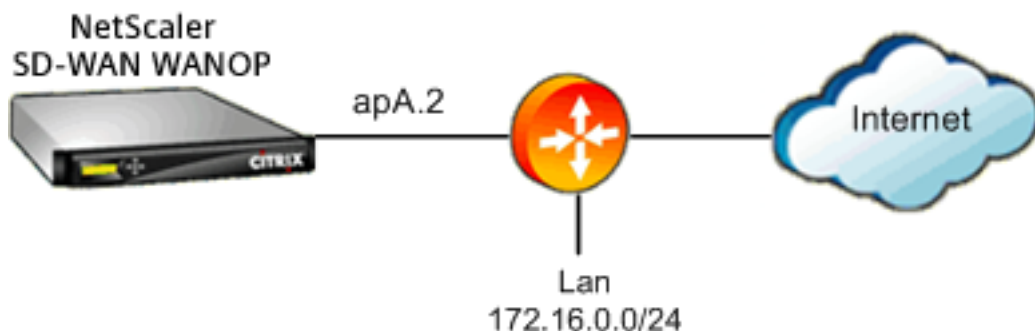
## IP-Adresse in Verknüpfungsdefinitionen verwenden



Um eine einfache Inline-LAN-Definition mithilfe von IP-basierten Regeln zu konfigurieren, können Sie die LAN- und WAN-Verbindungen definieren, ohne die Ethernet-Ports anzugeben. Verwenden Sie stattdessen das LAN-Subnetz:

- Erstellen Sie eine Regel für die LAN-Link-Definition, und geben Sie das LAN-Subnetz im Feld Src IP an.
- Erstellen Sie eine Regel für die WAN-Verbindungsdefinition, und geben Sie das LAN-Subnetz (nicht das WAN-Subnetz) im Feld Dst IP an.

## WCCP und Virtual Inline-Modi



Konfigurations-WCCP oder virtuelle Inline-Bereitstellung unter Verwendung von IP-basierten Regeln entspricht der Verwendung der IP-Adresse in der Linkdefinition, da LAN und WAN IP-Subnetze identisch sind.

Wenn WCCP-GRE verwendet wird, werden die GRE-Header ignoriert und die IP-Header innerhalb der gekapselten Datenpakete verwendet. Daher funktioniert dieselbe Link-Definition für WCCP-L2, WCCP-GRE, Inline und virtuelle Inline-Modi.

(WCCP und virtuelle Inline-Modi erfordern die Konfiguration Ihres Routers. WCCP erfordert auch eine Konfiguration auf der Seite Konfiguration: Erweiterte Bereitstellungen.)

## Verwalten und Überwachen mit Citrix Application Delivery Management

December 14, 2022

Die Unterstützung von Citrix SD-WAN WANOP AppFlow ermöglicht eine flexible, individuelle Überwachung Ihrer Citrix SD-WAN WANOP Appliances.

Die AppFlow Schnittstelle funktioniert mit Citrix Application Delivery Management (ADM). Citrix ADM erhält detaillierte Informationen von der Appliance unter Verwendung des offenen Appliance-Standards (<http://www.appflow.org>). Citrix ADM ermöglicht es Ihnen, Analysen der Citrix SD-WAN Appliances in Ihrem Netzwerk zu überwachen, zu verwalten und anzuzeigen.

Citrix ADM unterstützt eine breite Palette von Geräten und bietet eine umfassendere Ansicht Ihres Netzwerks. Die Citrix SD-WAN WANOP-Appliance bietet einen umfassenden Überblick über den WAN-Datenverkehr, einschließlich detaillierter Statistiken über den Datenverkehr virtueller Apps/Virtual Desktops. Sie bietet wichtige Einblicke in die WAN-Benutzererfahrung.

Weitere Informationen siehe [Verwalten von Citrix SD-WAN Instanzen mit Citrix Application Delivery Management](#).

## Beispiel für Virtual Apps/Virtual Desktops

Wenn in einer Citrix Virtual Apps and Desktops-Umgebung für einen Zweigstellenbenutzer eine geringe Leistung auftritt, muss er möglicherweise das Netzwerk, die Benutzer und Anwendungen überwachen, die auf Virtual Apps oder Virtual Desktops gehostet werden. Die Administratoren müssen möglicherweise folgende Fragen stellen:

- Welcher Teil des Netzwerks verursacht eine schlechte Benutzererfahrung?
- Was ist eine einfache Möglichkeit, die Langsamkeit in veröffentlichten Anwendungen zu identifizieren?
- Welche virtuellen Kanäle verbrauchen über einen bestimmten Zeitraum die größte Bandbreite?
- Welche Virtual Desktops- oder Virtual Apps-Benutzer verbrauchen über einen bestimmten Zeitraum die meisten Bandbreite?
- Was ist für einen bestimmten Virtual Desktops-Benutzer die durchschnittliche client- und serverseitige Latenz und der durchschnittliche Jitter?
- Was sind die wichtigsten Anwendungen für alle Virtual Apps-Benutzer, nach Up-Time und der Gesamtzahl der Starts in einem bestimmten Zeitraum?
- Was ist die Datacenter-Latenz?

Der Citrix SD-WAN WANOP AppFlow Support bietet Antworten auf alle oben genannten Fragen, sodass beispielsweise eine überlastete WAN-Verbindung von einem langsamen Server oder einem langsamen Client unterschieden werden kann.

## Citrix Cloud Connector

April 19, 2021

Die Citrix Cloud Connector-Funktion der Citrix SD-WAN WANOP-Appliance verbindet Unternehmensdatacenter mit externen Clouds und Hosting-Umgebungen und macht die Cloud zu einer sicheren Erweiterung Ihres Unternehmensnetzwerks. Cloud-gehostete Anwendungen werden so angezeigt, als ob sie in einem zusammenhängenden Unternehmensnetzwerk ausgeführt würden. Mit Citrix Cloud Connector können Sie Ihre Rechenzentren um die Kapazität und Effizienz von Cloud-Anbietern erweitern.

Mit dem Citrix Cloud Connector können Sie Ihre Anwendungen in die Cloud verschieben, um Kosten zu senken und die Zuverlässigkeit zu erhöhen.

Die WAN-Optimierungsfunktion der Citrix SD-WAN WANOP-Appliance beschleunigt den Datenverkehr und bietet LAN-ähnliche Leistung für Anwendungen, die in Rechenzentren und Clouds des Unternehmens ausgeführt werden.

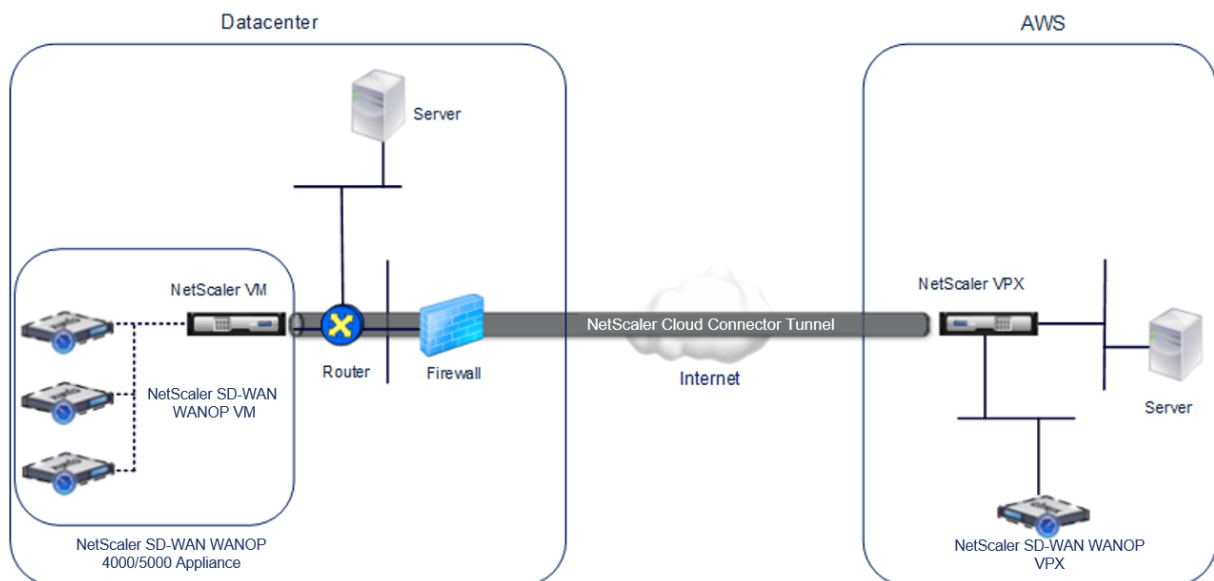
Zusätzlich zur Verwendung von Citrix Cloud Connector zwischen einem Rechenzentrum und einer Cloud können Sie mit ihm zwei Rechenzentren verbinden, um eine sichere und beschleunigte Verbindung mit hoher Kapazität zu erhalten.

Um die Citrix Cloud Connector Lösung zu implementieren, verbinden Sie ein Rechenzentrum mit einem anderen Rechenzentrum oder einer externen Cloud, indem Sie einen Tunnel namens Citrix Cloud Connector -Tunnel einrichten.

Um ein Datacenter mit einem anderen Datacenter zu verbinden, richten Sie einen Citrix Cloud Connector -Tunnel zwischen zwei Appliances ein, eine in jedem Rechenzentrum.

Um ein Rechenzentrum mit einer externen Cloud (z. B. Amazon AWS Cloud) zu verbinden, richten Sie einen Citrix Cloud Connector-Tunnel zwischen einer Citrix SD-WAN WANOP-Appliance im Rechenzentrum und einer virtuellen Appliance (VPX), die sich in der Cloud befindet. Der Remote-Endpunkt kann ein Citrix Cloud Connector oder ein Citrix VPX mit Platin-Lizenz sein.

Die folgende Abbildung zeigt einen Citrix Cloud Connector -Tunnel, der zwischen einem Rechenzentrum und einer externen Cloud eingerichtet wurde.



Die Appliances, zwischen denen ein Citrix Cloud Connector -Tunnel eingerichtet ist, werden als *Endpunkte* oder *Peers* des Citrix Cloud Connector-Tunnels bezeichnet.

Ein Citrix Cloud Connector -Tunnel verwendet die folgenden Protokolle:

- Generisches Routing Encapsulation (GRE) -Protokoll

- Open-Standard-IPsec-Protokoll-Suite, im Transportmodus

Das GRE-Protokoll bietet einen Mechanismus zum Einkapseln von Paketen aus einer Vielzahl von Netzwerkprotokollen, die über ein anderes Protokoll weitergeleitet werden. GRE wird verwendet, um:

- Verbinden Sie Netzwerke mit Nicht-IP- und nicht-routingfähigen Protokollen.
- Brücke über ein WAN (Wide Area Network).
- Erstellen Sie einen Transporttunnel für jede Art von Datenverkehr, der unverändert über ein anderes Netzwerk gesendet werden muss.

Das GRE-Protokoll kapselt Pakete, indem ein GRE-Header und ein GRE-IP-Header zu den Paketen hinzugefügt wird.

Die IPsec-Protokollsuite (Internet Protocol Security) sichert die Kommunikation zwischen Peers im Citrix Cloud Connector -Tunnel.

In einem Citrix Cloud Connector -Tunnel stellt IPSec Folgendes sicher:

- Datenintegrität
- Datenursprungsauthentifizierung
- Datenvertraulichkeit (Verschlüsselung)
- Schutz vor Replay-Angriffen

IPsec verwendet den Transportmodus, in dem das gekapselte GRE-Paket verschlüsselt ist. Die Verschlüsselung erfolgt durch das ESP-Protokoll (Encapsulating Security Payload). Das ESP-Protokoll stellt die Integrität des Pakets mithilfe einer HMAC-Hash-Funktion sicher und gewährleistet die Vertraulichkeit mithilfe eines Verschlüsselungsalgorithmus. Nachdem das Paket verschlüsselt und der HMAC berechnet wurde, wird ein ESP-Header generiert. Der ESP-Header wird nach dem GRE-IP-Header eingefügt und am Ende der verschlüsselten Nutzlast wird ein ESP-Trailer eingefügt.

Peers im Citrix Cloud Connector -Tunnel verwenden das IKE-Protokoll (Internet Key Exchange Version) (Teil der IPsec-Protokollsuite), um eine sichere Kommunikation auszuhandeln, wie folgt:

- Die beiden Peers authentifizieren sich gegenseitig mit einer der folgenden Authentifizierungsmethoden:
  - **Authentifizierung mit vorab freigegebenen Schlüsseln.** Eine Textzeichenfolge, die als Pre-Shared Key bezeichnet wird, wird auf jedem Peer manuell konfiguriert. Die vorab geteilten Schlüssel der Peers werden zur Authentifizierung gegeneinander zugeordnet. Damit die Authentifizierung erfolgreich ist, müssen Sie daher den gleichen vorab freigegebenen Schlüssel auf jedem Peers konfigurieren.

- **Digitale Zertifikatauthentifizierung.** Der Initiator (Absender) Peer signiert Nachrichtenaustauschdaten mithilfe seines privaten Schlüssels, und der andere Empfängerpeer verwendet den öffentlichen Schlüssel des Absenders, um die Signatur zu überprüfen. Normalerweise wird der öffentliche Schlüssel in Nachrichten ausgetauscht, die ein X.509v3-Zertifikat enthalten. Dieses Zertifikat bietet eine Sicherheitsstufe, dass die Identität eines Peers, wie im Zertifikat dargestellt, einem bestimmten öffentlichen Schlüssel zugeordnet ist.
- Die Kollegen verhandeln dann, um eine Einigung zu erzielen über:
  - Ein Verschlüsselungsalgorithmus.
  - Kryptografische Schlüssel zum Verschlüsseln von Daten in einem Peer und zum Entschlüsseln der Daten in der anderen.

Diese Vereinbarung über das Sicherheitsprotokoll, den Verschlüsselungsalgorithmus und die kryptografischen Schlüssel wird als Security Association (SA) bezeichnet. SAs sind einseitig (Simplex). Wenn beispielsweise zwei Peers, CB1 und CB2, über einen Connector-Tunnel kommunizieren, verfügt CB1 über zwei Sicherheitszuordnungen. Eine SA wird für die Verarbeitung ausgehender Pakete verwendet, und die andere SA wird für die Verarbeitung eingehender Pakete verwendet.

SAs verfallen nach einer bestimmten Zeitspanne, die als *Lebensdauer* bezeichnet wird. Die beiden Peers verwenden das IKE-Protokoll (Internet Key Exchange) (Teil der IPsec-Protokollsuite), um neue kryptografische Schlüssel auszuhandeln und neue SAs einzurichten. Der Zweck der begrenzten Lebensdauer ist es, Angreifer daran zu hindern, einen Schlüssel zu knacken.

Außerdem bieten Citrix SD-WAN WANOP-Instanzen auf den Endpunkten des Citrix Cloud Connector-Tunnels eine WAN-Optimierung über den Tunnel.

## Voraussetzungen für die Konfiguration des Citrix Cloud Connector -Tunnels

Bevor Sie einen Citrix Cloud Connector-Tunnel zwischen AWS Cloud und einer Citrix SD-WAN WANOP-Appliance einrichten, die für den Einarmmodus im Rechenzentrum konfiguriert ist, stellen Sie sicher, dass die folgenden Aufgaben abgeschlossen sind:

1. Stellen Sie sicher, dass die Citrix SD-WAN WANOP-Appliance im Rechenzentrum ordnungsgemäß eingerichtet ist. Weitere Informationen zur Bereitstellung einer Citrix SD-WAN WANOP-Appliance im Einarmmodus, der das WCCP/Virtual Inline-Protokoll verwendet, finden Sie unter [Standorte mit einem WAN-Router](#).
2. Installieren, konfigurieren und starten Sie eine virtuelle Citrix Appliance (VPX-Instanz) in der AWS-Cloud. Weitere Informationen finden Sie unter [Installieren von NetScaler VPX auf AWS](#).



3. Installieren, konfigurieren und starten Sie eine Instanz der virtuellen Citrix SD-WAN WANOP Appliance (VPX) in der AWS-Cloud. Weitere Informationen siehe [Installieren von SD-WAN VPX S AMI auf Amazon AWS](#).
4. Binden Sie in AWS die Citrix SD-WAN WANOP VPX-Instanz in AWS an einen virtuellen Lastausgleichsserver in der Citrix VPX-Instanz in AWS. Diese Bindung ist erforderlich, um Datenverkehr durch die Citrix SD-WAN WANOP VPX-Instances zu senden, um eine WAN-Optimierung über den Citrix Cloud Connector-Tunnel zu erreichen.

**So erstellen Sie einen virtuellen Lastausgleichsserver mithilfe der Befehlszeilenschnittstelle:**

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **ns-Modus** l2 aktivieren
- **add lb vserver** <cbvpxonaws\_vs\_name> ANY \* \* **-l2Conn ON -m MAC**</span>

**So fügen Sie die Citrix SD-WAN WANOP VPX-Instanz auf AWS als Service hinzu und binden sie mithilfe der Befehlszeilenschnittstelle an den virtuellen Lastausgleichsserver:**

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add service** < cbvpxonaws\_service\_name> <cbvpxonaws\_IP> ANY \* **-cltTimeout 14400 -svrTimeout 14400**</span>
- **bind lb vserver** <cbvpxonaws\_vs\_name> <cbvpxonaws\_service\_name></span>

## Konfigurieren des Cloud-Connector-Tunnels

April 19, 2021

Um den Citrix Cloud Connector-Tunnel zu konfigurieren, verwenden Sie das Konfigurationsdienstprogramm beider Citrix VPX-Appliances, um die folgenden Aufgaben auszuführen:

- **Erstellen eines IPSec-Profiles**—Eine IPSec-Profileinheit gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK an, die vom IPSec-Protokoll im Citrix Cloud Connector-Tunnel verwendet werden.
- **Erstellen Sie einen IP-Tunnel und verknüpfen Sie das IPSec-Profil damit**—Ein IP-Tunnel gibt die lokale IP-Adresse, die Remote-IP-Adresse, das zur Einrichtung des Citrix Cloud Connector-Tunnels verwendete Protokoll und eine IPSec-Profileinheit an. Die erstellte IP-Tunnel-Entity wird auch als Citrix Cloud Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel und assoziieren Sie den IP-Tunnel mit ihr**—Eine PBR-Entität gibt eine Reihe von Bedingungen und eine IP-Tunnelentität (Citrix Cloud Connector Tunnel) an.

Der Quell-IP-Adressbereich und der Ziel-IP-Bereich sind die Bedingungen für die PBR-Entität. Sie müssen den Quell-IP-Adressbereich und den Ziel-IP-Adressbereich festlegen, um das Subnetz anzugeben, dessen Datenverkehr den Citrix Cloud Connector-Tunnel durchqueren soll. Betrachten Sie beispielsweise ein Anforderungspaket, das von einem Client im Subnetz im Rechenzentrum stammt und für einen Server im Subnetz in der AWS-Cloud bestimmt ist. Wenn dieses Paket dem Quell- und Ziel-IP-Bereich der PBR-Entität auf der virtuellen Citrix Appliance auf der Citrix SD-WAN WANOP-Appliance im Rechenzentrum entspricht, wird es für die Citrix SD-WAN WANOP-Verarbeitung in Betracht gezogen, die das Paket über den Citrix Cloud Connector-Tunnel sendet, der mit der PBR-Entität verknüpft ist.

### **So erstellen Sie mithilfe der Befehlszeilenschnittstelle ein IPSEC-Profil:**

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **ipsec-Profil hinzufügen** <ipsec\_profile\_name> **-EnCalgo** AES **-hasHALGO** HMAC\_SHA1 **-Lebenszeit** 500 **-psk** <password>

### **So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mithilfe der Befehlszeilenschnittstelle an ihn:**

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add iptunnel** <tunnel\_name> <Remote CBC Public IP> <remote\_cbs\_Netmask> <lan\_subnet\_IP> **-Protokoll** GRE **-IPsecProfileName** <ipsec\_profile>

### **So erstellen Sie eine PBR-Regel und binden Sie den IPSEC-Tunnel über die Befehlszeilenschnittstelle daran:**

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr ALLOW** <pbr\_name> **-sRCip** = <local\_lan\_subnet> **-destip** = <remote\_lan\_subnet> **-ipTunnel** <tunnel\_name>
- **apply ns pbrs**

### **So erstellen Sie mithilfe des Konfigurationsdienstprogramms ein IPSEC-Profil:**

1. Navigieren Sie zu **System >Citrix Cloud Connector > IPsec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie im Dialogfeld IPsec-Profil hinzufügen die folgenden Parameter fest:
  - Name
  - Verschlüsselungsalgorithmus
  - Hash-Algorithmus
  - IKE-Protokollversion (wählen Sie V2)

4. Verwenden Sie eine der folgenden IPSec-Authentifizierungsmethoden, die von den beiden Peers zur gegenseitigen Authentifizierung verwendet werden.

- Legen Sie für die Authentifizierungsmethode für Pre-Shared Key Exists den Parameter Pre-Shared Key Exists fest.
- Legen Sie für die Authentifizierungsmethode für digitale Zertifikate die folgenden Parameter fest:

  - Öffentlicher Schlüssel
  - Privater Schlüssel
  - Öffentlicher Peer-Schlüssel

5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

**So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mithilfe des Konfigurationsdienstprogramms daran:**

1. Navigieren Sie zu **System > Citrix Cloud Connector > IP-Tunnel**.
2. Klicken Sie auf der Registerkarte “IPv4 Tunnels” auf **“Add”**.
3. Legen Sie im Dialogfeld IP-Tunnel hinzufügen die folgenden Parameter fest:
  - Name
  - Remote-IP
  - Remote-Maske
  - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option Subnetz-IP).
  - Lokale IP (Alle konfigurierten IPs des ausgewählten IP-Typs werden in der Dropdown-Liste Lokale IP aufgefüllt. Wählen Sie die gewünschte IP aus der Liste aus.)
  - Protokoll
  - IPsec-Profil

4. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

**So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit dem Konfigurationsdienstprogramm daran:**

1. Navigieren Sie zu **System > Netzwerk > PBR**.
2. Klicken Sie auf der Registerkarte PBR auf **Add**.
3. Legen Sie im Dialogfeld PBR erstellen die folgenden Parameter fest:
  - Name

- Aktion
- Nächster Hop-Typ (Wählen Sie IP Tunnel)
- IP-Tunnelname
- Quell-IP Niedrig
- Quell-IP hoch
- Ziel-IP niedrig
- Ziel-IP hoch

4. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

Die neue Tunnelkonfiguration von Citrix Cloud Connector auf der Citrix SD-WAN WANOP-Appliance im Rechenzentrum wird auf der Registerkarte Start der Benutzeroberfläche des Management Service angezeigt.

Die entsprechende neue Citrix Cloud Connector-Tunnelkonfiguration auf der Citrix VPX-Appliance in der AWS-Cloud wird im Konfigurationsdienstprogramm angezeigt.

Der aktuelle Status des Citrix Cloud Connector-Tunnels wird im Bereich Configured Citrix SD-WAN WANOP angegeben. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

## Konfigurieren des Cloud-Connector-Tunnels zwischen zwei Rechenzentren

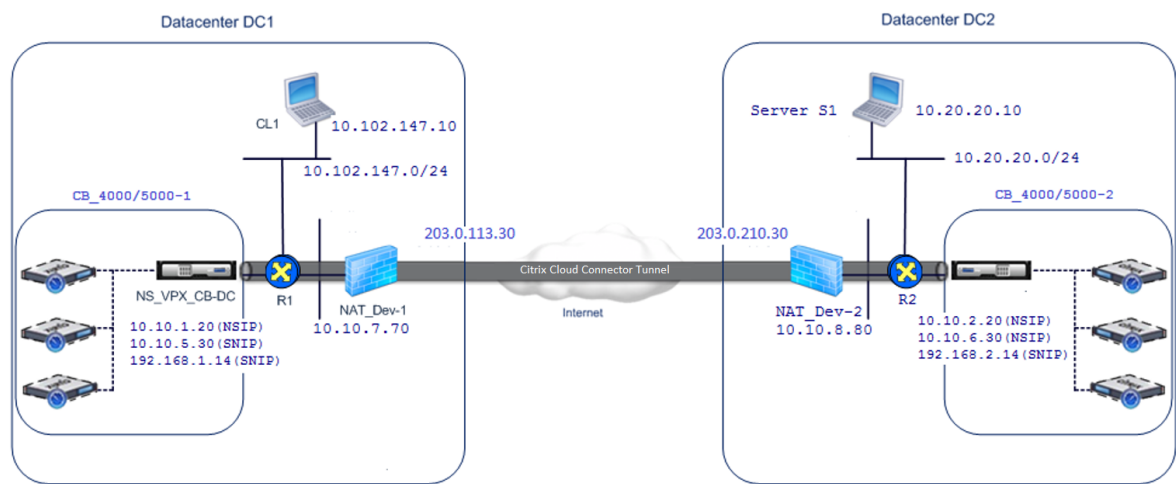
April 19, 2021

Sie können einen Citrix Cloud Connector-Tunnel zwischen zwei verschiedenen Rechenzentren konfigurieren, um Ihr Netzwerk zu erweitern, ohne es neu zu konfigurieren, und die Funktionen der beiden Rechenzentren nutzen. Ein Citrix Cloud Connector-Tunnel zwischen den beiden geografisch getrennten Rechenzentren ermöglicht es Ihnen, Redundanz zu implementieren und Ihr Setup vor Fehlern zu schützen. Der Citrix Cloud Connector-Tunnel trägt dazu bei, eine optimale Auslastung der Infrastruktur und Ressourcen in zwei Rechenzentren zu erreichen. Die Anwendungen, die in den beiden Rechenzentren verfügbar sind, werden für den Benutzer als lokal angezeigt.

Um ein Rechenzentrum mit einem anderen Rechenzentrum zu verbinden, richten Sie einen Citrix Cloud

Connector-Tunnel zwischen einer SD-WAN WANOP 4000/5000-Appliance, die sich in einem Rechenzentrum befindet, und einer anderen SD-WAN WANOP 4000/5000-Appliance, die sich im anderen Rechenzentrum befindet, ein.

Um zu verstehen, wie ein Citrix Cloud Connector-Tunnel zwischen zwei verschiedenen Rechenzentren konfiguriert wird, betrachten Sie ein Beispiel, in dem ein Cloud Connector-Tunnel zwischen der Citrix Appliance CB\_4000/5000-1 im Rechenzentrum DC1 und der Citrix Appliance CB\_4000/5000-2 im Rechenzentrum DC2 eingerichtet wird.



Sowohl CB\_4000/5000-1 als auch CB\_4000/5000-2 funktionieren im Einarmmodus (WCCP/PBR). Sie ermöglichen die Kommunikation zwischen privaten Netzwerken in Rechenzentren DC1 und DC2. Zum Beispiel ermöglichen CB\_4000/5000-1 und CB\_4000/5000-2 die Kommunikation zwischen Client CL1 im Rechenzentrum DC1 und Server S1 im Rechenzentrum DC2 über den Citrix Cloud Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Für die korrekte Kommunikation zwischen CL1 und S1 ist der L3-Modus auf NS\_VPX\_CB\_4000/5000-1 und NS\_VPX\_CB\_4000/5000-2 aktiviert, und Routen sind wie folgt konfiguriert:

- Router R1 hat eine Route zum Erreichen von S1 bis NS\_VPX\_CB\_4000/5000-1.
- NS\_VPX\_CB\_4000/5000\_1 hat eine Route zum Erreichen von NS\_VPX-CB\_4000/5000-2 bis R1.
- S1 sollte eine Route haben, die CL1 bis NS\_VPX-CB\_4000/5000-2 erreicht.
- NS\_VPX-CB\_4000/5000-2 hat eine Route zum Erreichen von NS\_VPX\_CB\_4000/5000-1 bis R2.

In der folgenden Tabelle sind die Einstellungen für CB\_4000/5000-1 im Rechenzentrum DC1 aufgeführt.

Entität	Name	Details
IP-Adresse des Clients CL1		10.102.147.10
<b>Einstellungen auf NAT-Dev-1</b>		
NAT-IP-Adresse auf der öffentlichen Seite		203.0.113.30*

Entität	Name	Details
NAT-IP-Adresse auf privater Seite <b>Einstellungen auf CB_4000/5000-1</b>		10.10.7.70
IP-Adresse des Verwaltungsdienstes CB_4000/5000-1 <b>Einstellungen auf NS_VPX_CB_4000/5000-1 unter CB_4000/5000-1</b>		10.10.1.10
Die NSIP-Adresse		10.10.1.20
SNIP-Adresse		10.10.5.30
Cloud Connector Tunnel	Cloud_Connector_DC1-DC2	<p>Lokale Endpunkt-IP-Adresse des Citrix Cloud Connector-Tunnels = 10.10.5.30, Remote-Endpunkt-IP-Adresse des Citrix Cloud Connector-Tunnels = 203.0.210.30*</p> <p><b>GRE-Tunnel details</b></p> <p>Name : Cloud_Connector_DC1-DC2</p> <p><b>IPSec-Profil details</b></p> <p>Name = Cloud_Connector_DC1-DC2, Verschlüsselungsalgorithmus = AES, Hash-Algorithmus = HMAC SHA1</p>

Entität	Name	Details
Richtlinienbasierte Route	CBC_DC1_DC2_PBR	Quell-IP-Bereich = Subnetz im Datacenter1 = 10.102.147.0-10.102.147.255, Ziel-IP-Bereich = Subnetz im Datacenter2 = 10.20.20.0-10.20.20.255, Nächster Hop-Typ = IP-Tunnel, IP-Tunnelname = CBC_DC1_DC2

\*Dies sollten öffentliche IP-Adressen sein.

In der folgenden Tabelle sind die Einstellungen für CB- 4000/5000-2 im Rechenzentrum DC2 aufgeführt.

Entität	Name	Details
IP-Adresse des Servers S1		10.20.20.10
<b>Einstellungen auf NAT-Dev-2</b>		
NAT-IP-Adresse auf der öffentlichen Seite		203.0.210.30*
NAT-IP-Adresse auf privater Seite		10.10.8.80
<b>Einstellungen auf CB_4000/5000-2</b>		
Verwaltungsdienst-IP-Adresse von CB_SDX-1		10.10.2.10
<b>Einstellungen auf NS_VPX_CB_4000/5000-2 unter CB_4000/5000-2</b>		
Die NSIP-Adresse		10.10.2.20
SNIP-Adresse		10.10.6.30

Entität	Name	Details
Citrix Cloud Connector -Tunnel	Cloud_Connector_DC1-DC2	<p>Lokale Endpunkt-IP-Adresse des Citrix Cloud Connector-Tunnels = 10.10.6.30, Remote-Endpunkt-IP-Adresse des Citrix Cloud Connector-Tunnels = 203.0.113.30*</p> <p><b>GRE-Tunnel details</b></p> <p>Name : Cloud_Connector_DC1-DC2</p> <p><b>IPSec-Profil details</b></p> <p>Name = Cloud_Connector_DC1-DC2, Verschlüsselungsalgorithmus = AES, Hash-Algorithmus = HMAC SHA1</p>
Richtlinienbasierte Route	CBC_DC1_DC2_PBR	<p>Quell-IP-Bereich = Subnetz im Datencenter 2 = 10.20.20.0-10.20.20.255, Ziel-IP-Bereich = Subnetz im Datencenter 1 = 10.102.147.0-10.102.147.255, Nächster Hop-Typ = IP-Tunnel, IP-Tunnelname = CBC_DC1_DC2</p>

\*Dies sollten öffentliche IP-Adressen sein.

Es folgt der Verkehrsfluss im Citrix Cloud Connector-Tunnel:

1. Client CL1 sendet eine Anforderung an Server S1.
2. Die Anfrage erreicht die virtuelle Citrix Appliance NS\_VPX\_CB\_4000/5000-1, die auf der Citrix SD-WAN WANOP-Anwendung CB\_4000/5000-1 ausgeführt wird.
3. NS\_VPX\_CB\_4000/5000-1 leitet das Paket zur WAN-Optimierung an eine der SD-WAN WANOP-Instanzen weiter, die auf der Citrix SD-WAN WANOP-Appliance CB\_4000/5000-1 ausgeführt werden. Nach der Verarbeitung des Pakets gibt die SD-WANOP-Instanz das Paket an



NS\_VPX\_CB\_4000/5000-1 zurück.

4. Das Anforderungspaket entspricht der in der PBR-Entität CBC\_DC1\_DC2\_PBR (konfiguriert in NS\_VPX\_CB\_4000/5000-1) angegebenen Bedingung, da die Quell-IP-Adresse und die Ziel-IP-Adresse des Anforderungspakets zum Quell-IP-Bereich bzw. Ziel-IP-Bereich gehören, der in CBC\_DC1\_DC2\_PBR festgelegt ist.
5. Da der Tunnel CBC\_DC1\_DC2\_PBR an CBC\_DC1\_DC2\_PBR gebunden ist, bereitet die Appliance das Paket vor, das über den Cloud\_Connector\_DC1-DC2-Tunnel gesendet werden soll.
6. NS\_VPX\_CB\_4000/5000-1 verwendet das GRE-Protokoll, um jedes der Anforderungspakete zu kapseln, indem ein GRE-Header und ein GRE-IP-Header zum Paket hinzugefügt wird. Im GRE-IP-Header ist die Ziel-IP-Adresse die Adresse des Cloud-Connector-Tunnels (Cloud\_Connector\_DC1-DC2) im Rechenzentrum DC2.
7. Für den Cloud Connector-Tunnel Cloud\_Connector\_DC1-DC2 überprüft NS\_VPX\_CB\_4000/5000-1 die storedIPSec-Sicherheitszuordnungsparameter (SA) für die Verarbeitung ausgehender Pakete, wie zwischen NS\_VPX\_CB\_4000/5000-1 und NS\_VPX\_CB\_4000/5000-2 vereinbart. Das IPSec Encapsulating Security Payload (ESP) -Protokoll in NS\_VPX\_CB\_4000/5000-1 verwendet diese SA-Parameter für ausgehende Pakete, um die Nutzlast des GRE-gekapselten Pakets zu verschlüsseln.
8. Das ESP-Protokoll gewährleistet die Integrität und Vertraulichkeit des Pakets, indem es die HMAC-Hash-Funktion und den Verschlüsselungsalgorithmus verwendet, der für den Citrix Cloud Connector-Tunnel Cloud\_Connector\_DC1-DC2 angegeben ist. Das ESP-Protokoll erzeugt nach Verschlüsselung der GRE-Nutzlast und Berechnung des HMAC einen ESP-Header und einen ESP-Trailer und fügt diese vor bzw. am Ende der verschlüsselten GRE-Nutzlast ein.
9. NS\_VPX\_CB\_4000/5000-1 sendet das resultierende Paket NS\_VPX\_CB\_4000/5000-2.
10. NS\_VPX\_CB\_4000/5000-2 überprüft die gespeicherten IPSec-Sicherheitszuordnungsparameter (SA) für die Verarbeitung eingehender Pakete, wie zwischen CB\_DC-1 und NS\_VPX-AWS für den Cloud Connector-Tunnel Cloud\_Connector\_DC1-DC2 vereinbart. Das IPSec-ESP-Protokoll auf NS\_VPX\_CB\_4000/5000-2 verwendet diese SA-Parameter für eingehende Pakete und den ESP-Header des Anforderungspakets, um das Paket zu entschlüsseln.
11. NS\_VPX\_CB\_4000/5000-2 entkapselt dann das Paket, indem der GRE-Header entfernt wird.
12. NS\_VPX\_CB\_4000/5000-2 leitet das resultierende Paket an CB\_VPX\_CB\_4000/5000-2 weiter, wodurch WAN-optimierungsbezogene Verarbeitung auf das Paket angewendet wird. CB\_VPX\_CB\_4000/5000-2 gibt dann das resultierende Paket an NS\_VPX\_CB\_4000/5000-2 zurück.
13. Das resultierende Paket ist dasselbe, das von CB\_VPX\_CB\_4000/5000-2 in Schritt 2 empfangen wurde. Dieses Paket hat die Ziel-IP-Adresse auf die IP-Adresse des Servers S1 festgelegt. NS\_VPX\_CB\_4000/5000-2 leitet dieses Paket an Server S1 weiter.

14. S1 verarbeitet das Anforderungspaket und sendet ein Antwortpaket. Die Ziel-IP-Adresse im Antwortpaket ist die IP-Adresse von Client CL1, und die Quell-IP-Adresse ist die IP-Adresse des Servers S1.

## **Konfigurieren des Cloud-Connector-Tunnels zwischen einem Rechenzentrum und AWS/Azure**

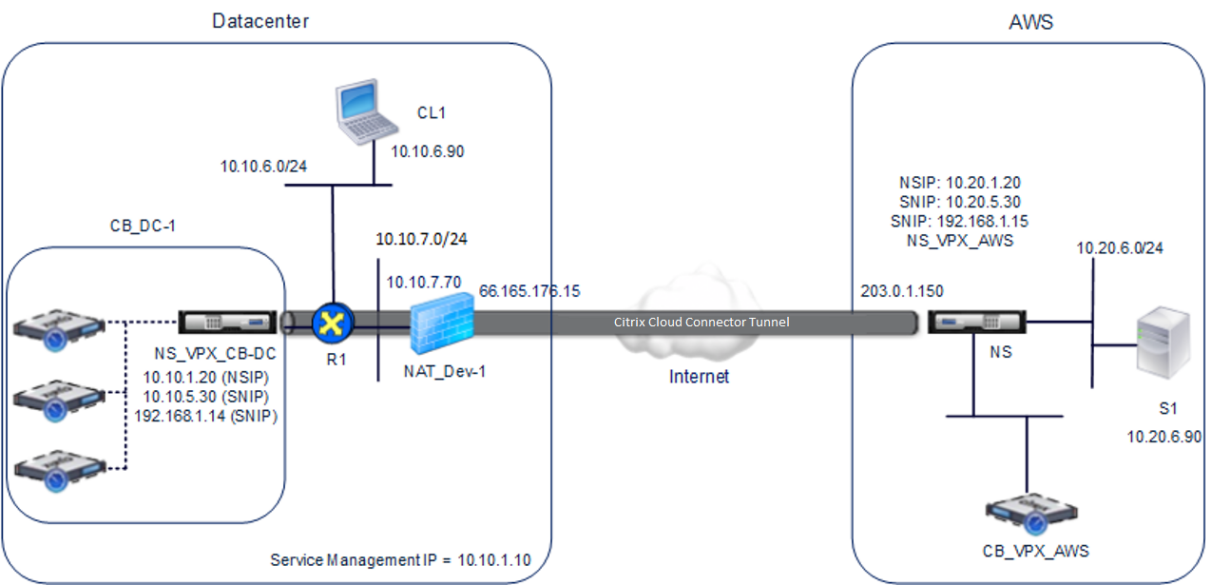
April 19, 2021

Sie können einen Cloud Connector-Tunnel zwischen einem Rechenzentrum und AWS oder Azure-Cloud konfigurieren.

Betrachten Sie ein Beispiel, in dem ein Citrix Cloud Connector-Tunnel zwischen der Citrix SD-WAN WANOP-Appliance CB\_DC-1, die im Einarmmodus WCCP/PBR in einem Rechenzentrum bereitgestellt wird, und einer AWS-Cloud konfiguriert ist. CB\_DC-1 ist mit dem Router R1 verbunden. Ein NAT-Gerät ist auch für Verbindungen zwischen dem Rechenzentrum und dem Internet mit R1 verbunden.

Hinweis: Die Einstellungen im Beispiel würden auch für jede Art von Citrix SD-WAN WANOP-Bereitstellung funktionieren. Diese Einstellung in diesem Beispiel enthält richtlinienbasierte Routen anstelle von Netbridge, damit der Datenverkehr des gewünschten Subnetzes durch den Citrix Cloud Connector-Tunnel geleitet wird.

Wie in der folgenden Abbildung gezeigt, wird der Citrix Cloud Cloud-Connector-Tunnel zwischen der virtuellen Citrix Appliance NS\_VPX\_CB-DC hergestellt, die auf der Citrix SD-WAN WANOP-Appliance CB\_DC-1 ausgeführt wird, und Citrix Virtual Appliance NS\_VPX-AWS, die in der AWS-Cloud ausgeführt wird. Zur WAN, die den Datenverkehr über den Citrix Cloud Connector-Tunnel optimiert, wird NS\_VPX\_CB-DC mit Citrix SD-WAN WANOP-Instanzen gepaart, die auf CB\_DC-1 ausgeführt werden, und auf der AWS-Seite ist die virtuelle Citrix SD-WAN WANOP-Anwendung CB\_VPX-AWS, die auf AWS ausgeführt wird, mit NS\_VPX-AWS verbunden.



In der folgenden Tabelle werden die Einstellungen im Datacenter in diesem Beispiel aufgeführt.

Entität	Name	Details
IP-Adresse des Clients CL1		10.10.6.90
<b>Einstellungen auf NAT-Dev-1</b>		
NAT-IP-Adresse auf der öffentlichen Seite		66.165.176.15 *
NAT-IP-Adresse auf privater Seite		10.10.7.70
<b>Einstellungen auf CB_DC-1</b>		
Verwaltungsdienst-IP-Adresse von CB_DC-1		10.10.1.10
<b>Einstellungen auf NS_VPX_CB-DC unter CB_DC-1</b>		
Die NSIP-Adresse		10.10.1.20
SNIP-Adresse		10.10.5.30
IPSec-Profil	CBC_DC_AWS_IPSec_Profil	IKE-Version = v2, Verschlüsselungsalgorithmus = AES, Hash-Algorithmus = HMAC SHA1

Entität	Name	Details
Cloud Connector Tunnel	CBC_DC_AWS	Lokale Endpunkt-IP-Adresse des Cloud Connector -Tunnels = 10.10.5.30, Remote-Endpunkt-IP-Adresse des Cloud Connectors = Öffentliche EIP-Adresse zugeordnet Cloud Connector-Endpunktadresse (SNIP) auf NS_VPX-AWS auf AWS = 203.0.1.150*, Tunnelprotokoll = GRE und IPSEC, IPSec-Profilname = CBC_DC_AWS_IPSec_profile
Richtlinienbasierte Route	CBC_DC_AWS_PBR	Quell-IP-Bereich = Subnetz im Rechenzentrum = 10.10.6.0-10.10.6.255, Ziel-IP-Bereich =Subnetz in AWS=10.20.6.0-10.20.6.255, Nächster Hop-Typ = IP-Tunnel, IP-Tunnelname = CBC_DC_AWS

\*Dies sollten öffentliche IP-Adressen sein.

In der folgenden Tabelle werden die Einstellungen in der AWS-Cloud in diesem Beispiel aufgeführt.

Entität   Name   Details
———   —   ———
IP-Adresse des Servers S1     10.20.6.90
**Einstellungen auf NS_VPX-AWS**
NSIP-Adresse     10.20.1.20
Öffentliche EIP-Adresse, die der NSIP-Adresse zugeordnet ist     203.0.1.120*
SNIP-Adresse     10.20.5.30
Öffentliche EIP-Adresse, die der SNIP-Adresse zugeordnet ist     203.0.1.150*
IPSec profile   CBC_DC_AWS_IPSec_Profile
IKE version = v2, Encryption algorithm = AES, Hash algorithm = HMAC SHA1
Cloud Connector tunnel   CBC_DC_AWS   Local endpoint IP address of the Cloud Connector tunnel =10.20.5.30, Remote endpoint IP address of the Cloud Connector tunnel = Public NAT IP address of NAT device NAT-Dev-1 in the datacenter = 66.165.176.15*, Tunnel protocol = GRE and IPSEC, IPSec profile

```
name = CBC_DC_AWS_IPSec_Profile |
| Policy based route | CBC_DC_AWS_PBR | Source IP range = Subnet in the AWS = 10.20.6.0-10.20.6.255,
Destination IP range = Subnet in datacenter = 10.10.6.0-10.10.6.255, Next hop type = IP Tunnel, IP tun-
nel name = CBC_DC_AWS |
```

\*Dies sollten öffentliche IP-Adressen sein.

Sowohl NS\_VPX\_CB-DC auf CB\_DC-1 als auch NS\_VPX-AWS funktionieren im L3-Modus. Sie ermöglichen die Kommunikation zwischen privaten Netzwerken im Rechenzentrum und AWS-Cloud. NS\_VPX\_CB-DC und NS\_VPX-AWS ermöglichen die Kommunikation zwischen Client CL1 im Rechenzentrum und Server S1 in der AWS-Cloud über den Cloud Connector -Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Hinweis: AWS unterstützt den L2-Modus nicht. Daher ist es notwendig, nur den L3-Modus auf beiden Endpunkten aktiviert zu haben.

Für die ordnungsgemäße Kommunikation zwischen CL1 und S1 ist der L3-Modus auf NS\_VPX\_CB-DC und NS\_VPX-AWS aktiviert, und Routen werden wie folgt konfiguriert:

- R1 hat eine Route, um S1 über NS\_VPX\_CB-DC zu erreichen.
- NS\_VPX\_CB-DC hat eine Route zum Erreichen von NS\_VPX-AWS über R1.
- S1 sollte eine Route haben, die CL1 über NS\_VPX-AWS erreicht.
- NS\_VPX-AWS verfügt über eine Route zum Erreichen von NS\_VPX\_CB-DC über einen Upstream-Router.

Im Folgenden sind die Routen aufgeführt, die auf verschiedenen Netzwerkgeräten im Rechenzentrum konfiguriert sind, damit der Cloud Connector -Tunnel ordnungsgemäß funktioniert:

Routen	Network	Gateway
<b>Routen auf Router R1</b>		
Route zum Erreichen des Servers S1	10.20.6.X/24	Tunnelendpunkt SNIP-Adresse NS_VPX_CB-DC = 10.10.5.30
Route zum Erreichen des entfernten Endpunkts des Cloud Connector -Tunnels	EIP-Adresse, die der Cloud Connector SNIP-Adresse NS_VPX-AWS zugeordnet ist = 203.0.1.50	Private IP-Adresse des NAT-Geräts = 10.10.7.70
<b>Routen auf NS_VPX_CB-DC</b>		
Route zum Erreichen von NS_VPX-AWS	EIP-Adresse, die der Cloud Connector SNIP-Adresse NS_VPX-AWS zugeordnet ist = 203.0.1.50	IP-Adresse von R1 = 10.10.5.1

Im Folgenden sind die Routen aufgeführt, die auf verschiedenen Netzwerkgeräten in der AWS-Cloud konfiguriert sind, damit der Cloud Connector -Tunnel ordnungsgemäß funktioniert:

Routen	Network	Gateway
<b>Routen auf Server S1</b>		
Route zum Erreichen von Client CL1	10.10.6.X/24	Tunnelendpunkt SNIP-Adresse von NS_VPX-AWS = 10.10.6.1
<b>Routen auf der virtuellen Citrix Appliance NS_VPX-AWS</b>		
Route zum Erreichen von NS_VPX_CB-DC	Öffentliche IP-Adresse von Nat_dev-1 im Rechenzentrum = 66.165.176.15*	IP-Adresse des Upstream-Routers in AWS

Im Folgenden ist der Datenverkehr eines Anforderungspakets von Client CL1 im Cloud Connector -Tunnel:

1. Client CL1 sendet eine Anforderung an Server S1.
2. Die Anfrage erreicht die virtuelle Citrix Appliance NS\_VPX\_CB-DC, die auf der Citrix SD-WAN WANOP-Appliance CB\_DC-1 ausgeführt wird.
3. NS\_VPX\_CB-DC leitet das Paket zur WAN-Optimierung an eine der Citrix SD-WAN WANOP-Instanzen weiter, die auf der Citrix SD-WAN WANOP-Appliance CB\_DC-1 ausgeführt werden. Nach der Verarbeitung des Pakets gibt die Citrix SD-WAN WANOP-Instanz das Paket an NS\_VPX\_CB-DC zurück.
4. Das Anforderungspaket entspricht der in der PBR-Entität CBC\_DC\_AWS\_PBR (konfiguriert in NS\_VPX\_CB-DC) angegebenen Bedingung, da die Quell-IP-Adresse und die Ziel-IP-Adresse des Anforderungspakets zum Quell-IP-Bereich bzw. Ziel-IP-Bereich gehören, der in CBC\_DC\_AWS\_PBR festgelegt ist.
5. Da der Cloud-Connector-Tunnel CBC\_DC\_AWS an CBC\_DC\_AWS\_PBR gebunden ist, bereitet die Appliance das Paket vor, das über den CBC\_DC\_AWS-Tunnel gesendet werden soll.
6. NS\_VPX\_CB-DC verwendet das GRE-Protokoll, um jedes der Anforderungspakete zu kapseln, indem ein GRE-Header und ein GRE-IP-Header zum Paket hinzugefügt wird. Der GRE-IP-Header hat die Ziel-IP-Adresse auf die IP-Adresse des Cloud Connector-Tunnels (CBC\_DC-AWS) auf AWS-Seite festgelegt.
7. Für den Cloud Connector -Tunnel CBC\_DC-AWS prüft NS\_VPX\_CB-DC die gespeicherten IPSec-Sicherheitszuordnungsparameter (SA) für die Verarbeitung ausgehender Pakete, wie zwischen NS\_VPX\_CB-DC und NS\_VPX-AWS vereinbart. Das IPSec Encapsulating Security Payload (ESP)

- Protokoll in NS\_VPX\_CB-DC verwendet diese SA-Parameter für ausgehende Pakete, um die Nutzlast des gekapselten GRE-Pakets zu verschlüsseln.
8. Das ESP-Protokoll gewährleistet die Integrität und Vertraulichkeit des Pakets durch Verwendung der HMAC-Hash-Funktion und des Verschlüsselungsalgorithmus, der für den Cloud Connector -Tunnel CBC\_DC-AWS angegeben ist. Das ESP-Protokoll erzeugt nach Verschlüsselung der GRE-Nutzlast und Berechnung des HMAC einen ESP-Header und einen ESP-Trailer und fügt diese vor bzw. am Ende der verschlüsselten GRE-Nutzlast ein.
  9. NS\_VPX\_CB-DC sendet das resultierende Paket an NS\_VPX-AWS.
  10. NS\_VPX-AWS prüft die gespeicherten IPSec-Sicherheitszuordnungsparameter (SA) für die Verarbeitung eingehender Pakete, wie zwischen CB\_DC-1 und NS\_VPX-AWS für den Cloud Connector -Tunnel CBC\_DC-AWS vereinbart. Das IPsec-ESP-Protokoll auf NS\_VPX-AWS verwendet diese SA-Parameter für eingehende Pakete und den ESP-Header des Anforderungspakets, um das Paket zu entschlüsseln.
  11. NS\_VPX-AWS entkapselt dann das Paket, indem der GRE-Header entfernt wird.
  12. NS\_VPX-AWS leitet das resultierende Paket an CB\_VPX-AWS weiter, wodurch die WAN-Optimierung bezogene Verarbeitung auf das Paket angewendet wird. CB\_VPX-AWS gibt dann das resultierende Paket an NS\_VPX-AWS zurück.
  13. Das resultierende Paket ist das gleiche Paket wie das von CB\_DC-1 in Schritt 2 empfangene Paket. Dieses Paket hat die Ziel-IP-Adresse auf die IP-Adresse des Servers S1 festgelegt. NS\_VPX-AWS leitet dieses Paket an Server S1 weiter.
  14. S1 verarbeitet das Anforderungspaket und sendet ein Antwortpaket. Die Ziel-IP-Adresse im Antwortpaket ist die IP-Adresse von Client CL1, und die Quell-IP-Adresse ist die IP-Adresse des Servers S1.

## Office 365-Beschleunigung

April 19, 2021

Citrix SD-WAN WANOP optimiert WAN, um eine konsistente Benutzererfahrung für Geschäftsanwendungen in Zweigstellen und Remote-Standorten zu bieten.

Microsoft Office 365 ist eine SaaS-Anwendung (Software-as-a-Service), die die Office-Suite von Microsoft für Unternehmensanwendungen bereitstellt. Diese Anwendung wird in der Cloud gehostet und wird bei Bedarf an Benutzer bereitgestellt.

Die Office 365-Beschleunigungsfunktion ermöglicht es den Zweigstellen, die Optimierungsvorteile zu nutzen, die Citrix SD-WAN WANOP für Microsoft Office 365-Anwendungen bietet.

## Anwendungsfall

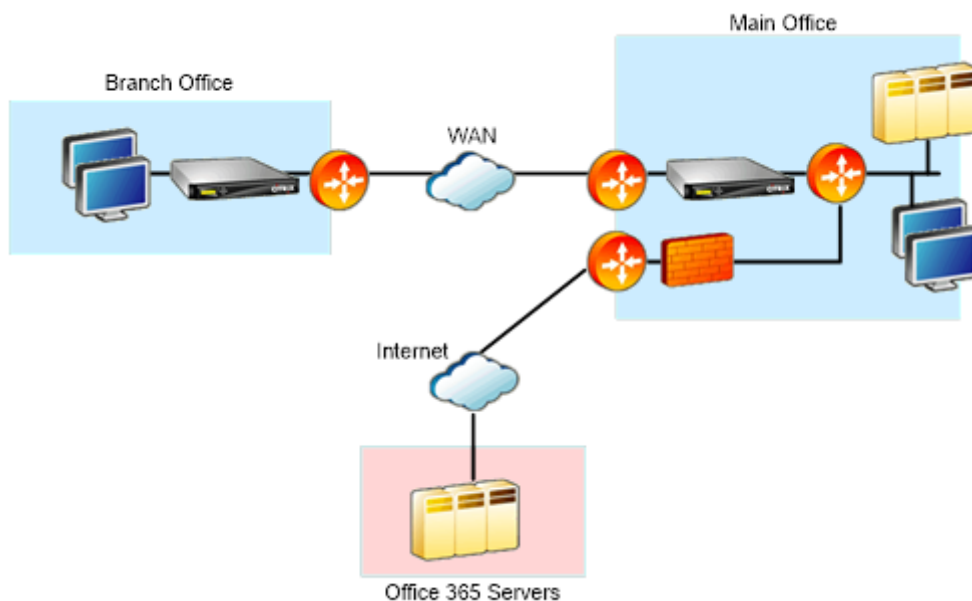
Wenn das WAN-Segment deutlich langsamer ist als das Internet-Segment, und Microsoft Office 365-Server sind näher an der größeren Niederlassung als die Zweigstelle.

## Topologie

Der Zweigstelle Office 365-Datenverkehr wird über das WAN an die Hauptniederlassung gesendet und dann über das Internet an Office 365-Server weitergeleitet. Das Segment zwischen Zweigstelle und Zentrale wird beschleunigt.

### Hinweis

Das Segment zwischen dem Hauptbüro und den Microsoft Office 365-Servern wird nicht beschleunigt. Es wird empfohlen, dass das Hauptbüro eine Verbindung zum nächstgelegenen Office 365-Server herstellt.



## Wie funktioniert das?

Die Citrix SD-WAN WANOP SSL-Beschleunigung kann den Office 365-Datenverkehr entschlüsseln und beschleunigen und ermöglicht so eine Komprimierung. Kurz gesagt, Office 365-Zweigstellenbeschleunigung kann als Sonderfall der RPC-über-HTTPS-Beschleunigung betrachtet werden.



## Prozedur

1. Erstellen Sie ein sicheres Peering zwischen den Citrix SD-WAN WANOP-Appliances der Zweigstelle und der Hauptverwaltung.
2. Generieren Sie Proxyzertifikaten/privaten Schlüssel in der Zertifizierungsstelle (Domain Certification Authority, CA).
3. Fügen Sie alle erforderlichen Zertifizierungsstellen in Citrix SD-WAN WANOP hinzu.
  - a) Zertifizierungsstelle, Zwischenzertifizierungsstellen, Stammzertifizierungsstelle der Microsoft-Zertifikate.
  - b) Proxy-Zertifikate/Private Schlüssel, die für Office 365-URLs generiert werden.

### Hinweis

Um Sicherheitswarnungen in Ihren Browsern zu vermeiden, müssen die Proxyzertifikate vom Zertifizierungsstellenserver Ihrer Windows-Domäne signiert werden. Dies macht es für jeden Domänenbenutzer akzeptabel.

4. Erstellen Sie ein SSL-geteiltes Proxy-Profil und binden Sie den geteilten Proxy an die Service-Klasse (Web (internetsicher)).
5. Starten Sie die Office 365-Verbindung und überprüfen Sie die beschleunigten Verbindungen.

### Warnung

Zweigstellengeräte, die nicht Teil der Domäne sind, zeigen Sicherheitswarnungen an, es sei denn, Sie installieren die Zertifikate manuell. Firefox-Benutzer müssen die Zertifikate auch manuell installieren, da Firefox den Zertifikatspeicher des Geräts nicht berücksichtigt.

## Konfigurieren der Office 365-Beschleunigung

So konfigurieren Sie die Office 365-Beschleunigung:

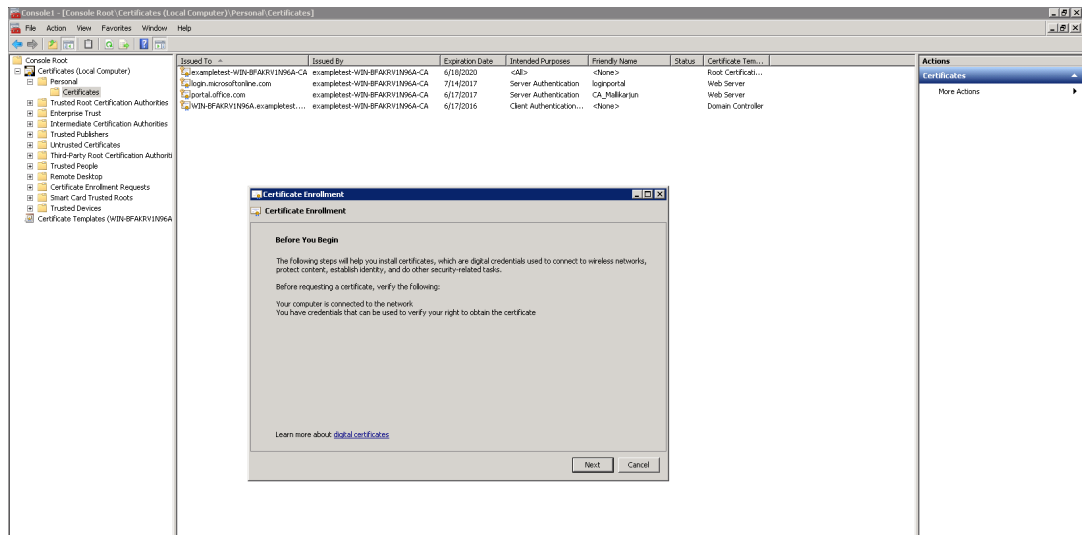
1. Richten Sie eine sichere Peering-Beziehung zwischen den beiden Citrix SD-WAN WANOP-Appliances ein, wie in [Secure Peering](#) beschrieben
2. Erstellen Sie ein neues Zertifikat.

### Hinweis

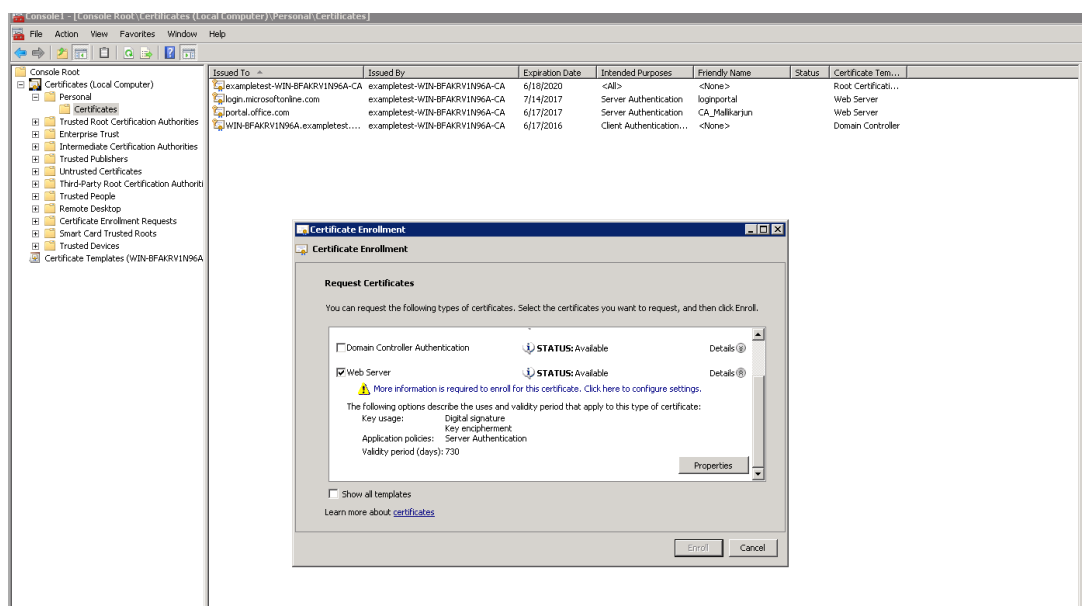
Die serverseitige Citrix SD-WAN WANOP-Appliance dient als Vermittler zwischen Office 365 und den Clients, sodass diese Zertifikate vom serverseitigen Domänencontroller signiert werden, sich jedoch auf die Office 365-Domänen beziehen.

- a) Melden Sie sich beim **Zertifizierungsstellenserver** für Ihre Windows-Domäne an.

- b) Fügen Sie bei Bedarf die Snap-Ins für **Zertifizierungsstelle**, **Zertifikatvorlage** und **Zertifikate** hinzu.
- c) Navigieren Sie zu **Zertifikatvorlagen** > **Webserver-Eigenschaften** > **Sicherheit**, und wählen Sie alle Optionen aus.
- d) Navigieren Sie zu **Zertifikate** > **Persönlich** > **Zertifikate (Computer)** > **Alle Aufgaben** > **Neues Zertifikat anfordern**.



- e) Klicken Sie im Fenster „Zertifikatsregistrierung“ auf **Weiter**.
- f) Wählen Sie im Fenster „Registrierungsrichtlinie für Zertifikatsregistrierung auswählen“ die Option **Active Directory-Registrierungsrichtlinie** aus.
- g) Wählen Sie im Fenster **Active Directory Registrierungsrichtlinie** die Option **Webserver** > **Details** > **Eigenschaften**.



3. Kopieren Sie Informationen aus Office365-Zertifikaten in Ihre neuen Zertifikate. Sie erhalten ein einzelnes Zertifikat aus drei Office365-Zertifikaten. Gehen Sie wie folgt vor:

- a) Geben Sie in einem Browser wie Chrome die URL ein -<https://login.microsoftonline.com>.

**Hinweis**

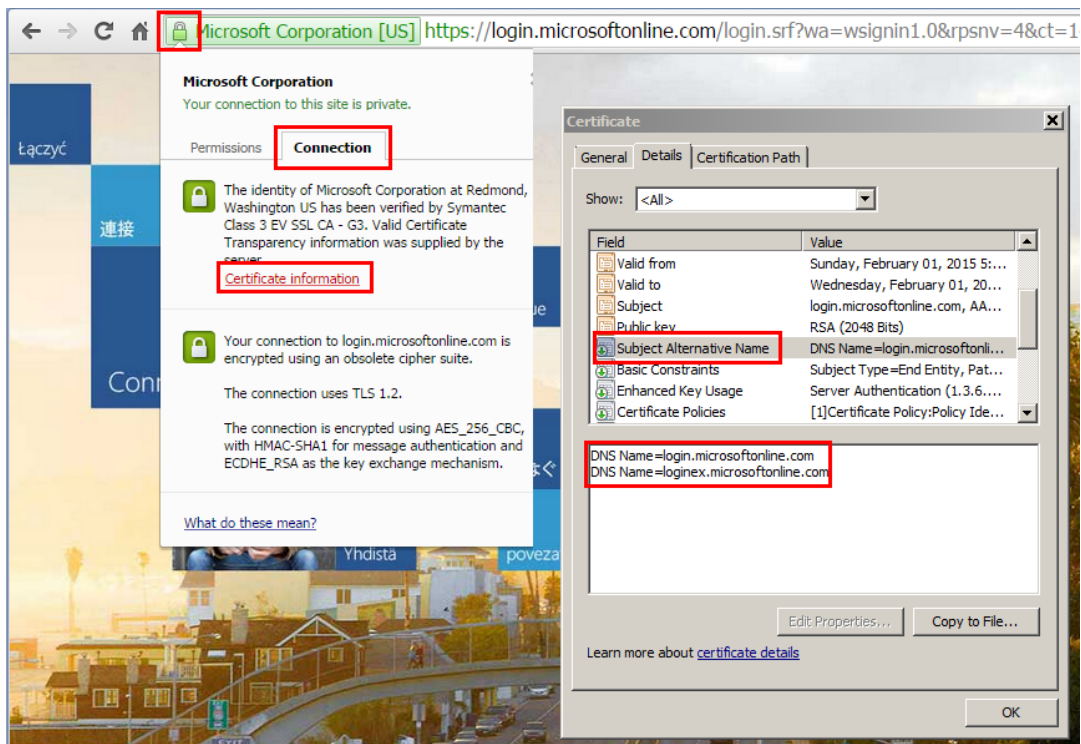
Melden Sie sich nicht an.

- b) Klicken Sie auf das Vorhängeschloss-Symbol in der URL-Leiste und wählen Sie **Verbindung** > **Zertifikatinformationen** > **Details**.

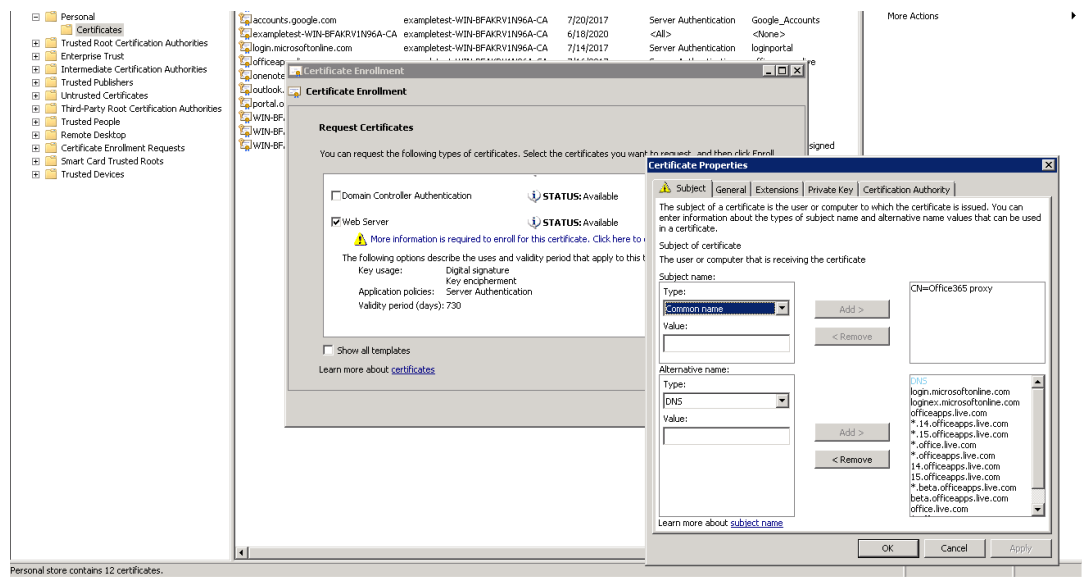
**Hinweis**

Diese Anweisungen gelten für den Chrome-Browser; das Verfahren ist auch für andere Browser identisch.

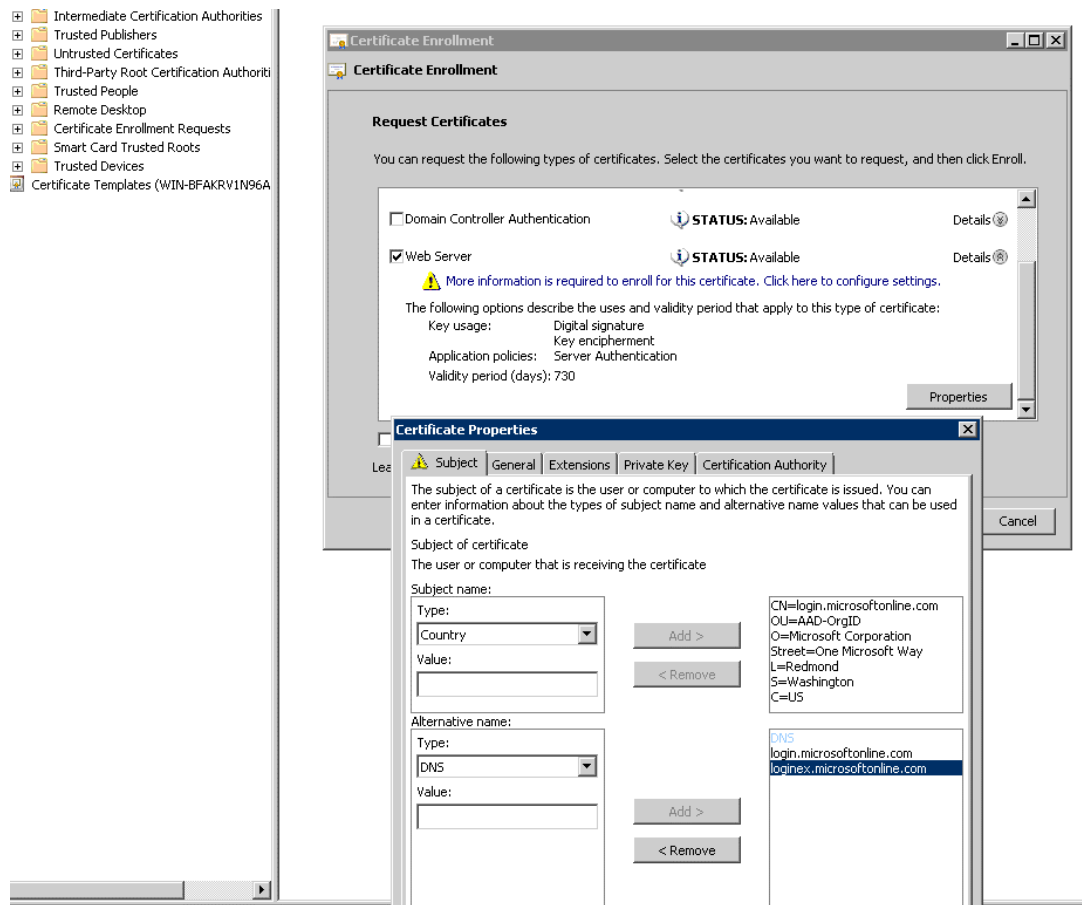
- c) Klicken Sie auf **Subject Alternative Name**. Dadurch wird eine Liste von DNS-Namen wie login.microsoftonline.com angezeigt. Kopieren Sie die Informationen in das Textfeld darunter.



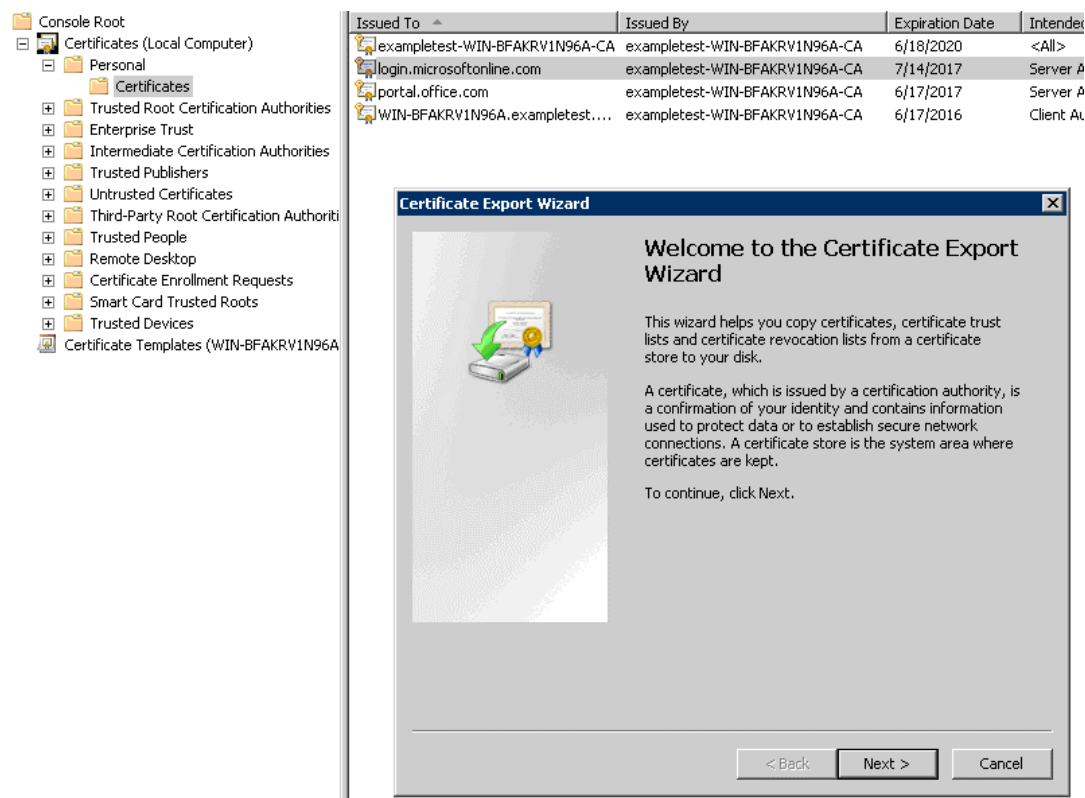
- d) Kehren Sie zum Fenster **Zertifikateigenschaften Ihres neuen Zertifikats** zurück. Fügen Sie die alternativen Namen im Feld **Wert** mit **Typ** als **DNS** hinzu, damit sie mit jedem alternativen Namen im Microsoft-Zertifikat übereinstimmen.



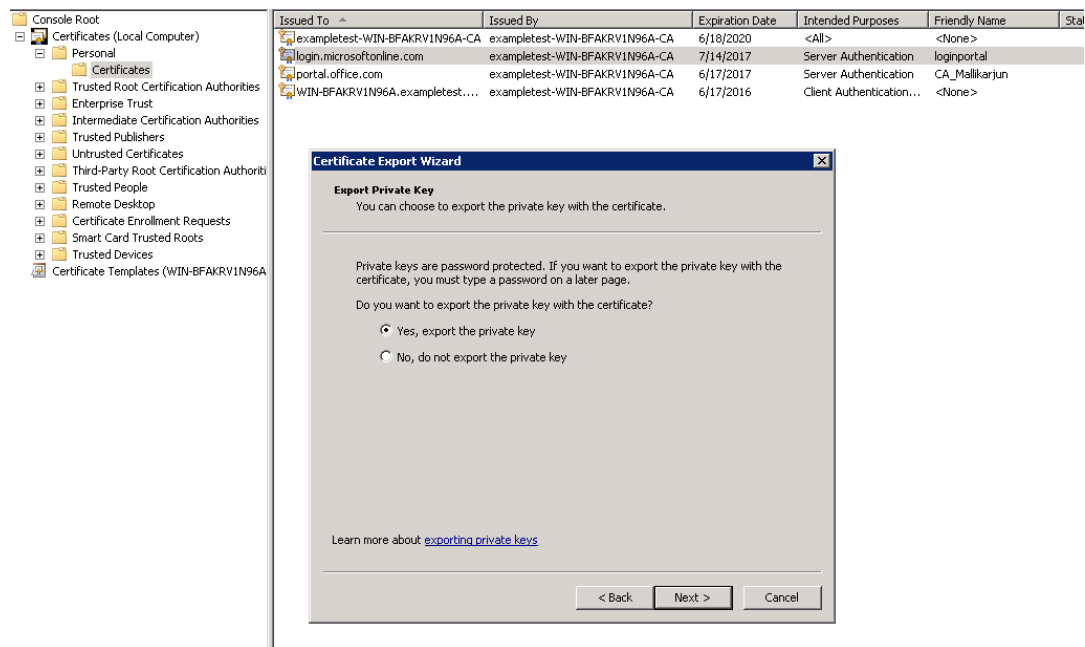
- e) Wiederholen Sie den Vorgang zum Erkennen alternativer Antragstellernamen und fügen Sie sie Ihrem Zertifikat für, <https://outlook.office365.com>, <https://portal.office.com>, <https://office.live.com> und <https://sharepoint.com> hinzu (die SharePoint-URL ist kundenspezifisch).
- f) Erstellen Sie einen allgemeinen Namen für Ihr neues Zertifikat. Das obige Beispiel zeigt einen allgemeinen Namen als Office365-Proxy.



- g) Wählen Sie auf der Registerkarte **Privater Schlüssel** die Option **Privaten Schlüssel exportieren**.
  - h) Klicken Sie auf **OK, Registrieren** und **Fertig stellen**.
4. Exportieren Sie das Zertifikat.
- a) Wählen Sie unter **Zertifikate > Persönlich > Zertifikate** das oben erstellte Proxy-Zertifikat aus, und wählen Sie dann **Alle Aufgaben > Exportieren** aus.

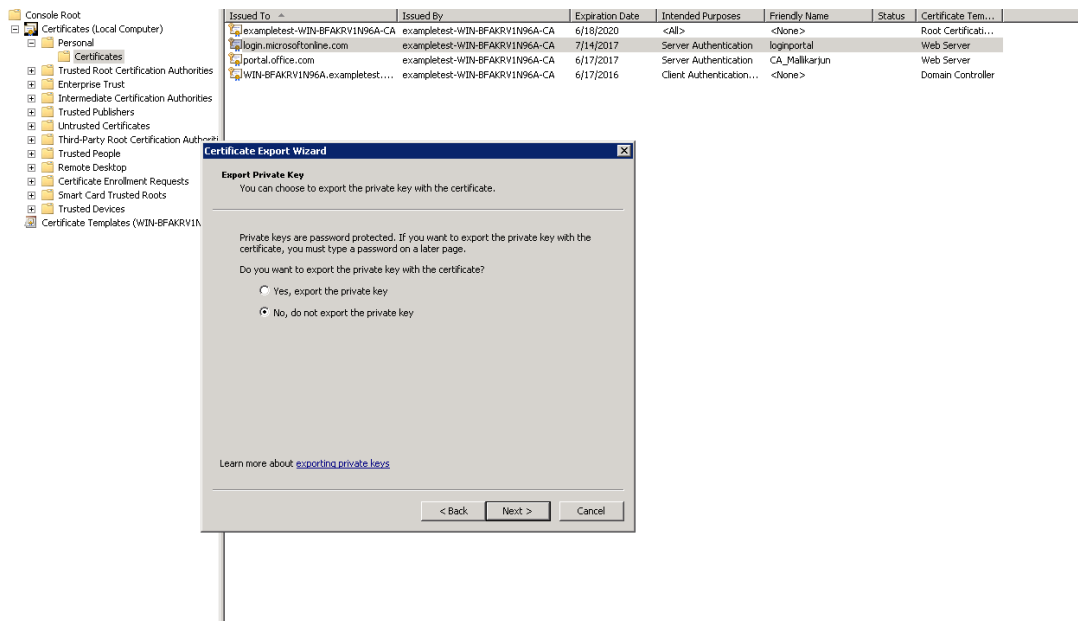


- b) Der **Zertifikatexport-Assistent** wird angezeigt. Klicken Sie auf **Weiter**.
- c) Wählen Sie unter **Private Key exportieren** die Option **Ja, den privaten Schlüssel exportieren** und klicken Sie auf **Weiter**.

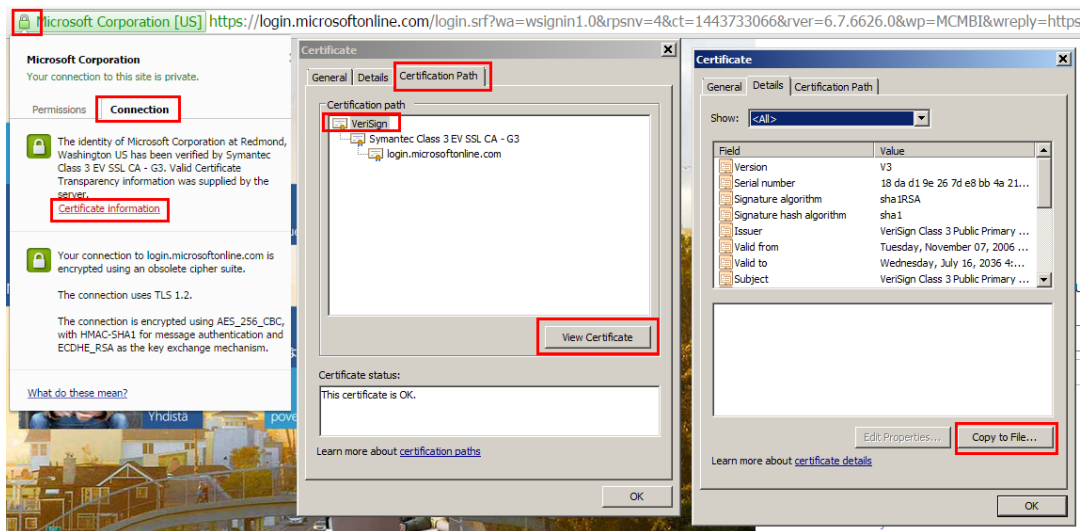


- d) Behalten Sie die Standardwerte für das Exportdateiformat bei.

- e) Geben Sie das Kennwort ein und bestätigen Sie es, exportieren Sie den privaten Schlüssel, und speichern Sie das Zertifikat als *loginportal.pfx*.
5. Exportieren Sie Ihre Zertifikate.
- a) Klicken Sie im **Zertifikatexport-Assistenten** auf **Weiter**. Wählen Sie unter **Private Key exportieren** die Option **Nein, den privaten Schlüssel nicht exportieren**. Klicken Sie auf **Weiter**.



- b) Behalten Sie die Standardwerte für das Exportdateiformat bei.
- c) Geben Sie das Kennwort ein und bestätigen Sie es, und exportieren Sie den privaten Schlüssel und das Zertifikat. Speichern Sie die Datei in eine Datei unter einem Dateinamen wie *office365\_keys.pfx*.
6. Laden Sie die öffentlichen Schlüssel der Stammzertifizierungsstelle und Zwischenzertifizierungsstellen der Microsoft-Zertifikate herunter.
- a) Navigieren Sie im Browser zu <https://login.microsoftonline.com>. Klicken Sie im Browser auf das Vorhängeschloss-Symbol. Navigieren Sie zu **Verbindung > Zertifikatinformationen > Zertifizierungspfad**.
- b) Wählen Sie das Stammzertifikat (das oben in der Liste) aus, und klicken Sie dann auf **Zertifikat anzeigen > Details > In Datei kopieren**. Der **Zertifikatexport-Assistent** wird angezeigt. Klicken Sie auf **Weiter**.



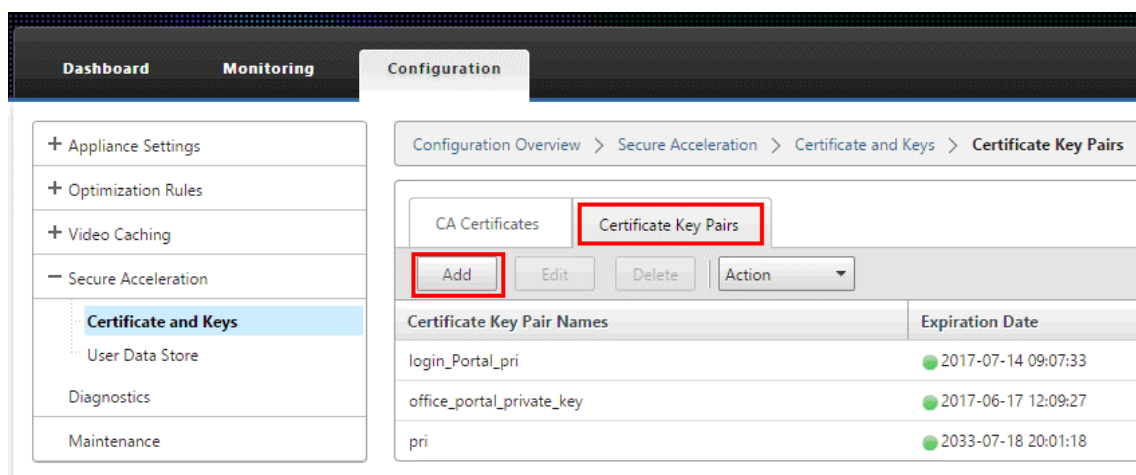
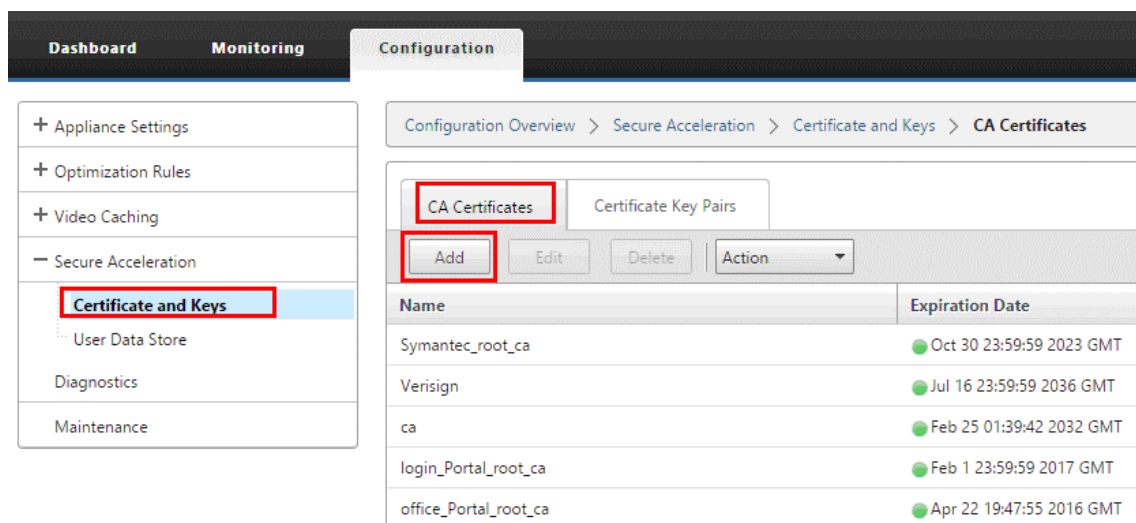
- c) Geben Sie den Dateinamen ein und speichern Sie die Datei.

#### Hinweis

Alternativ können Sie Wireshark oder OpenSSL verwenden, um die Stamm- und Zwischenzertifizierungsstellennamen abrufen und die Zertifikate von der 'AUTHENTIC' Quelle abrufen (z. B. Windows SSL Store).

- d) Wiederholen Sie Schritt 6, um die Stamm- und Zwischenzertifizierungsstellen der folgenden Domänen zu speichern:
- login.microsoftonline.com
  - portal.office.com
  - outlook.office365.com
  - \*.sharepoint.com
  - office.live.com
7. Fügen Sie der serverseitigen Citrix SD-WAN WANOP-Appliance alle Office 365-Server-Zertifizierungsstellen, Proxy-Zertifikat/Schlüsselpaare und private Schlüssel hinzu. Die Zertifizierungsstellen werden über die Registerkarte **Zertifizierungsstellenzertifikate** auf der Seite **Zertifikate und Schlüssel** hinzugefügt. Zertifikate und Zertifikat/Schlüsselpaare werden auf der Registerkarte **Zertifikat/Schlüsselpaare** hinzugefügt.





8. Erstellen Sie ein SSL-Teilproxy-Profil und binden Sie den geteilten Proxy an die Web-Service-Klasse (Internet-Secure).
  - a) Navigieren Sie zu **Konfiguration > Sichere Beschleunigung > SSL-Profil > Profil hinzufügen**.
  - b) Geben Sie den Profilnamen Ihrer Wahl ein. Wählen Sie **Profil aktiviert, Alternative Namen des Antragstellers analysieren** und **Proxy teilen** aus.
  - c) Wählen Sie unter **Serverseitige Proxykonfiguration > Verifizierungsspeicher** die Option **Alle konfigurierten Zertifizierungsstellenspeicher verwenden** aus.
  - d) Wählen Sie unter **Clientseitige Proxy-Konfiguration > Zertifikat/Privatschlüssel** das zuvor erstellte und exportierte Cert/Private Schlüsselpaar aus (das im Beispiel als loginportal.pfx gezeigt). Wählen Sie **Zertifikatskette erstellen aus**. Wählen Sie unter **Zertifikatskettenspeicher** die Zertifizierungsstelle aus, die dem Zertifikat/Schlüsselpaar zugeordnet ist.

SSL Profile

Profile Name\*  
Office365\_Profile

☒ Profile Enabled

☒ Parse Subject Alternative Names

Proxy type  
☒ Split ☐ Transparent

☒ Enable Exclude List

Certificate Verification\*  
None - allow all requests

Server-Side Proxy Configuration

Verification Store  
Use all configured CA stores

☐ Authentication Required

Protocol Version\*  
SSL Version 2.3 or TLS 1.0

Cipher Specification\*  
TADH:HIGH:MEDIUM:85LENGTH

Renegotiation Type\*  
Old Style Renegotiation Disabled

Client-Side Proxy Configuration

Certificate/Private Key\*  
single\_cert\_private

☒ Disable Session Re-use

☒ Build Certificate Chain

Certificate Chain Store  
Use all configured CA stores

Protocol Version\*  
SSL Version 2.3 or TLS 1.0

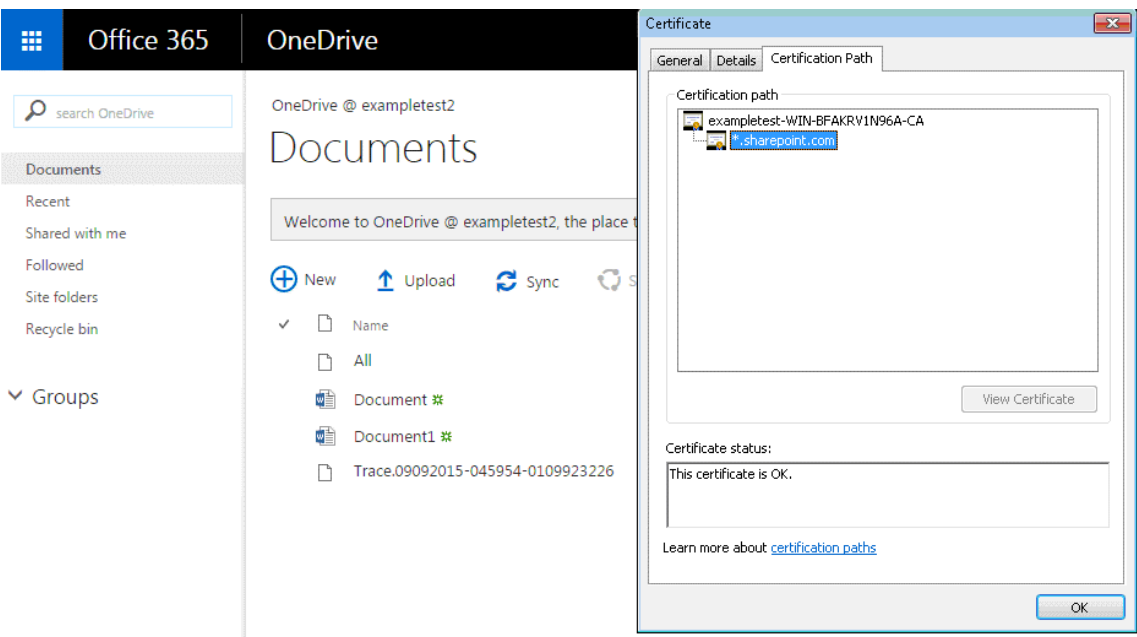
Cipher Specification\*  
TADH:HIGH:MEDIUM:85LENGTH

Renegotiation Type\*  
Old Style Renegotiation Disabled

Create Close

9. Binden Sie das erstellte SSL-Profil an die Dienstklasse Internet (Web-Secure). Navigieren **Sie zu Konfigurieren > Optimierungsregeln > Service-Klassen**, und fügen Sie das SSL-Profil zur SSL-Profilliste hinzu.
10. Aktivieren Sie die Beschleunigung und die festplattenbasierte Komprimierung für die **Internet-Serviceklasse (Web-Secure)**.
11. Starten Sie eine Office 365-Sitzung über Ihren Browser.

Die Verbindung wird beschleunigt. Im Browser sollte das Zertifikat Ihre Stammzertifizierungsstelle, nicht das eigentliche Office 365-Zertifikat, als Zertifizierungsstellenzertifikat der serverseitigen Appliance anzeigen.



12. Überprüfen Sie auf der Seite **Appliance-Überwachung > Verbindungen**, ob die Office 365-Verbindungen komprimiert sind und SSL-Beschleunigung erhalten.

The screenshot shows the 'Monitoring > Accelerated Connections' page in the Citrix SD-WAN WANOP interface. It features a table with columns: Details, Initiator, Responder, Duration, Idle, Bytes Transferred, Compression Ratio/Type, Bandwidth Savings (%), and SSL Proxy. The 'Compression Ratio/Type' and 'SSL Proxy' columns are highlighted with red boxes. The table lists several connections, all showing a compression ratio of 1.0 to 1 (Disk) and SSL Proxy set to True.

Details	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)	SSL Proxy
	172.16.139.221 : 50454	132.245.163.178 : 443	3m 31s	0m 11s	6.67 KB	1.1 to 1 (Disk)	29.6	True
	172.16.139.221 : 50453	132.245.163.178 : 443	3m 32s	0m 31s	6.19 KB	1.2 to 1 (Disk)	35.9	True
	172.16.139.221 : 50456	191.236.88.160 : 443	2m 2s	0m 53s	6.08 KB	1.6 to 1 (Disk)	46.8	True
	172.16.139.221 : 50459	132.245.165.130 : 443	1m 33s	1m 32s	3.15 KB	1.9 to 1 (Disk)	27.1	True
	172.16.139.216 : 11745	172.229.161.125 : 443	3m 25s	3m 4s	54 bytes	1.0 to 1 (Disk)	0	True
	172.16.139.216 : 11744	132.245.164.34 : 443	3m 25s	3m 21s	0 bytes	1.0 to 1 (Disk)	0	True
	172.16.139.216 : 11747	132.245.164.226 : 443	3m 24s	3m 21s	0 bytes	1.0 to 1 (Disk)	0	True

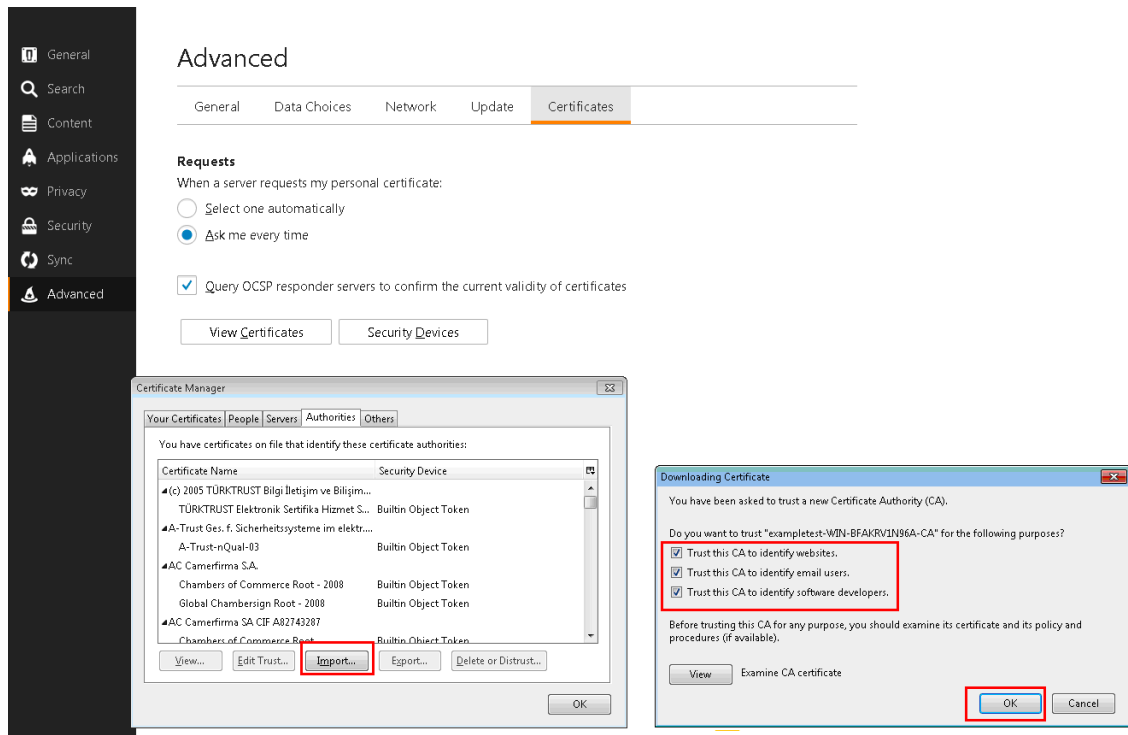
### Hinweis

Firefox akzeptiert die Zertifikate des Geräts standardmäßig nicht, verfügt aber über einen eigenen Zertifikatspeicher. Daher müssen Anmeldeinformationen, die im normalen Windows-Domänenverhalten von anderen Browsern und vom Gerät als Ganzes akzeptiert werden, manuell in Firefox installiert werden. Um Zertifikate in Firefox zu installieren, befolgen Sie die Anweisungen im Abschnitt Installieren von Zertifikaten für Firefox.

### Installieren Sie die Zertifikate in Firefox

So installieren Sie das Proxyzertifikat der serverseitigen Appliance im Firefox-Zertifikatspeicher:

1. Navigieren Sie im Firefox-Browser zu **Optionen > Erweitert > Zertifikat > Zertifikate anzeigen > Behörden > Importieren**.
2. Laden Sie das lokale Zertifizierungsstellen-Proxyzertifikat hoch, wählen Sie alle Optionen im Assistenten zum **Herunterladen von Zertifikaten** aus, und klicken Sie auf **OK**.



## SCPS Unterstützung

April 19, 2021

Citrix SD-WAN WANOP unterstützt die TCP-Variante SCPS (Space Communications Protocol Standard). SCPS ist weit verbreitet für die Satellitenkommunikation verwendet.

Allgemeine Informationen <http://www.scps.org> zu SCPS finden Sie unter.

SCPS ist eine TCP-Variante, die in der Satellitenkommunikation und ähnlichen Anwendungen verwendet wird. Die Appliance kann SCPS-Verbindungen beschleunigen, wenn die Option **SCPS** auf der Seite Konfiguration: Tuning ausgewählt ist.

Der praktische Hauptunterschied zwischen SCPS und dem Standardverhalten der Appliance besteht darin, dass SCPS-Stil selektive negative Bestätigungen (SNACKs) anstelle von standardmäßigen selektiven Bestätigungen (SACKs) verwendet wird. Diese beiden Methoden zur Verbesserung der Neuübertragungen von Daten schließen sich gegenseitig aus. Wenn also die Appliance an einem Ende der

Verbindung SCPS aktiviert hat und eine nicht, leidet die Weiterübertragungsleistung. Diese Bedingung verursacht auch eine Warnung SCPS-Modus Mismatch.

Wenn Sie SCPS-fähige Appliances mit nicht SCPS-fähigen Appliances mischen müssen, stellen Sie sie so bereit, dass keine Abweichungen auftreten. Sie können entweder IP-basierte Dienstklassenregeln verwenden oder die Bereitstellung so anordnen, dass jeder Pfad über passende Appliances verfügt.

## Sichere Verkehrsbeschleunigung

April 19, 2021

Sichere Traffic-Accelration wird durch sicheres Peering erreicht. Mehrere erweiterte Funktionen erfordern, dass die Citrix SD-WAN WANOP-Appliances an den beiden Enden der Verbindung eine *sichere Peer-Beziehung* zueinander aufbauen und einen SSL-Signaltunnel (auch als *Signalverbindung* bezeichnet) einrichten. Diese Funktionen sind SSL-Komprimierung, signierte CIFS-Unterstützung und verschlüsselte MAPI-Unterstützung.

Wenn Secure Peering aktiviert ist, wird die Komprimierung automatisch für alle Partner-Appliances (und Computer, auf denen das Citrix SD-WAN WANOP Plug-in ausgeführt wird) deaktiviert, die keine sichere Peer-Beziehung mit der lokalen Appliance hergestellt haben.

Um eine sichere Peer-Beziehung herzustellen, müssen Sie Sicherheitsschlüssel und Zertifikate generieren und einen sicherenden Signaltunnel zwischen den Appliances konfigurieren. Bestellen Sie vor der Konfiguration des Tunnels eine Kryptolizenz bei Citrix.

## Sicheres Peering

April 19, 2021

Wenn eine Appliance sicheres Peering aktiviert hat, werden Verbindungen mit einem Partner, für den es keine sichere Peer-Beziehung aufweist, nicht verschlüsselt oder komprimiert, obwohl die TCP-Durchflusssteuerungsbeschleunigung weiterhin verfügbar ist. Die Komprimierung ist deaktiviert, um sicherzustellen, dass Daten, die im Komprimierungsverlauf von gesicherten Partnern gespeichert sind, nicht mit ungesicherten Partnern geteilt werden können.

Wenn die Appliance an einem Ende einer Verbindung erkennt, dass die andere Appliance sicheres Peering aktiviert hat, versucht sie, einen SSL-Signaltunnel zu öffnen. Wenn sich die beiden Appliances über diesen Tunnel erfolgreich authentifizieren, haben sie eine sichere Peering-Beziehung. Alle beschleunigten Verbindungen zwischen den beiden Appliances werden verschlüsselt, und die Komprimierung ist aktiviert.

**Hinweis**

Eine Appliance mit aktiviertem sicherem Peering komprimiert keine Verbindungen zu ungesicherten Partnern. Die Verwendung derselben Appliance mit einer Mischung aus gesicherten und ungesicherten Partnern ist schwierig. Beachten Sie diesen Punkt, wenn Sie Ihr beschleunigtes Netzwerk entwerfen.

Für den Zugriff auf die Sicherheitsparameter ist ein Keystore-Kennwort erforderlich. Dieses Schlüsselspeicherkenwort unterscheidet sich vom Administratorkennwort, damit die Sicherheitsverwaltung von anderen Aufgaben getrennt werden kann. Wenn das Keystore-Kennwort zurückgesetzt wird, gehen alle vorhandenen verschlüsselten Daten und privaten Schlüssel verloren.

Um Daten zu schützen, selbst wenn die Appliance gestohlen wurde, muss das Schlüsselspeicherkenwort bei jedem Neustart der Appliance erneut eingegeben werden. Bis dies geschehen ist, sind sicheres Peering und Komprimierung deaktiviert.

**Erstellen von Sicherheitsschlüsseln und Zertifikaten**

Citrix SD-WAN WANOP-Produkte werden ohne die erforderlichen Schlüssel und Zertifikate für den SSL-Signaltunnel ausgeliefert. Sie müssen sie selbst generieren. Sie können Schlüssel und Zertifikate über Ihren normalen Prozess zum Generieren von Anmeldeinformationen oder mit dem openssl -Paket von generieren<http://www.openssl.org>.

Zu Testzwecken können Sie ein selbstsigniertes X509-Zertifikat basierend auf einem privaten Schlüssel generieren und verwenden (den Sie ebenfalls generieren). Verwenden Sie in der Produktion Zertifikate, die sich auf eine vertrauenswürdige Zertifizierungsstelle beziehen. Im folgenden Beispiel wird openssl von der Befehlszeile auf einem PC aufgerufen, um einen privaten Schlüssel (my.key) und ein selbstsigniertes Zertifikat (my.crt) zu generieren:

```
1 pre codeblock
2 # Generate a 2048-bit private key
3 openssl genrsa -out my.key 2048
4 # Now create a Certificate Signing Request
5 openssl req -new -key my.key -out my.csr
6 # Finally, create a self-signed certificate with a 365-day expiration
7 openssl x509 -req -days 365 -in my.csr -signkey my.key -out my.crt
8 <!--NeedCopy-->
```

Informationen zur Verwendung in der Produktion finden Sie in den Sicherheitsrichtlinien Ihrer Organisation.

## Konfigurieren von sicherem Peering

Es gibt zwei Möglichkeiten, ein sicheres Peering einzurichten:

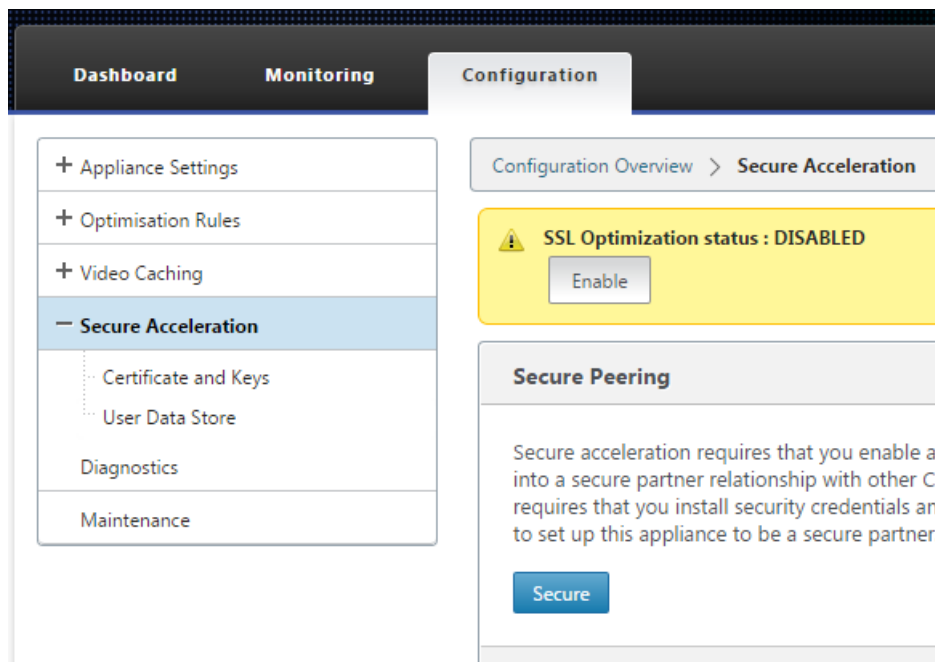
1. Verwenden von Anmeldeinformationen, die von den Appliances generiert werden.
2. Verwenden von Anmeldeinformationen, die Sie selbst angeben.

Da eine Appliance mit aktiviertem sicherem Peering nur Verbindungen mit Partner-Appliances komprimiert, mit denen sie über eine sichere Peering-Beziehung verfügt, sollte dieses Verfahren gleichzeitig auf alle Ihre Appliances angewendet werden.

### So bereiten Sie die Appliances für sicheres Peering vor:

Führen Sie das folgende Verfahren für jede Appliance im Netzwerk aus.

1. Installieren Sie eine Kryptolizenz auf der Appliance. Ohne eine Kryptolizenz ist keine sichere Beschleunigung verfügbar.
  - a) Wenn Sie dies noch nicht getan haben, erwerben Sie Kryptolizenzen von Citrix.
  - b) Wenn Sie einen Netzwerklizenzserver verwenden, gehen Sie zu **Konfiguration > Appliance-Einstellungen > Lizenzierung**. Klicken Sie im Abschnitt **Lizenz hinzufügen** auf **Bearbeiten**, wählen Sie den Remote-Lizenzserver aus und legen Sie Crypto License On fest.
  - c) Wenn Sie lokale Lizenzierung verwenden, gehen Sie zu **Konfiguration > Appliance-Einstellungen > Lizenzierung**. Klicken Sie auf der Seite **Lizenz hinzufügen** auf die Option Lokaler Lizenzserver, und klicken Sie auf **Hinzufügen**, um eine lokale Kryptolizenz hochzuladen.
  - d) Überprüfen Sie die erfolgreiche Lizenzinstallation auf der Seite **Konfiguration > Einheits-einstellungen > Lizenzierung**. Unter Lizenzinformationen sollte eine Kryptolizenz als aktiv und mit einem Ablaufdatum in der Zukunft angezeigt werden.
2. Rufen Sie die Seite **Konfiguration > Sichere Beschleunigung** auf. Wenn die Seite eine Schaltfläche mit der Bezeichnung **Sichern** aufweist, klicken Sie darauf.



3. Gehen Sie folgendermaßen vor, wenn Sie automatisch zu einem Keystore-Fenster wechseln:
  - a) Geben Sie zweimal ein Schlüsselspeicherkenwort ein und klicken Sie auf Speichern.
  - b) Wenn der Bildschirm aktualisiert wird, um den Abschnitt Secure Peering Zertifikate und Schlüssel anzuzeigen, klicken Sie auf Secure Peering und CA Certificate aktivieren, und klicken Sie dann auf Speichern.
  - c) Fahren Sie mit Schritt 6 fort.
4. Wenn Sie nicht automatisch zum Fenster Keystore-Einstellungen weitergeleitet wurden, klicken Sie unter **Secure Peering** auf das Bleistiftsymbol und dann unter **Keystore-Einstellungen** auf **das Bleistiftsymbol**. Öffnen Sie im Pulldownmenü Keystore-Status, und geben Sie zweimal ein Keystore-Kennwort ein. Klicken Sie auf **Save**.
5. Aktivieren Sie Secure Peering, indem Sie auf die Seite **Konfiguration > Sichere Beschleunigung** gehen und auf die Schaltfläche **Aktivieren** klicken. Ignorieren Sie in diesem Stadium alle Warnungen. Diese Einstellung ermöglicht sicheres Peering, wenn die erforderliche zusätzliche Konfiguration abgeschlossen ist.
6. Aktivieren Sie die Verschlüsselung des Komprimierungsverlaufs, indem Sie zu **Konfiguration > Benutzerdatenspeicher** für **sichere Beschleunigung** navigieren und auf das Bleistiftsymbol klicken. Klicken Sie auf **Festplattenverschlüsselung aktivieren**, und klicken Sie dann auf **Speichern**. Die Verschlüsselung des Benutzerdatenspeichers verhindert das unbefugte Lesen des datenträgerbasierten Komprimierungsverlaufs, falls die Appliance gestohlen oder an die Fabrik zurückgegeben wird. Die Sicherheit der Datenträgerdatenverschlüsselung beruht auf dem Schlüsselspeicherkenwort. Diese Funktion verwendet AES-256-Verschlüsselung. (Die Daten-



trägerdatenverschlüsselung verschlüsselt nicht den gesamten Datenträger, sondern nur den Komprimierungsverlauf.)

7. Wenn Sie Appliance-generierte Anmeldeinformationen verwenden, fahren Sie mit dem nächsten Schritt fort. Wenn Sie Ihre eigenen Anmeldeinformationen verwenden, gehen Sie wie folgt vor:

- a) Gehen Sie zu **Konfiguration > Sichere Beschleunigung**, und klicken Sie unter Secure Peering auf das Stiftsymbol, und klicken Sie dann auf das Stiftsymbol unter **Secure Peering Zertifikate und Schlüssel**. Klicken Sie auf **Secure Peering and Certificate Configuration > CA Certificate** aktivieren. Die Felder für die Anmeldeinformationen werden angezeigt.
- b) Klicken Sie unter **Zertifikat/Schlüsselpaarname** auf das Symbol **+**, und laden Sie das Cert/Schlüsselpaar für diese Appliance hoch oder fügen Sie es ein. Geben Sie bei Bedarf auch das Schlüsselkennwort oder das Dateikennwort ein. Klicken Sie auf **Erstellen**.
- c) Klicken Sie unter **CA-Zertifikatspeichernamen** auf das Symbol **+**, und laden Sie das CA-Zertifikat für diese Appliance hoch oder fügen Sie es ein.
- d) Behalten Sie die Standardwerte für die Felder Zertifikatüberprüfung und SSL-Verschlüsselungsspezifikation bei, sofern Ihre Organisation nichts anderes erfordert.
- e) Klicken Sie auf **Save**.

Secure Peering

**Keystore Settings**

Keystore Status  
Opened

**Secure Peering Certificate and Keys**

Secure communications with the CloudBridge partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☐ Private CA ☒ CA Certificate

Certificate/Key Pair Name  
private\_172\_16\_0\_243

CA Certificate Store Name  
PrivateRootCA

Certificate Verification  
Signature/Expiration

SSL Cipher Specification  
[ADH:AECDH:IMDS:HGH:STRENGTH]

☐ Edit Cipher Specification

Save Cancel

8. Wiederholen Sie dies für den Rest Ihrer Geräte.
9. Wenn Sie selbst bereitgestellte Anmeldeinformationen verwenden, ist die sichere Peering-Konfiguration abgeschlossen.
10. Wenn Sie Appliance-generierte Anmeldeinformationen verwenden, führen Sie das folgende Verfahren aus.

**So verwenden Sie Secure Peering mit Appliance-generierten Anmeldeinformationen:**

1. Verwenden Sie das obige Verfahren Vorbereiten der Geräte für die Sicherung des Peering, um Ihre Geräte für diesen Vorgang vorzubereiten.
2. Wechseln Sie auf einer Datacenter-Appliance zu **Konfiguration > Sichere Beschleunigung**, und klicken Sie auf die Schaltfläche **Aktivieren**, falls vorhanden, um sicheres Peering zu aktivieren.
3. Klicken Sie auf das Stiftsymbol unter Secure Peering. Der Keystore sollte offen sein. Wenn nicht, öffnen Sie es jetzt.
4. Klicken Sie auf das Stiftsymbol unter **Secure Peering Certificate and Keys**. Klicken Sie auf die Optionen **Secure Peering und Private CA aktivieren**, und klicken Sie dann auf **Speichern**. Dadurch werden ein lokales selbstsigniertes Zertifizierungsstellenzertifikat und ein lokales Zertifikatschlüsselpaar generiert.
5. Klicken Sie unter **Verbundene Peers** auf **+**. Geben Sie die IP-Adresse, den Benutzernamen des Administrators und das Administratorkennwort für eine Ihrer Remote-Appliances ein, und klicken Sie auf **Verbinden**. Dadurch wird ein Zertifizierungsstellenzertifikat-Schlüsselpaar für die Remote-Appliance ausgegeben und in die Remote-Appliance kopiert.

**Hinweis**

Bei SD-WANOP-Appliances kann die IP-Adresse einer beliebigen Schnittstelle sein, auf der der Webzugriff aktiviert ist. Bei SD-WAN PE-Appliances ist die IP-Adresse die Verwaltungs-IP-Adresse.

6. Wiederholen Sie diesen Vorgang für Ihre anderen Remote-Appliances.
7. Überprüfen Sie auf der Datacenter-Appliance die Konnektivität, indem Sie zu **Überwachung > Partner und Plug-ins > Sichere Partner** gehen. Für jede Remote-Appliance sollte der Inhalt des Felds Sicher True und der Verbindungsstatus Verbunden verfügbar sein.

## CIFS, SMB2 und MAPI

April 19, 2021

Windows ist eines der gängigen Betriebssysteme, die im Netzwerk bereitgestellt werden. Das Windows-Betriebssystem unterstützt verteilte Ressourcen, die über mehrere Standorte verteilt sind. Beispielsweise können Sie Ressourcen in Ihrem Rechenzentrum von verschiedenen Zweigstellen aus zugänglich machen. Für den Zugriff über das Netzwerk verwendet Windows das CIFS-Protokoll (Common Internet File System) für den Zugriff auf freigegebene Dateien und MAPI-Protokolle (Messaging Application Programming Interface) für den Zugriff auf E-Mails über Microsoft Outlook. Das

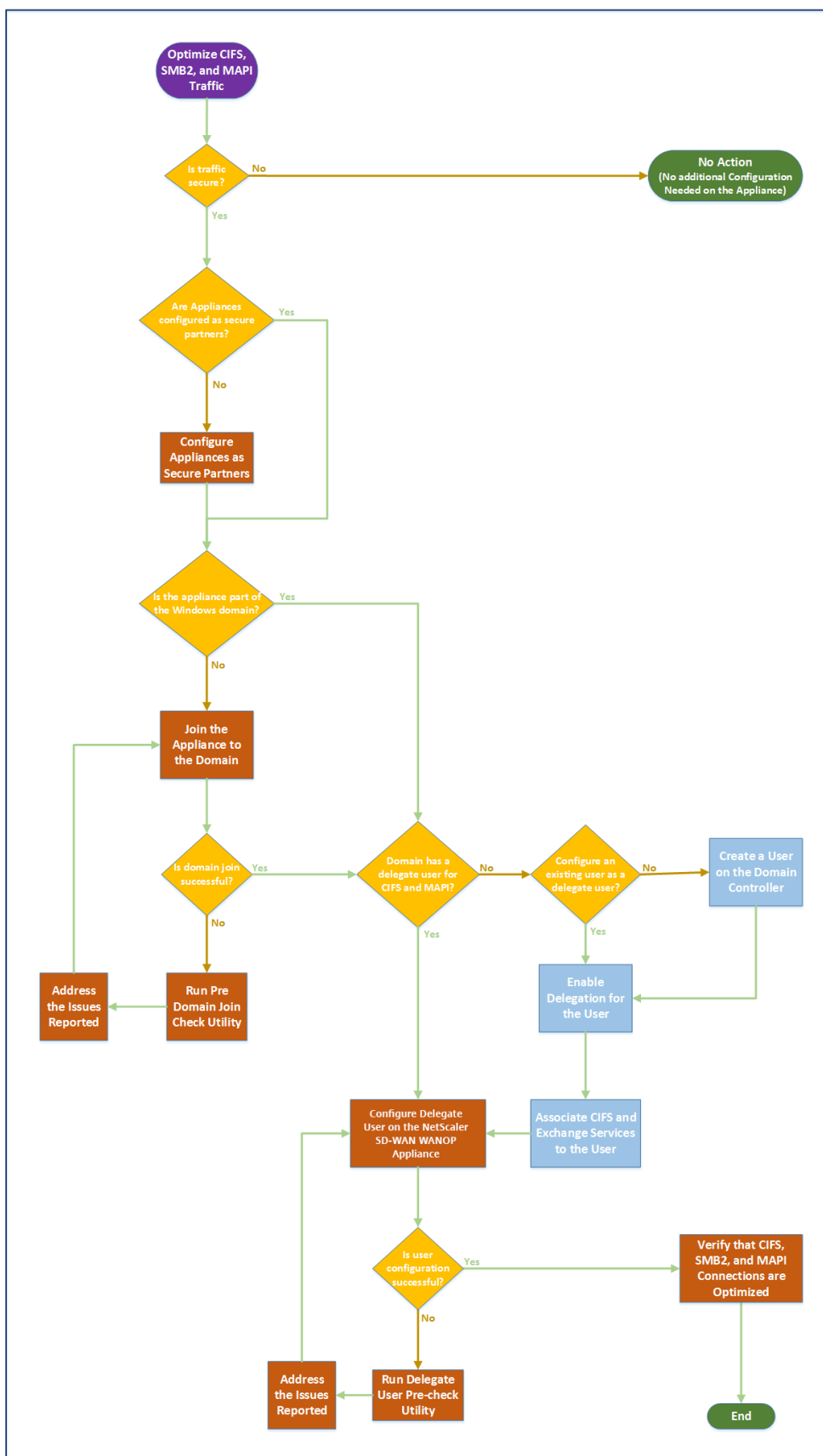
heißt, Windows verwendet CIFS-Protokoll für CIFS-basierte (Windows und Samba) Dateiübertragung und Verzeichnissuche, und Microsoft Outlook verwendet das MAPI-Protokoll für den Zugriff auf Outlook-Daten.

Sie können eine Citrix SD-WAN WANOP-Appliance verwenden, um die CIFS-, Server-Message-Block-Version 2 (SMB2) und MAPI-Verbindungen über das Netzwerk zu optimieren.

Neben der Unterstützung des Windows-Betriebssystems unterstützen Citrix SD-WAN WANOP-Appliances CIFS und SMB2 auf NetApp- und Hitachi-Speichersystemen.

Das folgende Flussdiagramm zeigt das vollständige Verfahren zur Konfiguration einer Citrix SD-WAN WANOP-Appliance zur Optimierung des CIFS-, SMB2- und MAPI-Datenverkehrs.

Konfigurieren einer Citrix SD-WAN WANOP-Appliance zur Optimierung des CIFS-, SMB2- und MAPI-Datenverkehrs



## **Konfigurieren der Citrix SD-WAN WANOP-Appliance zur Optimierung des sicheren Windows-Datenverkehrs**

April 19, 2021

Sie müssen die Citrix SD-WAN WANOP-Appliance zur Windows-Sicherheitsinfrastruktur hinzufügen, bevor Sie das signierte Windows-Dateisystem und den verschlüsselten MAPI-Outlook/Exchange-Datenverkehr optimieren können.

Als Ergebnis von Verbesserungen am Windows-Sicherheitssystem in den letzten Windows-Versionen sichern Clients und Server den Datenverkehr durch Authentifizierung und Verschlüsselung. Dies erfordert, dass die Citrix SD-WAN WANOP-Appliance ein vertrauenswürdiges Mitglied der Windows-Sicherheitsinfrastruktur ist, bevor sie das signierte Windows-Dateisystem und den verschlüsselten MAPI-Outlook/Exchange-Datenverkehr optimieren kann.

Nachdem Sie die Appliance zur Windows-Sicherheitsinfrastruktur hinzugefügt haben, verfügt die Appliance über folgende Funktionen:

- Beschleunigung des Dateiserververkehrs für Microsoft Windows-Server, NetApp-Server und Hitachi HNAS mithilfe von signiertem SMB- und signiertem SMB2-Protokoll.
- Beschleunigung des Microsoft Exchange-Serververkehrs, wenn Outlook-Clients mit verschlüsseltem MAPI oder RPC über HTTPS darauf zugreifen.

### **Funktionsweise der Citrix SD-WAN WANOP-Appliance in einem Windows-Sicherheitssystem**

Das Hinzufügen der Appliance zu einer Windows-Domäne erfordert Administratoranmeldeinformationen. Wenn sie der Windows-Domäne beitrifft, wird die Appliance zu einem vertrauenswürdigen Mitglied der Domäne. Dadurch kann die Appliance als Mitglied der Sicherheitsinfrastruktur der Domäne deklariert werden.

Nachdem die Appliance Teil der Windows-Sicherheitsinfrastruktur geworden ist, müssen Benutzer authentifiziert werden, bevor sie auf Ressourcen zugreifen können. Um die Schwierigkeiten beim Konfigurieren einer großen Anzahl von Benutzern in der Domäne zu vermeiden, können Sie die Authentifizierungszuständigkeit an einen Benutzer delegieren.

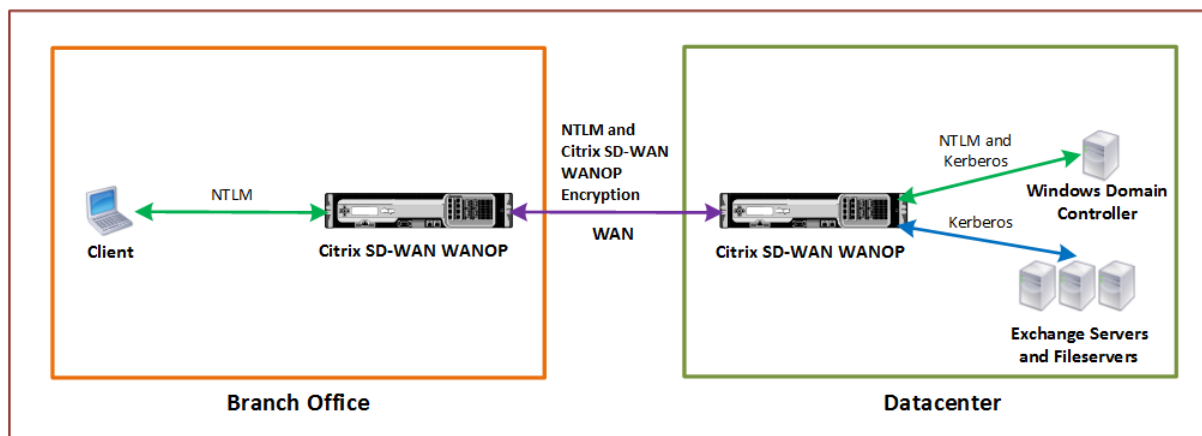
Sie erstellen einen Delegatbenutzer im Active Directory. Dieser Benutzer ähnelt einem normalen Benutzer, aber mit speziellen Berechtigungen. Nach dem Erstellen des Delegate-Benutzers müssen Sie diesen Benutzer auf der Citrix SD-WAN WANOP-Appliance konfigurieren. Die Appliance verwendet den Delegatbenutzer, um sich im Namen von Benutzern zu authentifizieren, wenn sie mithilfe

von Windows-Protokollen wie CIFS und MAPI auf authentifizierte und verschlüsselte Datenströme zugreifen.

Zur Beschleunigung des CIFS- und MAPI-Datenverkehrs ermöglicht der standardmäßige Windows-Delegierungsmechanismus die Einschränkung der Sicherheitsdelegierung auf die relevanten Dienste. Diese eingeschränkte Delegierung ist seit der Veröffentlichung von Windows Server 2003 verfügbar.

Nachdem die Appliance Teil der Domäne geworden ist, beschleunigt die Appliance den sicheren Windows-Datenverkehr. Eine Rechenzentrums-Appliance, die einer Windows-Domäne beitrifft, muss eine sichere Peer-Beziehung mit der Remote-Appliance oder dem Citrix SD-WAN WANOP Plug-in haben, aber nur die Rechenzentrums-Appliance tritt der Windows-Domäne bei. Für Zwecke der CIFS- oder MAPI-Beschleunigung fungiert die Remote-Appliance als Slave für die Datacenter-Appliance und wird über den sicheren SSL-Tunnel zwischen den beiden gesteuert. Daher verlassen die Anmeldeinformationen des Delegaten nicht das Datacenter.

Die folgende Abbildung zeigt ein Beispiel-Topologiediagramm für diese Einrichtung.



In der obigen Abbildung greift ein Zweigstellenclient auf Ressourcen des Rechenzentrums zu. Der Zweigstellenclient, der sich in einer anderen Domäne befindet, verwendet die NTLM-Authentifizierung als Teil des Windows-Sicherheitssystems. Wie bei allen beschleunigten Verbindungen zwischen zwei Citrix SD-WAN WANOP-Appliances in einer sicheren Peer-Beziehung werden die CIFS- oder MAPI-Verbindungen und NTLM-Authentifizierungen über das WAN verschlüsselt. Abhängig von der Version des Windows-Domänencontrollers wird die Benutzeranforderung des Rechenzentrums Citrix SD-WAN WANOP-Appliance mit dem NTLM- oder Kerberos-Authentifizierungsprotokoll authentifiziert. Nachdem die Domäne den Benutzer authentifiziert hat, verwenden nachfolgende Zugriffsanforderungen an den Exchange-Server und Dateiserver das Kerberos-Authentifizierungsprotokoll. Die Citrix SD-WAN WANOP Appliance optimiert dann die Verbindungen zwischen dem Client und dem Server.

Wenn die Appliances keine sichere Peer-Beziehung haben oder wenn die Datacenter-Appliance der Domäne nicht erfolgreich beigetreten ist, verwenden die Verbindungen die TCP-Durchflusssteuerungsbeschleunigung, die keine Sicherheitsoperationen, keine Komprimierung oder Datentransformationen durchführt.

Die Verbindungen zwischen dem Client und dem Server werden so hergestellt, als wären die Citrix SD-WAN WANOP Appliances nicht vorhanden.

Sie können verschiedene Clientauthentifizierungsmodi unter Windows-Betriebssystemen konfigurieren. Die Arten von Verbindungen, die die Citrix SD-WAN WANOP-Appliance optimiert, hängen vom konfigurierten Client-Authentifizierungsmodus ab.

In der folgenden Tabelle sind die Windows-Client-Authentifizierungsmodi unter Windows und die entsprechenden Citrix SD-WAN WANOP-Optimierungen aufgeführt.

Unterstützte Authentifizierung und Optimierung für Windows-Betriebssystem

Client-Betriebssystem	Client-Authentifizierungsmodus	Optimierung	Anmerkungen
Windows XP/Windows Vista/Windows 7/Windows 8	Authentifizierung aushandeln (SPNEGO)	TCP-Durchflussregelbeschleunigung, Kompression, CIFS-Protokollbeschleunigung	Standardeinstellung für alle Windows-Versionen.
Windows XP/Windows Vista/Windows 7/Windows 8	Nur NTLM oder nur Kerberos	TCP-Durchflussregelbeschleunigung nur	Nicht-Standard-Authentifizierungsmodi

Hinweis: Wenn Sie nur die Client-Authentifizierungsmodi NTLM oder nur Kerberos verwenden, wird der Datenverkehr nicht beschleunigt, wenn er verschlüsselt ist.

### Anforderungen zum Hinzufügen einer Citrix SD-WAN WANOP-Appliance zum Windows-Sicherheitssystem

Um den Datenverkehr für gesicherten Windows signierten SMB- und verschlüsselten MAPI-Datenverkehr zu optimieren, muss Ihre Citrix SD-WAN WANOP-Bereitstellung die folgenden Anforderungen erfüllen, bevor Sie die Appliance zur Windows-Sicherheitsinfrastruktur hinzufügen:

- Sowohl die clientseitige als auch die serverseitige Beschleunigungs-Appliances müssen eine sichere Peer-Beziehung aufgebaut haben.
- Die Appliances müssen einen NTP-Server verwenden, der eng mit der Zeit auf dem Windows-Domänenserver synchronisiert ist. Idealerweise sind die Appliances und der Windows-Domänenserver alle Clients desselben NTP-Servers.
- Outlook **darf nicht** für die (nicht standardmäßige) **Kerberos-** oder **NTLM-Option** konfiguriert werden. Die Standardoption (ausgehandelt) ist für die Beschleunigung erforderlich.

- Der Client und der Server können Mitglieder jeder Domäne sein, die eine bidirektionale Vertrauensstellung mit der Domäne der serverseitigen Appliance hat. Die unidirektionale Vertrauensstellung wird nicht unterstützt.
- Ein Kerberos-Delegatbenutzer muss auf dem Domänencontroller eingerichtet sein, um von der Appliance verwendet werden, die an der Sicherheitsinfrastruktur der Domäne beteiligt ist.
- Die DNS-Server-IP-Adressen für die Domäne müssen auf der serverseitigen Appliance konfiguriert und erreichbar sein.
- Die Domänenserver müssen vollständig erreichbar sein, wobei sowohl Forward- als auch Reverse-Lookups für alle IP-Adressen der Domänencontroller, die auf den DNS-Servern konfiguriert sind.
- Der Hostname der serverseitigen Citrix SD-WAN WANOP Appliance muss eindeutig sein. Die Verwendung des standardmäßigen Hostnamens hostname führt wahrscheinlich zu Problemen.

**Hinweis**

Der Macintosh-Outlook-Client verwendet nicht den MAPI-Standard (Outlook/Exchange) und wird durch dieses Feature nicht beschleunigt.

**Hinzufügen einer Citrix SD-WAN WANOP-Appliance zur Windows-Sicherheitsinfrastruktur**

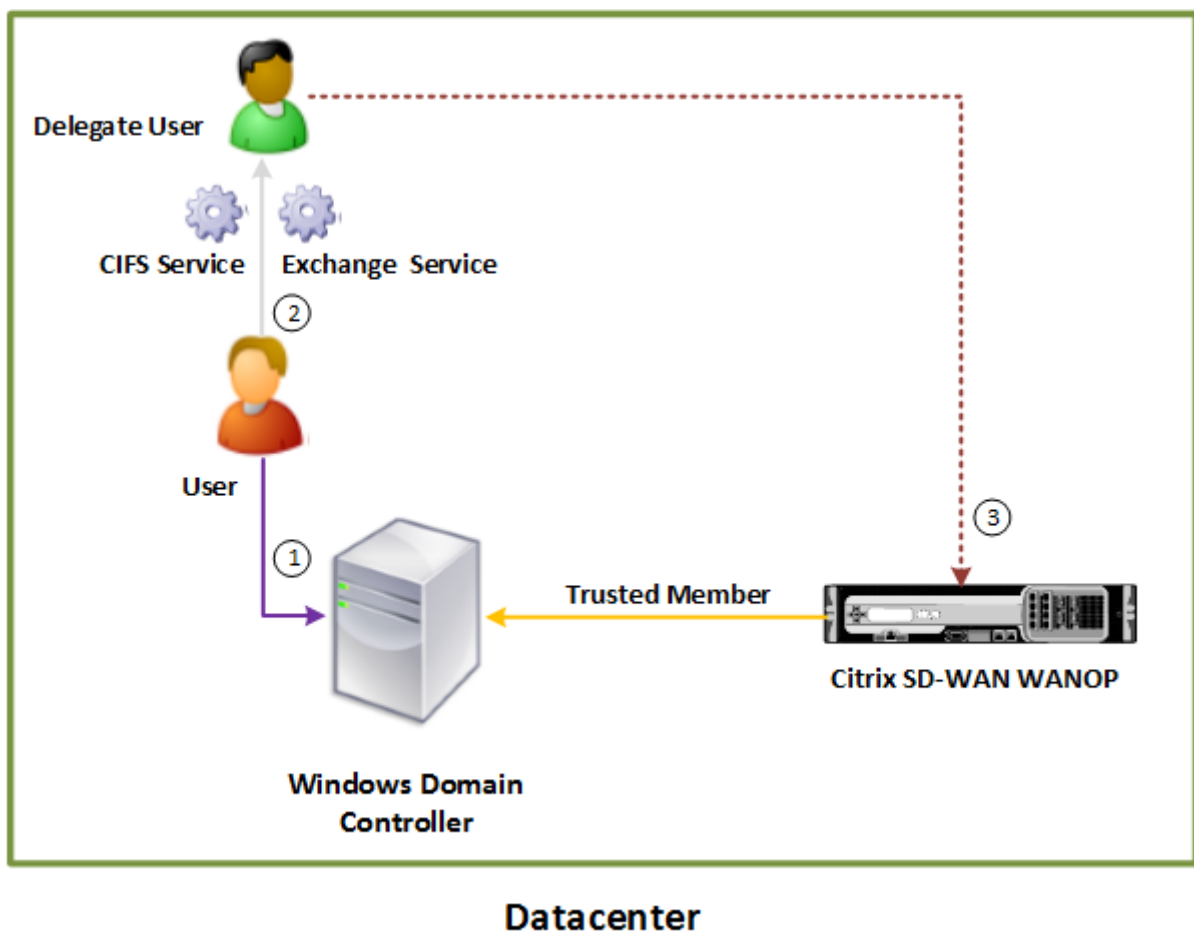
Um den sicheren Windows-Datenverkehr zu optimieren, muss die Citrix SD-WAN WANOP-Appliance Teil des Windows-Sicherheitssystems sein und sich mit dem Sicherheitssystem oder der Domäne authentifizieren. Wie in der folgenden Abbildung dargestellt, müssen Sie die Appliance als Teil des Windows-Sicherheitssystems machen, um die Appliance einer Domäne beitreten (unter Verwendung von Administratoranmeldeinformationen). Darüber hinaus müssen Sie einen neuen oder vorhandenen Benutzer als Delegatbenutzer konfigurieren, indem Sie CIFS- und Exchange-Dienste diesem Benutzer zuordnen. Sie müssen diesen Delegate-Benutzer dann auf der Citrix SD-WAN WANOP-Appliance konfigurieren.

Sie können das Dienstprogramm **vor der Domänenüberprüfung** verwenden, um herauszufinden, ob Probleme beim Beitritt der Appliance zu einer Domäne auftreten.

**Hinweis**

Das Windows-Sicherheitssystem verwendet den Exchange-Dienst, um MAPI-Verbindungen zu verwalten. Konfigurieren des Setups zur Optimierung des sicheren Windows-Datenverkehrs





### Verbinden Sie eine Citrix SD-WAN WANOP Appliance mit der Windows-Domäne:

Wenn die Appliance der Domäne beitrifft, tauscht sie einen gemeinsamen Schlüssel mit dem Domänencontroller aus, sodass die Appliance unbegrenzt Teil der Domäne bleibt. Stellen Sie beim Beitritt einer Appliance zu einer Domäne sicher, dass Sie über Administratoranmeldeinformationen für den Domänencontroller verfügen.

Um sicherzustellen, dass die Citrix SD-WAN WANOP-Appliance den CIFS- und MAPI-Verkehr optimiert (einschließlich des als RPC gekapselten Datenverkehrs über HTTPS), müssen Sie die Appliance zu einem Teil der Domäne machen, zu der der Windows-Fileserver und Exchange-Server gehören. Sie müssen die serverseitige Appliance der Domäne beitreten.

Hinweis: Die Anmeldeinformationen für die Domänenverwaltung werden nicht auf der Appliance gespeichert.

### So verbinden Sie eine Citrix SD-WAN WANOP Appliance mit einer Windows-Domäne:

1. Navigieren Sie zur Registerkarte **Konfiguration > Sichere Beschleunigung > Windows-Domäne**.
2. Klicken Sie auf **Windows-Domäne beitreten**.

3. Geben Sie den Windows-Domännennamen in das Feld Domänenname ein.
4. Geben Sie im Feld Benutzername den Benutzernamen des Domänencontroller Administrators ein.
5. Geben Sie im Feld Kennwort das Administratorkennwort des Domänencontroller an.
6. Bearbeiten Sie bei Bedarf die DNS-Server auf Konsistenz mit der Windows-Domäne.
7. Klicken Sie auf **OK**.
8. Fügen Sie im Abschnitt Delegierte Benutzer einen Delegatbenutzer hinzu, wie in den folgenden Verfahren beschrieben.

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN WANOP 10.2 interface. The left sidebar lists various settings, with 'Secure Acceleration' selected. The main panel shows the 'Secure Acceleration' configuration. At the top, 'SSL Optimization status' is 'ACTIVE'. Below, 'Secure Peering' is 'Enabled'. The 'Windows Domain' section is expanded, showing fields for 'Domain Name' (example.com), 'User Name' (user), 'Password' (masked), and 'DNS Servers' (172.16.0.71). There are 'OK' and 'Cancel' buttons at the bottom.

### Konfigurieren Sie einen Delegatbenutzer:

Nachdem Sie die Appliance einer Windows-Domäne hinzugefügt haben, müssen Sie einen Benutzer erstellen, mit dem die Appliance Benutzer bei der Domäne authentifizieren kann. Dieser Benutzer wird als *Delegatbenutzer* bezeichnet.

Hinweis: Um ein Delegatbenutzerkonto zu erstellen, benötigen Sie Administratorzugriff auf den Windows-Domänencontroller und die Appliance. Wenn Sie keinen Administratorzugriff auf den Windows-Domänencontroller haben, stellen Sie sicher, dass ein autorisierter Administrator die erforderlichen Aufgaben auf dem Domänencontroller ausführt.

Das Einrichten der Benutzerauthentifizierung mithilfe der Kerberos-Delegierung umfasst zwei Aufgaben: Die Konfiguration eines Delegate-Benutzers auf dem Domänencontroller und das anschließende Hinzufügen dieses Benutzers zur Citrix SD-WAN WANOP-Appliance.

### **Konfigurieren Sie einen Delegatbenutzer auf einem Domänencontroller:**

Bevor Sie einen Delegate-Benutzer auf einer Citrix SD-WAN WANOP-Appliance konfigurieren, müssen Sie einen Delegate-Benutzer mit den erforderlichen Eigenschaften auf dem Domänencontroller konfigurieren. Sie können entweder ein Delegatbenutzerkonto erstellen oder ein vorhandenes Benutzerkonto als Delegatbenutzerkonto verwenden.

Aktivieren Sie nach dem Erstellen eines Kontos oder der Auswahl eines vorhandenen Kontos die Delegierung für diesen Benutzer. Anschließend ordnen Sie den Delegatbenutzer den CIFS- und Exchange-Diensten zu, damit der Datenverkehr für diese Dienste beschleunigt werden kann. Nachdem Sie diesen Benutzer der Citrix SD-WAN WANOP-Appliance hinzugefügt haben, zeigt die Appliance delegierte Anmeldeinformationen für die mit diesem Konto verbundenen Dienste an.

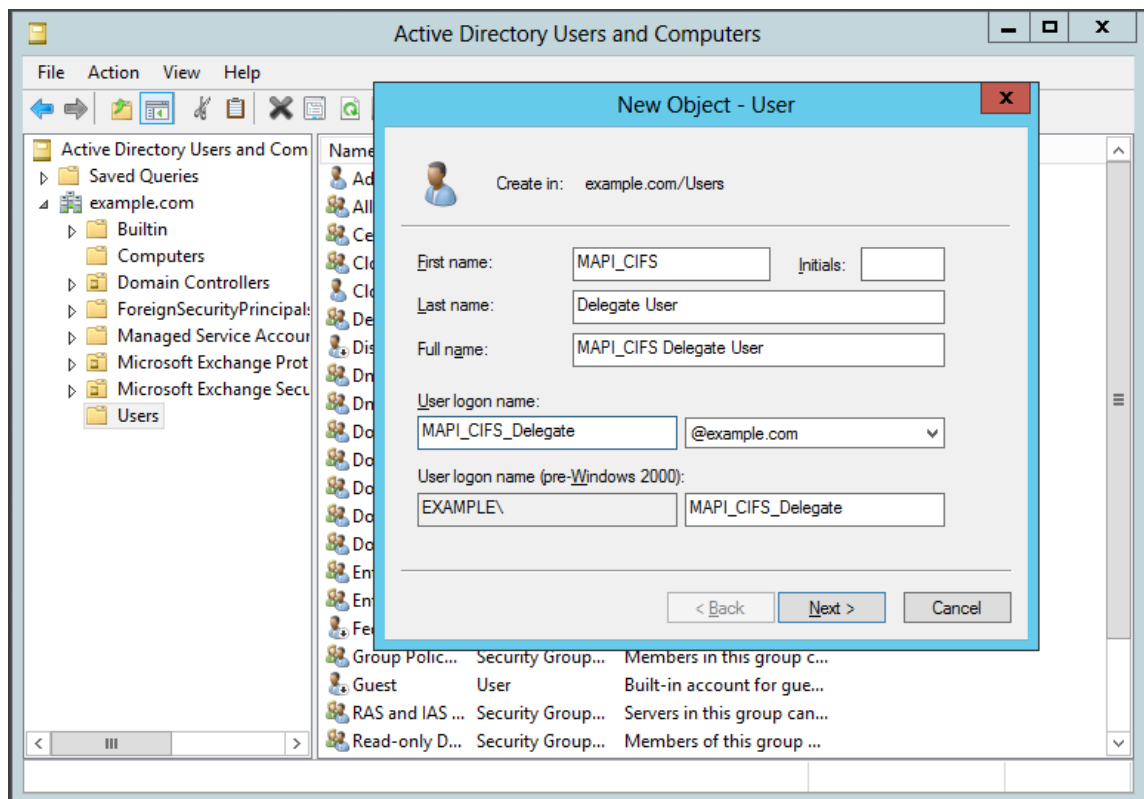
### **Erstellen Sie ein Delegatbenutzerkonto:**

Erstellen Sie ein Delegate-Benutzerkonto auf dem Windows-Domänencontroller, damit die Citrix SD-WAN WANOP-Appliance dieses Konto im Namen der Benutzer verwenden kann, um sie beim Domänencontroller zu authentifizieren.

Hinweis: Wenn Sie einen vorhandenen Benutzer als Delegatbenutzer konfigurieren möchten, überspringen Sie diese Prozedur.

### **So erstellen Sie ein Delegatbenutzerkonto:**

1. Melden Sie sich beim Windows-Domänencontroller als Administrator an. Stellen Sie sicher, dass der Dateiserver oder Exchange-Server Mitglied dieser Domäne ist.
2. Öffnen Sie im **Startmenü** das Fenster **Active Directory Benutzer und -Computer**.
3. Erstellen Sie einen Delegatbenutzer, wie im folgenden Screenshot gezeigt:

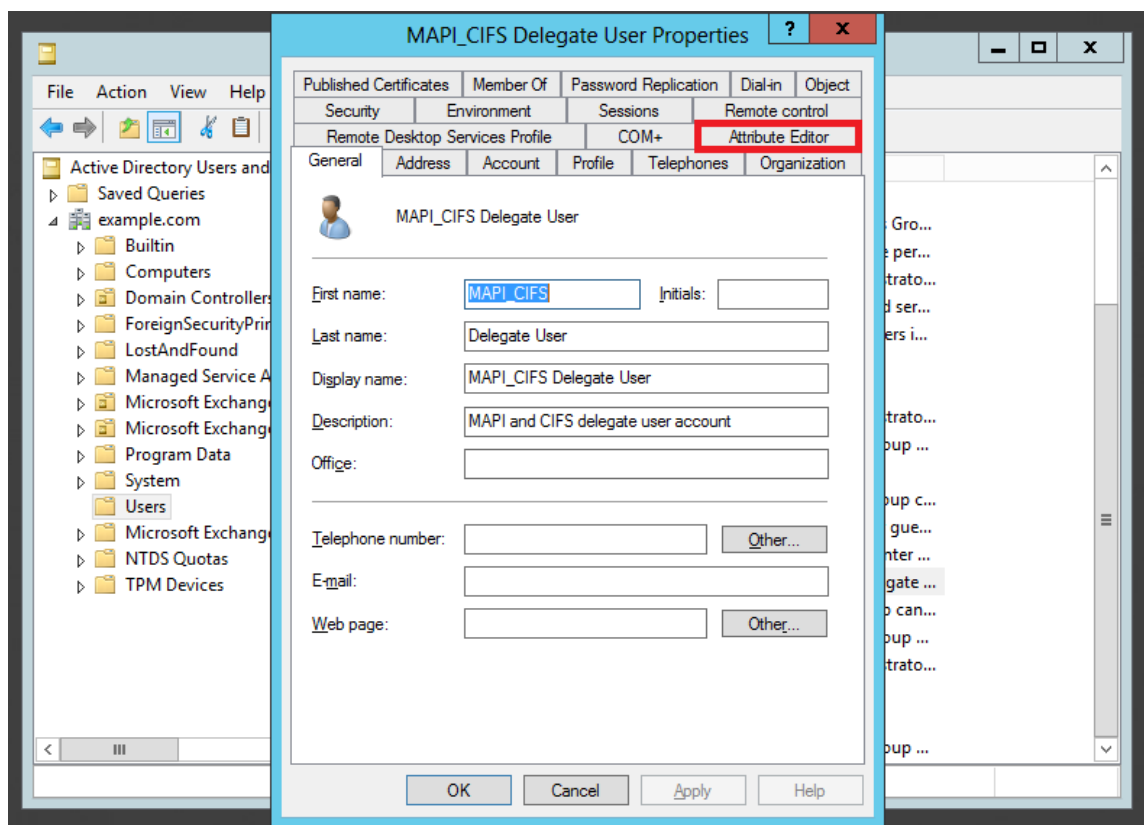


### Delegierung für einen Benutzer aktivieren:

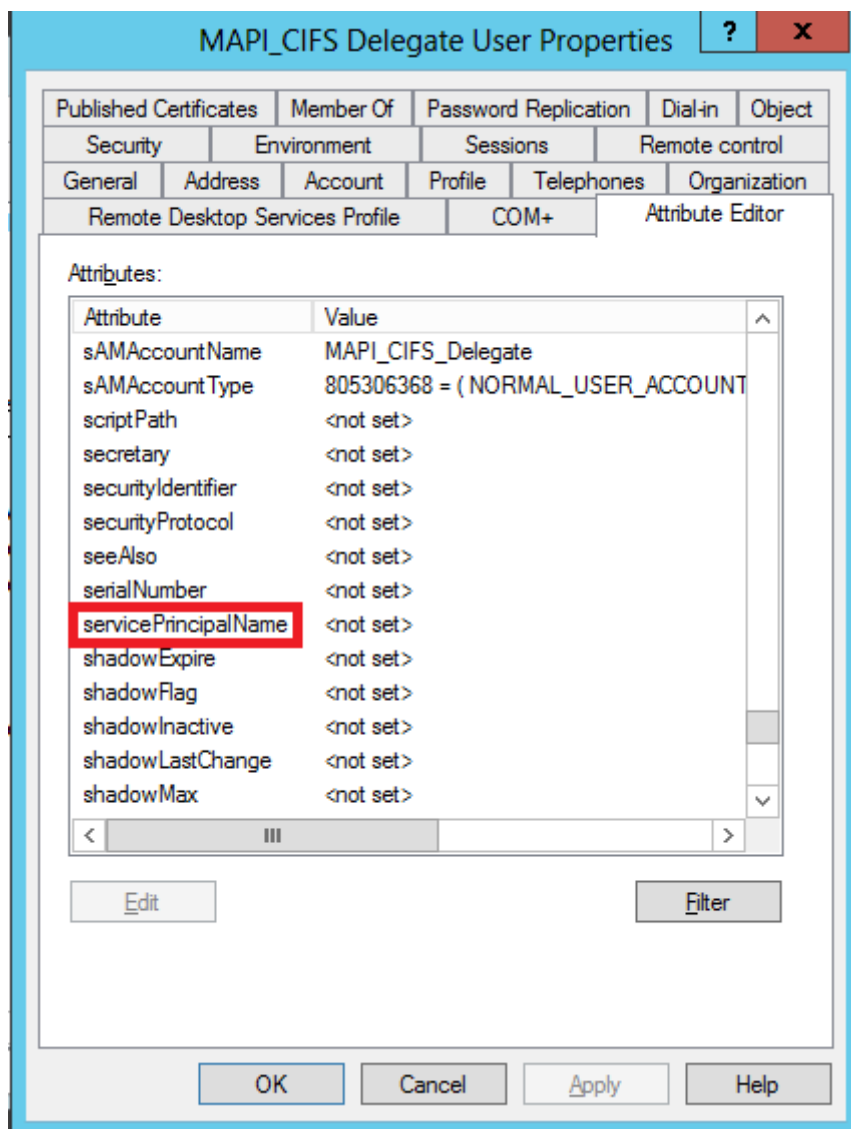
Bisher ähnelt der von Ihnen erstellte Benutzer jedem Benutzer, den Sie auf dem Active Directory -Server erstellen. Um die Delegierung für den Benutzer zu aktivieren, müssen Sie das Dienstprinzipalname-Attribut des Benutzers festlegen, um den *Delegatbenutzer* mit den erforderlichen Diensten zu delegieren und zuzuordnen. Dadurch erhält der Benutzer spezielle Berechtigungen, die ihm zugewiesen sind und ihn zu einem Delegatbenutzer machen.

### So aktivieren Sie die Delegierung für den Benutzer:

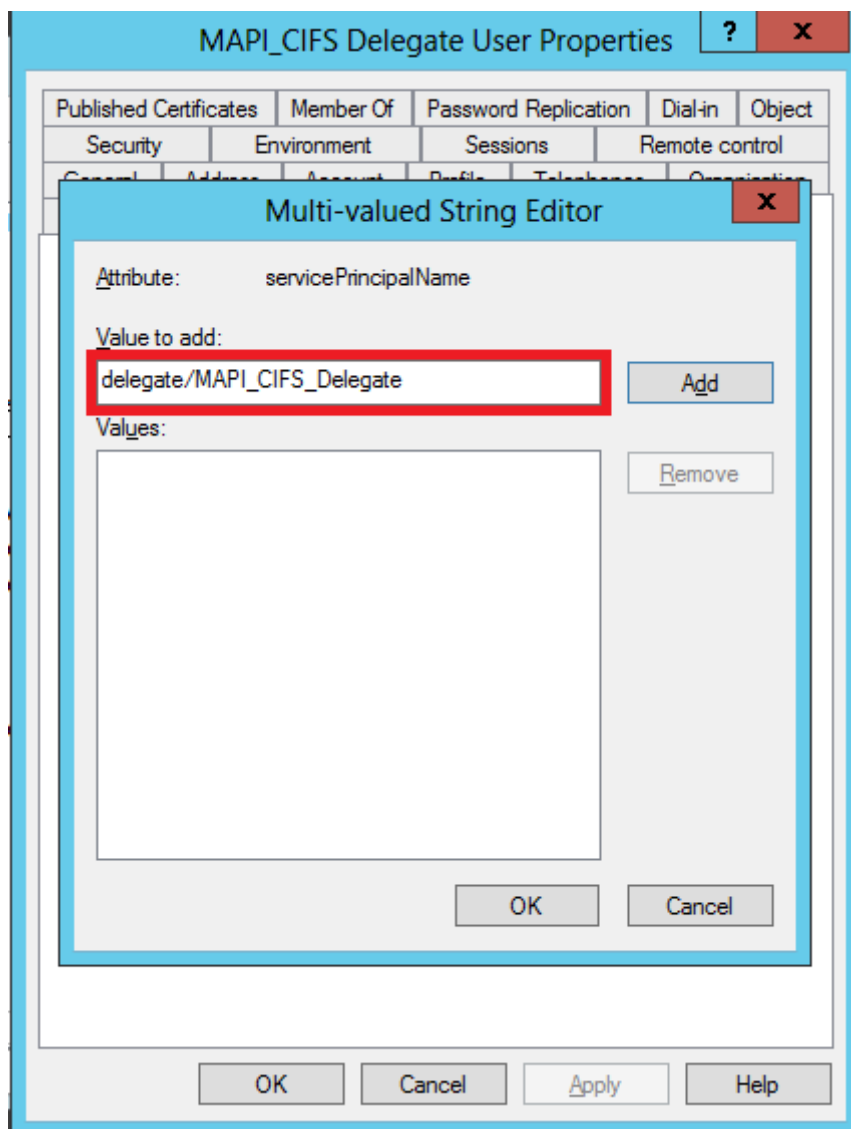
1. Öffnen Sie im **Startmenü** das Fenster **Active Directory Benutzer und -Computer**.
2. Wählen Sie im Menü Ansicht die Option **Erweiterte Funktionenaus**.
3. Wählen Sie den Knoten **Benutzer** aus.
4. Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie als Delegatbenutzer festlegen möchten.
5. Wählen Sie im Kontextmenü **Eigenschaften** und navigieren Sie zur Registerkarte **Attribut-Editor**, wie im folgenden Screenshot gezeigt:



6. Wählen Sie in der Liste **Attribute** die Option **ServicePrincipalName** aus, wie im folgenden Screenshot gezeigt:



7. Klicken Sie auf **Edit**.
8. Geben Sie im Dialogfeld **Mehrwertiger String-Editor** im Feld Zu **hinzuzufügender Wert delegate/<Benutzername>** an, wie im folgenden Screenshot gezeigt:



9. Klicken Sie auf **Hinzufügen**.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf **Apply**.
12. Klicken Sie auf **OK**.
13. Öffnen Sie das Dialogfeld **MAPI-CIFS-Delegate-Benutzereigenschaften** des Benutzers, und stellen Sie sicher, dass die Registerkarte **Delegierung** dem Dialogfeld hinzugefügt wurde, wie im folgenden Screenshot gezeigt:

**MAPI\_CIFS Delegate User Properties**

Organization | Published Certificates | Member Of | Password Replication  
 Dial-in | Object | Security | Environment | Sessions  
 Remote control | Remote Desktop Services Profile | COM+ | Attribute Editor  
 General | Address | Account | Profile | Telephones | **Delegation**

MAPI\_CIFS Delegate User

First name:  Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

### Ordnen Sie den Delegatbenutzer CIFS- und Exchange-Diensten zu:

Nachdem Sie die Registerkarte Delegierung für den Benutzer aktiviert haben, können Sie den Benutzer Dienste zuordnen, für die der Benutzer delegierte Anmeldeinformationen präsentieren kann. Wenn Sie diesen Benutzer zur Citrix SD-WAN WANOP-Appliance hinzufügen, stellt die Appliance delegierte Anmeldeinformationen für die mit diesem Konto verknüpften Dienste bereit.

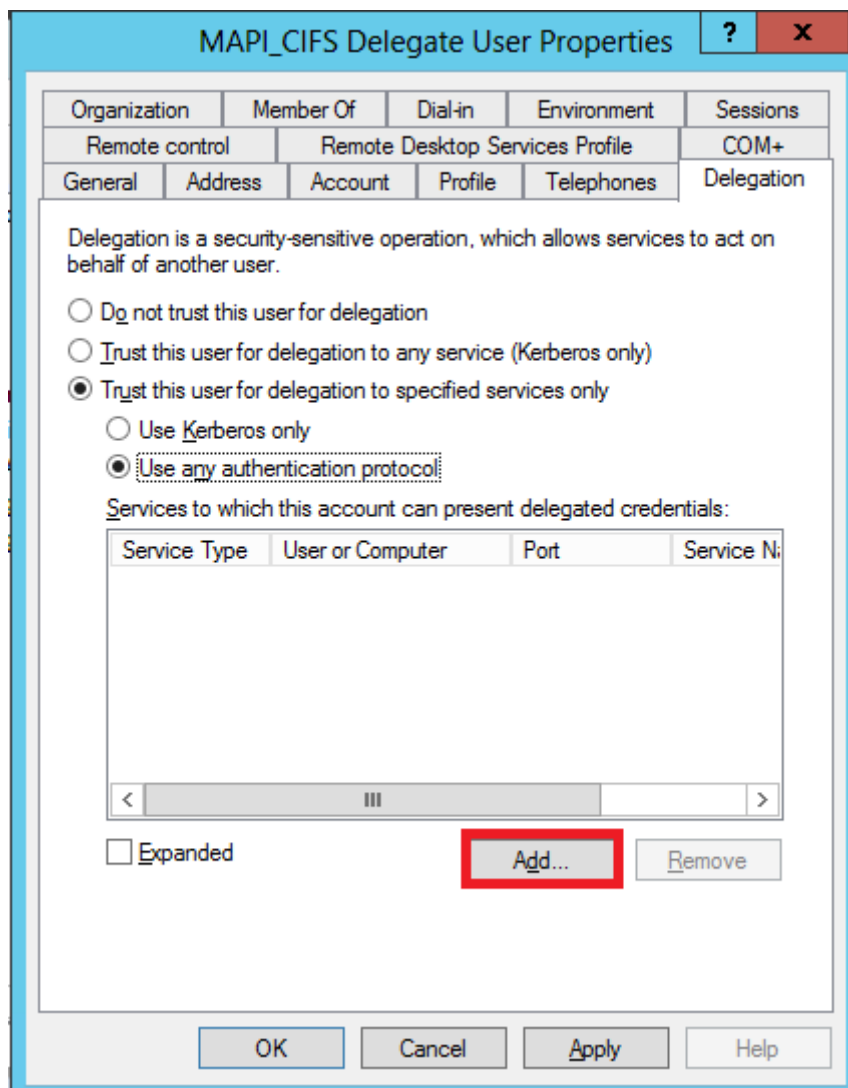
Hinweis: Die Windows-Sicherheitsinfrastruktur verwendet den Exchange-Dienst, um den MAPI-Datenverkehr zu verwalten.

### So ordnen Sie den Delegatbenutzer CIFS- und Exchange-Diensten zu:

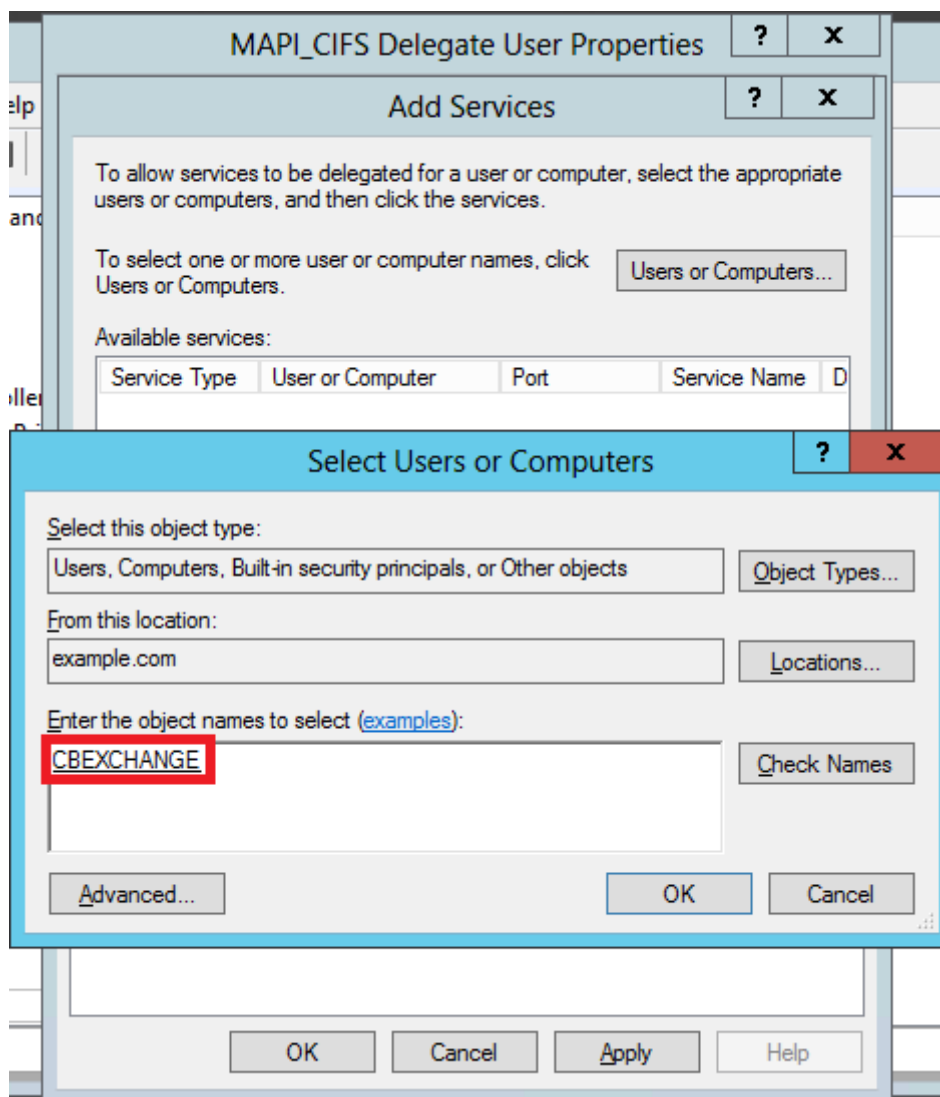
1. Wählen Sie auf der Registerkarte Delegierung die Option **Nur diesem Benutzer für Delegierung an bestimmte Dienste vertrauen** aus.
2. Wählen Sie die Option **Beliebiges Authentifizierungsprotokoll verwenden** aus.



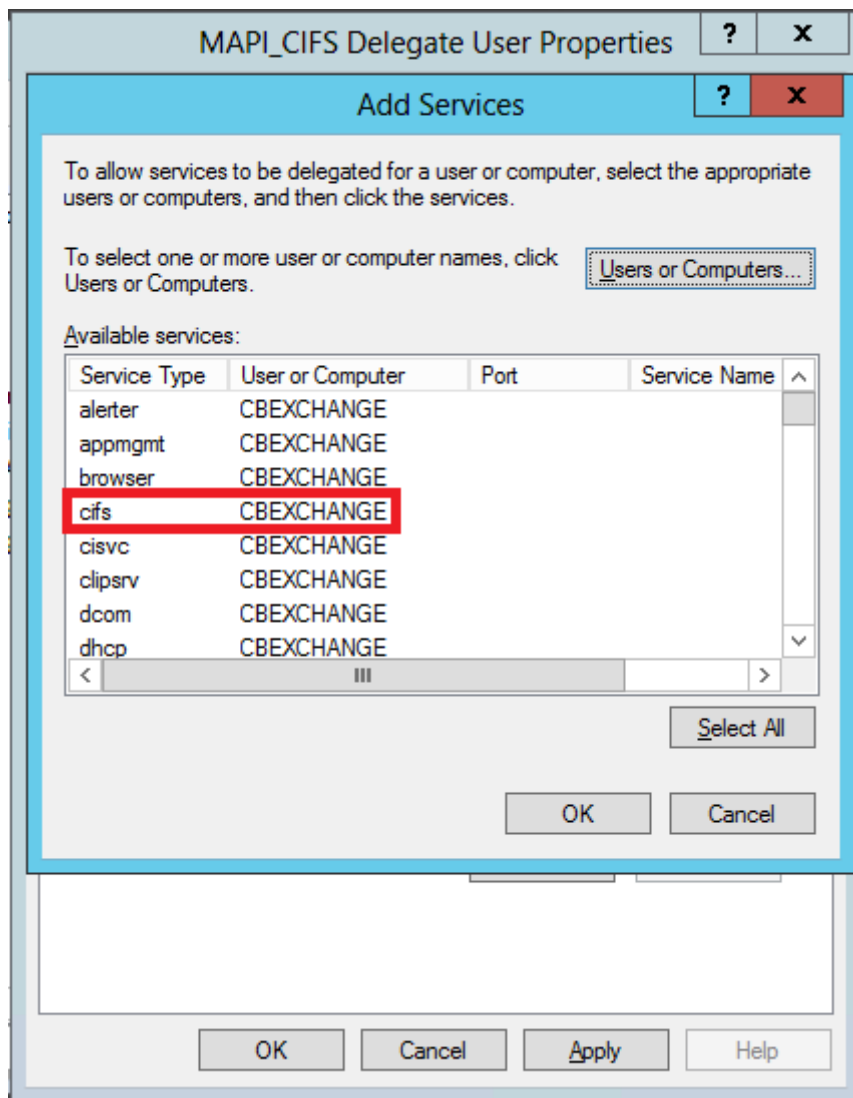
3. Klicken Sie auf **Hinzufügen**, wie im folgenden Screenshot gezeigt:



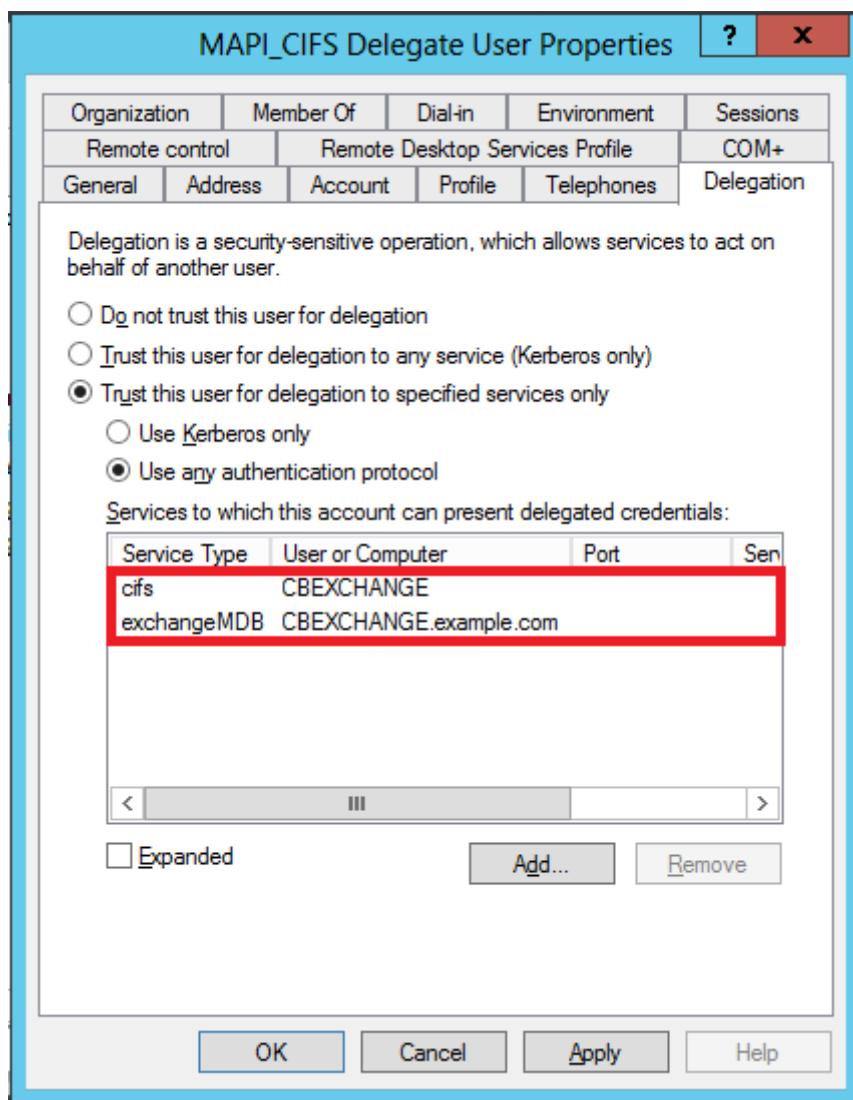
4. Klicken **Sie im Dialogfeld Dienst hinzufügen** auf **Benutzer und Computer** .
5. Fügen **Sie im Dialogfeld Benutzer oder Computer auswählen** den zu wählenden lokalen Computer hinzu, wie im folgenden Screenshot gezeigt:



6. Klicken Sie auf **OK**.
7. Wählen Sie im Dialogfeld Dienste hinzufügen aus der Liste **Verfügbare Dienstecifs** aus, wie im folgenden Screenshot gezeigt:



- Wenn Sie die MAPI-Beschleunigung auf der Citrix SD-WAN WANOP-Appliance einrichten müssen, halten Sie die **Strg-Taste gedrückt** und wählen Sie den **ExchangeMDB-Dienst** aus.
- Klicken Sie auf **OK**. Die von Ihnen ausgewählten Dienste werden zu den **Diensten hinzugefügt, denen dieses Konto delegierte Anmeldeinformationen anzeigen kann**, wie im folgenden Screenshot gezeigt:



10. Klicken Sie auf **OK**.

11. Schließen Sie das Fenster **Active Directory Benutzer und -Computer**.

#### Konfigurieren Sie einen Delegate-Benutzer auf einer Citrix SD-WAN WANOP-Appliance:

Nachdem Sie den Delegate-Benutzer auf dem Active Directory Directory-Server konfiguriert haben, müssen Sie diesen Benutzer auf der Citrix SD-WAN WANOP-Appliance konfigurieren, damit die Appliance die delegierten Anmeldeinformationen dieses Benutzers für die Domäne darstellen kann. Dadurch kann die Appliance den Netzwerkverkehr für die erweiterten CIFS- und MAPI-Beschleunigungsfunktionen aktiv optimieren.

#### So fügen Sie der serverseitigen Appliance den Delegatbenutzer hinzu:

1. Navigieren Sie zur Registerkarte **Konfiguration > Sichere Beschleunigung > Windows-Domäne**.

2. Klicken Sie auf die Schaltfläche **Windows-Domäne beitreten**, falls vorhanden.
3. Klicken Sie unter **Delegieren Benutzer** auf **Hinzufügen**.
4. Geben Sie im Feld **Domänenname** den Domännennamen an. Dies ist in der Regel die Domäne, die Sie im Abschnitt **Windows-Domäne** angegeben haben.
5. Geben Sie im Feld **Benutzername** den Benutzernamen des Delegatbenutzers ein.
6. Geben Sie im Feld **Kennwort** das Kennwort des Delegatbenutzers an.
7. Klicken Sie auf **Hinzufügen**.

**Delegate Users**

Add X Edit Delete Services

Add a delegate user account of the Windows domain controller. The CloudBridge appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name\*  
example.com  
[Check Delegate User](#)

User Name\*  
delegate\_user

Password\*  
..... ?

Add Cancel

User Name	Domain Name
No items	

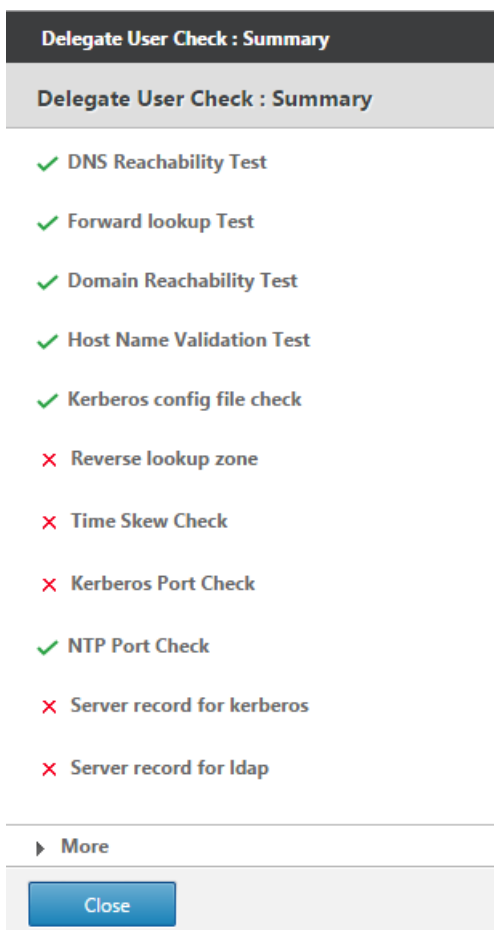
## Stellen Sie sicher, dass die Appliance der Domäne beigetreten ist

Wenn Sie nach dem Hinzufügen der Appliance zur Domäne feststellen, dass die Appliance den sicheren Windows-Datenverkehr nicht optimiert, hat möglicherweise ein Fehler verhindert, dass die Appliance der Domäne beitrifft. Sie können das Dienstprogramm **vor der Domänenüberprüfung** verwenden, um herauszufinden, ob Probleme mit dem Beitritt der Appliance zur Domäne auftreten. Sie können dieses Dienstprogramm sogar ausführen, um mögliche Probleme zu identifizieren, bevor Sie versuchen, die Appliance einer Domäne beitreten.

### So überprüfen Sie den Delegatbenutzer:

1. Melden Sie sich bei der serverseitigen Citrix SD-WAN WANOP-Appliance an.
2. Navigieren Sie zu **Konfiguration > Sichere Beschleunigung > Registerkarte Windows**.

3. Klicken Sie auf die Schaltfläche **Windows-Domäne beitreten**, falls vorhanden.
4. Wählen Sie einen Delegatbenutzer aus, und klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf **Delegate-Benutzer überprüfen**.
6. Warten Sie, bis die Delegate-Benutzerdomänenüberprüfung abgeschlossen ist, und überprüfen Sie die Ergebnisse.



## Konfigurieren der CIFS- und SMB2/SMB3-Beschleunigung

April 19, 2021

Die CIFS-Beschleunigungsfunktion bietet eine Reihe von protokollspezifischen Leistungsverbesserungen für CIFS-basierte Dateiübertragung (Windows und Samba) und Verzeichnissuche, einschließlich Verbesserungen beim CIFS-Transport und verwandten Protokollen wie DCERPC.

CIFS-Beschleunigung besteht aus drei Teilen:

- TCP-Durchflusssteuerungsbeschleunigung —Dies wird bei allen beschleunigten CIFS-Verbindungen ausgeführt, unabhängig von der Protokollversion (SMB1, SMB2 oder SMB3) oder Authentifizierungs- und Verschlüsselungsgrad.
- CIFS-Protokollbeschleunigung: Diese Optimierungen erhöhen die CIFS-Leistung, indem die Anzahl der Roundtrips reduziert wird, die zum Ausführen eines CIFS-Befehls erforderlich sind. Diese Optimierungen werden automatisch auf SMB1- und SMB2-CIFS-Verbindungen durchgeführt, die entweder keine CIFS-Paketauthentifizierung (Signieren) verwenden oder wenn Signaturen verwendet werden und die Appliances der Windows-Domäne in einer Rolle Sicherheitsdelegaten beigetreten sind.
- CIFS-Komprimierung —CIFS-Verbindungen werden automatisch komprimiert, wenn sie die Anforderungen für die CIFS-Protokollbeschleunigung erfüllen. Darüber hinaus werden SMB3-Verbindungen komprimiert, wenn sie nicht signiert und entsiegelt sind.

In Netzwerken, in denen CIFS-Signierung aktiviert ist, erfordern die Beschleunigung und Komprimierung des CIFS-Protokolls, dass Sie entweder die CIFS-Paketauthentifizierung deaktivieren (Signieren) oder Ihre Rechenzentrum-Appliances der Windows-Domäne beitreten lassen und eine sichere Peer-Beziehung zwischen den Datacenter-Appliances und Ihren Remote-Appliances herstellen und Citrix SD-WAN WANOP Plug-ins.

**Tabelle 1. CIFS-Beschleunigungsfunktionen, nach SMB-Protokollversion und ob die Appliance der Windows-Domäne beigetreten ist.**

SMB-Version	TCP-Flusssteuerung	Komprimierung	Protokollbeschleunigung
		<i>Signieren deaktiviert</i>	
<b>SMB 1.0</b>	J	J	J
<b>SMB 2.0</b>	J	J	J
<b>SMB 2.1</b>	J	J	N
<b>SMB 3.0</b>	J	J	N
		<i>Signierung aktiviert, Citrix SD-WAN WANOP ist der Domäne beigetreten **</i>	
<b>SMB 1.0</b>	J	J	J
<b>SMB 2.0</b>	J	J	J
<b>SMB 2.1</b>	J	J	J
<b>SMB 3.0</b>	J	J	Y *

SMB-Version	TCP-Flusssteuerung	Komprimierung	Protokollbeschleunigung
		<i>Signierung aktiviert, Citrix SD-WAN WANOP ist der Domäne nicht beigetreten</i>	
<b>SMB 1.0</b>	J	N	N
<b>SMB 2.0</b>	J	N	N
<b>SMB 2.1</b>	J	N	N
<b>SMB 3.0</b>	J	N	N

\* SMB 3.0 Support wurde in Version 7.4.2 hinzugefügt.

\*\* Citrix SD-WAN WANOP unterstützt keine NTLMv2-Authentifizierung (Standard für Windows 7) bis hin zu SMB 1/SMB 2/ SMB 3 und mit NetApp-Server. Aktivieren der Kerberos-Authentifizierung ermöglicht Beschleunigung.

**Tabelle 2. Welche SMB-Protokollversion wird vom Client- und Server-Betriebssystem verwendet.**

Client/Server-Betriebssystem	Windows 8, Windows 10 oder Windows Server 2012	Windows 7 oder Windows Server 2008 R2	Windows Vista oder Windows Server 2008	Frühere Versionen von Windows
<b>Windows 8, Windows 10 oder Windows Server 2012</b>	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
<b>Windows 7 oder Windows Server 2008 R2</b>	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
<b>Windows Vista oder Windows Server 2008</b>	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
<b>Frühere Versionen von Windows</b>	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0



**Unterstützte Versionen von CIFS:**

Nicht jede CIFS-Implementierung verwendet Anforderungsmuster, die von der Appliance erkannt werden. Diese nicht unterstützten Versionen erreichen keine Beschleunigung in allen Fällen, wie in der folgenden Tabelle gezeigt.

**Tabelle 3. Citrix SD-WAN WANOP Unterstützung für CIFS-Server und Clients.**

Produkt	Server	Client
Windows Server 2003-2012	Ja*	Ja*
Windows XP, Vista, 7, 8, 2000	Ja*	Ja*
NetApp	Ja**	Nicht zutreffend
Hitachi	Ja**	Nicht zutreffend
Windows NT	Ja	Nein
Windows ME und früher	Nein	Nein
Andere	Siehe Hinweis	Siehe Hinweis

\* SMB 3.0-Unterstützung wurde in Version 7.4.2 eingeführt.

\*\* Der Betrieb mit SMB 3.0 wurde ab Version 7.4.2 nicht getestet.

**Hinweis:** Die meisten CIFS-Implementierungen von Drittanbietern emulieren einen der oben aufgeführten Server oder Clients. Soweit die Emulation erfolgreich ist, wird der Datenverkehr beschleunigt oder nicht, wie in der obigen Tabelle gezeigt. Wenn sich die Emulation anders verhält als der CIFS-Beschleuniger erwartet, wird die CIFS-Beschleunigung für diese Verbindung beendet.

Das Verhalten der CIFS-Beschleunigung mit einer bestimmten CIFS-Implementierung kann nicht sicher bekannt sein, bis es getestet wurde.

Die Modi der CIFS-Beschleunigung sind:

- Lese- und Schreibvorgänge in großen Dateien
- Kleine Dateien lesen und schreiben
- Verzeichnissuche.

**Lese- und Schreibvorgänge großer Dateien**—Diese SMB1-Optimierungen sind für Dateiübertragungen von mindestens 640 KB geeignet. Sichere Read-Ahead- und Write-Behind Techniken werden verwendet, um die Daten ohne Pausen für jede Übertragung zu streamen (eine Übertragung beträgt 64 KB oder weniger).

Diese Optimierungen werden nur dann aktiviert, wenn die Übertragung eine BATCH- oder EXCLUSIVE Sperre hat und einfach ist. Dateikopien sind immer einfach. Dateien, die über Anwendungen geöffnet werden, sind möglicherweise oder nicht, je nachdem, wie sie innerhalb der Anwendung behandelt werden.

Geschwindigkeitsverhältnisse von 10x sind leicht mit CIFS-Beschleunigung erhältlich, vorausgesetzt, dass Ihre Verbindung und Festplatten schnell genug sind, um das Zehnfache Ihrer aktuellen Übertragungsgeschwindigkeiten aufzunehmen. 50x Beschleunigung kann bei Bedarf erhalten werden, ist aber aufgrund des Speicherverbrauchs normalerweise nicht aktiviert. Wenden Sie sich an Ihren Citrix Vertreter, wenn 10x nicht ausreicht.

**Lese- und Schreibvorgänge in kleinen Dateien**—Verbesserungen bei kleinen Dateien zentrieren sich mehr auf Metadaten (Verzeichnis-) Optimierungen als auf Datenstreaming. Native CIFS kombiniert Metadatenanforderungen nicht effizient. CIFS-Beschleunigung tut es. Wie bei der Beschleunigung großer Dateien werden diese Optimierungen nur durchgeführt, wenn sie sicher sind (z. B. werden sie nicht ausgeführt, wenn dem CIFS-Client keine exklusive Sperre für das Verzeichnis gewährt wurde.) Wenn das SMB2-Protokoll verwendet wird, werden Dateimetadaten lokal zwischengespeichert, um noch größere Verbesserungen zu erzielen.

**Verzeichnissuche**—Standard-CIFS-Clients führen das Durchsuchen von Verzeichnissen äußerst ineffizient durch und erfordern eine enorme Anzahl von Roundtrips, um einen Remote-Ordner zu öffnen. CIFS-Beschleunigung reduziert die Anzahl der Roundtrips auf 2 oder 3. Wenn das SMB2-Protokoll verwendet wird, werden Verzeichnisdaten lokal zwischengespeichert, um noch größere Verbesserungen zu erzielen.

## **CIFS-Protokollbeschleunigung**

CIFS-Beschleunigung wird auf allen Modellen unterstützt. CIFS ist ein TCP-basiertes Protokoll und profitiert von der Flusssteuerung. CIFS wird jedoch in einer Weise implementiert, die in Langstreckennetzen sehr ineffizient ist und eine übermäßige Anzahl von Hin- und Rückfahrten erfordert, um einen Vorgang abzuschließen. Da das Protokoll sehr empfindlich auf die Verbindungslatenz reagiert, muss die volle Beschleunigung protokollbewusst sein.

CIFS-Beschleunigung reduziert die Anzahl der Roundtrips durch eine Vielzahl von Techniken. Das Muster der Anfragen vom Client wird analysiert und seine nächste Aktion wird prognostiziert. In vielen Fällen ist es sicher, auf die Vorhersage zu reagieren, auch wenn sie falsch ist, und diese sicheren Operationen sind die Grundlage vieler Optimierungen.

Beispielsweise geben SMB1-Clients sequentielle Datei-Lesevorgänge nicht überlappend aus und warten darauf, dass jeder 64 KB gelesene Lesevorgang abgeschlossen ist, bevor die nächste Ausgabe ausgegeben wird. Durch die Implementierung von Read-Ahead kann die Appliance sicher bis zu 10-fache Beschleunigung liefern, indem sie die erwarteten Daten im Voraus abrufen.

Zusätzliche Techniken beschleunigen das Durchsuchen von Verzeichnissen und Operationen mit kleinen Dateien. Die Beschleunigung wird nicht nur auf CIFS-Vorgänge angewendet, sondern auch auf die zugehörigen RPC-Vorgänge.

## **Voraussetzungen**

CIFS-Beschleunigung wird auf allen Modellen unterstützt. CIFS ist ein TCP-basiertes Protokoll und profitiert von der Flusststeuerung. CIFS wird jedoch in einer Weise implementiert, die in Langstreckennetzen sehr ineffizient ist und eine übermäßige Anzahl von Hin- und Rückfahrten erfordert, um einen Vorgang abzuschließen. Da das Protokoll sehr empfindlich auf die Verbindungslatenz reagiert, muss die volle Beschleunigung protokollbewusst sein.

CIFS-Beschleunigung reduziert die Anzahl der Roundtrips durch eine Vielzahl von Techniken. Das Muster der Anfragen vom Client wird analysiert und seine nächste Aktion wird prognostiziert. In vielen Fällen ist es sicher, auf die Vorhersage zu reagieren, auch wenn sie falsch ist, und diese sicheren Operationen sind die Grundlage vieler Optimierungen.

Beispielsweise geben SMB1-Clients sequentielle Datei-Lesevorgänge nicht überlappend aus und warten darauf, dass jeder 64 KB gelesene Lesevorgang abgeschlossen ist, bevor die nächste Ausgabe ausgegeben wird. Durch die Implementierung von Read-Ahead kann die Appliance sicher bis zu 10-fache Beschleunigung liefern, indem sie die erwarteten Daten im Voraus abruft.

Zusätzliche Techniken beschleunigen das Durchsuchen von Verzeichnissen und Operationen mit kleinen Dateien. Die Beschleunigung wird nicht nur auf CIFS-Vorgänge angewendet, sondern auch auf die zugehörigen RPC-Vorgänge.

Wenn Ihr Netzwerk CIFS-Signatur verwendet, muss die Appliance ein vertrauenswürdiges Mitglied der Domäne sein. Informationen zum Erstellen der Appliance zu einem vertrauenswürdigen Mitglied der Domäne finden Sie unter [Hinzufügen einer Citrix SD-WAN WANOP Appliance zur Windows-Sicherheitsinfrastruktur](#).

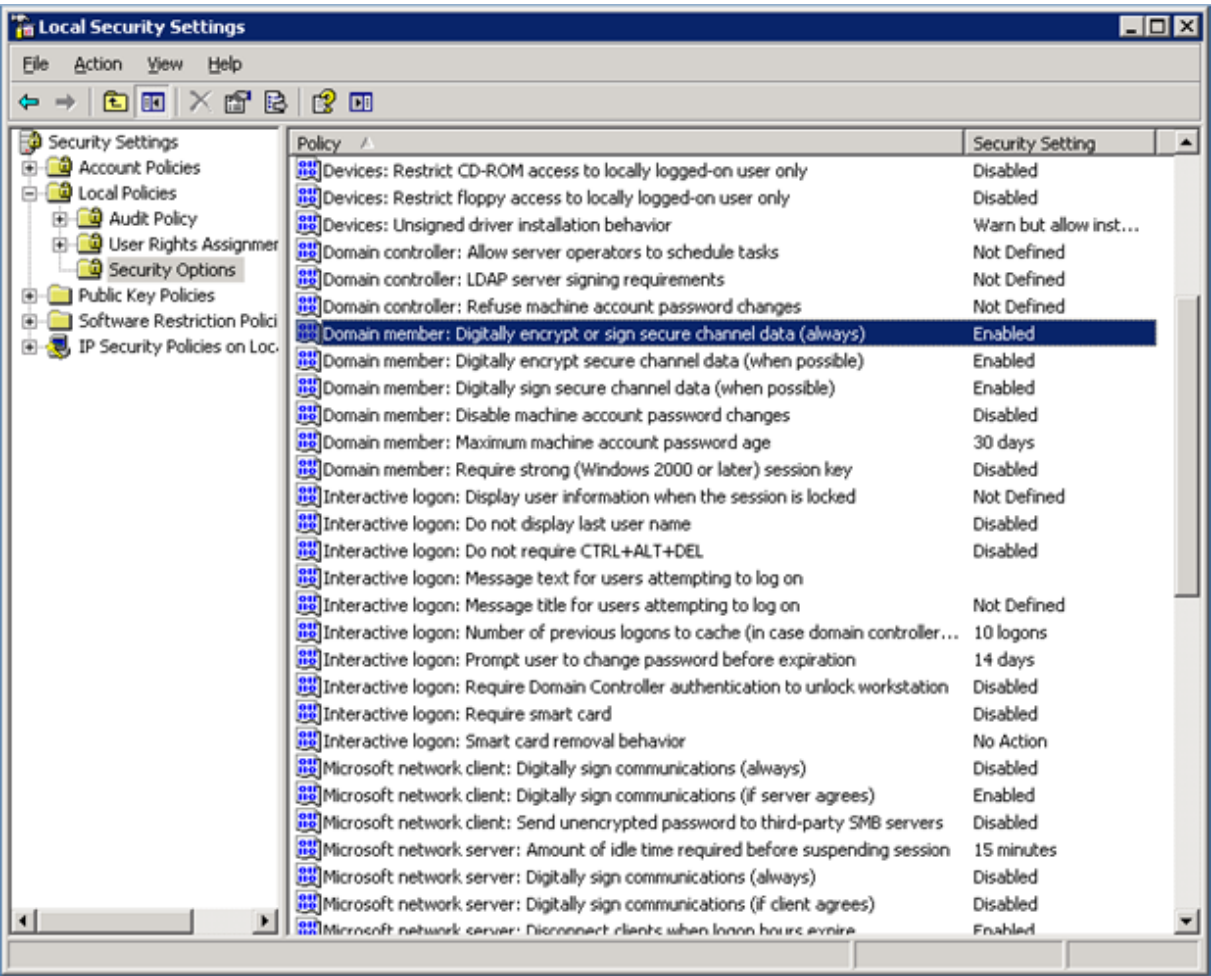
## **Konfigurieren der CIFS-Protokollbeschleunigung**

Die CIFS-Beschleunigung ist standardmäßig für Verbindungen aktiviert, die keine CIFS-Signatur verwenden. Wenn Ihr Netzwerk Signaturen verwendet, kann es entweder deaktiviert werden oder die serverseitigen Appliances können [der Windows-Domäne beitreten](#).

### **CIFS-Signatur deaktivieren**

Abhängig von den Sicherheitseinstellungen müssen die Sicherheitseinstellungen für Windows-Server oder Domänenserver möglicherweise angepasst werden.

Abbildung 1. Windows Server-Sicherheitsoptionen, Windows Server 2003 und Windows Server 2008.



Windows-Dateiserver haben zwei Sicherheitsmodi: Versiegelung und Signieren.

Die Versiegelung verschlüsselt den Datenstrom und verhindert die Beschleunigung des CIFS-Protokolls insgesamt.

Signieren fügt Authentifizierungsdaten zu jedem Datenpaket hinzu, ohne den Datenstrom zu verschlüsseln. Dies verhindert die Beschleunigung, es sei denn, Sie haben die unter beschriebenen Verfahren implementiert [Hinzufügen einer Citrix SD-WAN WANOP Appliance zur Windows-Sicherheitsinfrastruktur](#). Wenn diese Anforderung erfüllt ist, wird das Signieren automatisch beschleunigt. Andernfalls muss die Signierung deaktiviert sein (wenn sie nicht bereits deaktiviert ist), damit die Protokollbeschleunigung stattfinden kann.

Standardmäßig bieten Windows-Dateiserver Signaturen, erfordern diese jedoch nicht, außer für Domänenserver, für die dies standardmäßig erforderlich ist.

Um die CIFS-Beschleunigung bei Systemen zu erreichen, die derzeit signiert werden müssen, müssen Sie die Systemsicherheitseinstellungen ändern, um diese Anforderung zu deaktivieren. Sie können

dies in den lokalen Sicherheitseinstellungen auf dem Dateiserver oder in Gruppenrichtlinien tun. In den folgenden Beispielen für Windows Server 2003 und Windows Server 2008 werden die lokalen Einstellungen angezeigt. Die konzernpolitischen Änderungen sind natürlich fast identisch.

Citrix SD-WAN WANOP

### **So ändern Sie die Servereinstellung, um CIFS-Beschleunigung zuzulassen**

1. Navigieren Sie zur Seite Lokale Sicherheitseinstellungen des Systems.
2. Domänenmitglied festlegen: Verschlüsseln oder signieren Sie sichere Kanaldaten digital (immer) auf Deaktiviert.
3. Microsoft-Netzwerkclient festlegen: Kommunikation digital signieren (immer) auf Deaktiviert.
4. Microsoft Netzwerkserver festlegen: Kommunikation digital signieren (immer) auf Deaktiviert.

### **CIFS-Statistiken interpretieren**

Auf der Seite Überwachung: Dateisystem (CIFS/SMB) wird eine Liste der beschleunigten CIFS-Verbindungen angezeigt. Diese Verbindungen sind in optimierte und nicht optimierte Verbindungen unterteilt. Da alle diese Verbindungen beschleunigt werden (mit Flusssteuerung und Komprimierung), haben optimierte Verbindungen zusätzlich zur Flusssteuerung und -komprimierung CIFS-Optimierungen, während nicht optimierte Verbindungen nur Flusssteuerung und -komprimierung haben.

### **CIFS-Verwaltungszusammenfassung**

- Die CIFS-Beschleunigung bietet deutliche Verbesserungen auch bei relativ kurzen Strecken.
- Die CIFS-Beschleunigung beginnt, wenn der Client zum ersten Mal auf ein Dateisystem zugreift. Wenn die Beschleunigung aktiviert ist, wenn der Dateiserver und Client bereits ausgeführt und ausgeführt wird, erfolgt keine Beschleunigung für viele Minuten, bis die bereits vorhandenen CIFS-Verbindungen vollständig geschlossen sind. CIFS-Verbindungen sind sehr hartnäckig und dauern lange, bevor sie sich selbst schließen, selbst im Leerlauf. Dieses Verhalten ist während des Tests ärgerlich, hat aber wenig Bedeutung in der normalen Bereitstellung.
- Durch Aufheben einer Bereitstellung und Neubereitstellen eines Dateisystems in Windows werden die CIFS-Verbindungen nicht geschlossen, da Windows das Dateisystem nicht vollständig aufhebt. Der Neustart des Clients oder Servers funktioniert. Verwenden Sie für eine weniger invasive Maßnahme den Befehl `NET USE devicename /DELETE` von der Windows-Befehlszeile, um die Bereitstellung des Volumes vollständig aufzuheben. Unter Linux trennen `smbmount` und `umount` das Volume vollständig.

- Das Deaktivieren und erneute Aktivieren von CIFS-Lese- und Schreiboptimierungen auf der Appliance führt zu ähnlichen Problemen. Vorhandene Verbindungen werden nicht beschleunigt, wenn CIFS aktiviert ist, und die Anzahl der Protokollfehler erkannt auf der Seite Überwachung: Dateisystem (CIFS/SMB) erhöht sich kurz.
- CIFS-Statistiken können verwirrend sein, da nur die Appliance, die am weitesten vom Dateiserver entfernt ist, eine CIFS-Beschleunigung mit vollständigen Statistiken meldet. Die andere Appliance sieht es als gewöhnliche Beschleunigung.
- CIFS-Beschleunigung wird im Proxy-Modus nicht unterstützt.
- Wenn die CIFS-Beschleunigung nicht mit einem Windows-Server stattfindet, überprüfen Sie die Sicherheitseinstellungen des Servers.

## **MAPI-Beschleunigung konfigurieren**

April 19, 2021

Die Beschleunigung von Microsoft Outlook bietet eine verbesserte Leistung für den Datenverkehr zwischen Microsoft Outlook-Clients und Microsoft Exchange-Servern. Dies erhöht den Durchsatz mit einer Vielzahl von Optimierungen, einschließlich Datenvorabruf und -komprimierung.

Diese Funktion wird auch als MAPI-Beschleunigung bezeichnet, nachdem das MAPI-Protokoll zwischen Outlook und Exchange Server verwendet wird.

In Netzwerken, in denen der Outlook-Datenstrom unverschlüsselt ist (der Standardwert vor Outlook 2007), erfordert dieses Feature keine Konfiguration.

(In Netzwerken, in denen die Outlook-Daten verschlüsselt sind (standardmäßig mit Outlook 2007 und höher), kann die Beschleunigung auf zwei Arten abgerufen werden: durch Deaktivieren der Verschlüsselung in den Outlook-Clients oder durch die Verwendung der Appliances der Windows-Domäne beitreten[]/en-us/citrix-sd-wan-wanop/10-2/secure-traffic-acceleration/cifs-smb2-mapi.html.)

## **Unterstützte Outlook-Exchange-Versionen und -Modi**

Citrix SD-WAN WANOP-Appliances bieten unter den folgenden Umständen MAPI-Beschleunigung für Microsoft Outlook 2003-2016 und Exchange Server 2003-2010:

- Jede Kombination von unterstützten Clients und Servern (unter Verwendung des MAPI-Protokolls) wird unterstützt.
- Wenn die serverseitige Appliance einer Windows-Domäne beigetreten ist, werden Verbindungen mit MAPI-Verschlüsselung beschleunigt. Andernfalls sind sie nicht, und die Verschlüsselung sollte in den Outlook-Clients deaktiviert werden.

### Hinweis

In Exchange Server 2013 wurde das MAPI-Protokoll über das HTTP-Protokoll in RPC geändert, dieses Protokoll wird unterstützt. Mit Exchange Server SP1 wurde das RPC-über-HTTP-Protokoll in MAPI über HTTP-Protokoll geändert, dieses Protokoll wird derzeit nicht unterstützt.

## Voraussetzungen

Wenn Ihr Netzwerk verschlüsselte Outlook-Daten verwendet, die die Standardeinstellung in Outlook 2007 und höher ist, müssen Sie eine der folgenden Voraussetzungen implementieren, um sicherzustellen, dass MAPI-Verbindungen beschleunigt werden:

- Deaktivieren Sie die Verschlüsselung in den Outlook-Clients.
- Führen Sie die unter beschriebenen Aufgaben aus [Hinzufügen einer Citrix SD-WAN WANOP Appliance zur Windows-Sicherheitsinfrastruktur](#).

## Konfiguration

Die Outlook-Beschleunigung ist ein Feature mit Null-Konfiguration, das standardmäßig aktiviert ist. (Wenn nicht gewünscht, kann sie deaktiviert werden, indem die Beschleunigung in der MAPI-Dienstklasse auf der Seite

**Konfiguration: Dienstklassenrichtlinie** deaktiviert wird.) Die Outlook-Beschleunigung erfolgt automatisch, wenn die folgenden Bedingungen erfüllt sind:

- Am Ende des WAN befindet Exchange Server eine Appliance.
- Entweder gibt es am Outlook-Ende des WAN eine Appliance oder auf dem System, auf dem Outlook ausgeführt wird, wird auch das Citrix SD-WAN WANOP Plug-in ausgeführt.
- Der gesamte Outlook/Exchange-Datenverkehr wird durch die Appliances (oder Appliance und Plug-In) geleitet.
- Der Exchange Server oder Outlook wird neu gestartet (die Beschleunigung beginnt erst, wenn vorhandene MAPI-Verbindungen geschlossen sind).
- Entweder ist die Verschlüsselung in Outlook deaktiviert oder die serverseitige Appliance gehört zur Windows-Domäne und hat eine sichere Peer-Beziehung mit der clientseitigen Appliance (oder dem Citrix SD-WAN WANOP Plug-in). Wenn die Appliance der Windows-Domäne beigetreten ist, muss die Authentifizierung für die Domäne auf der Standardeinstellung (aushandeln) beibehalten werden, damit die Beschleunigung funktioniert.

## **Deaktivieren der Verschlüsselung in Outlook 2007 oder Outlook 2010**

Sofern die serverseitige Appliance nicht der Windows-Domäne beigetreten ist und eine sichere Peer-Beziehung mit der clientseitigen Appliance (oder Citrix SD-WAN WANOP Plug-in) hat, muss die Verschlüsselung zwischen Outlook und Exchange Server deaktiviert werden, damit eine Beschleunigung stattfindet.

Die Verschlüsselung wurde vor Outlook 2007 standardmäßig deaktiviert. Ab Outlook 2007 ist die Verschlüsselung standardmäßig aktiviert.

## **Leistungshinweis**

MAPI verwendet ein anderes Datenformat als andere Protokolle. Dieser Unterschied verhindert eine effektive Protokollübergreifende Komprimierung. Das heißt, eine Datei, die zuerst über FTP und dann als E-Mail-Anhang übertragen wurde, erhält keinen Komprimierungsvorteil bei der zweiten Übertragung. Wenn die gleichen Daten zweimal im MAPI-Format gesendet werden, erhält die zweite Übertragung volle Komprimierung.

## **SSL-Komprimierung**

April 19, 2021

Die Citrix SD-WAN WANOP SSL-Komprimierung wendet Multisession-Komprimierung auf SSL-Verbindungen (z. B. HTTPS-Verkehr) an und bietet Komprimierungsverhältnisse von bis zu 10.000:1.

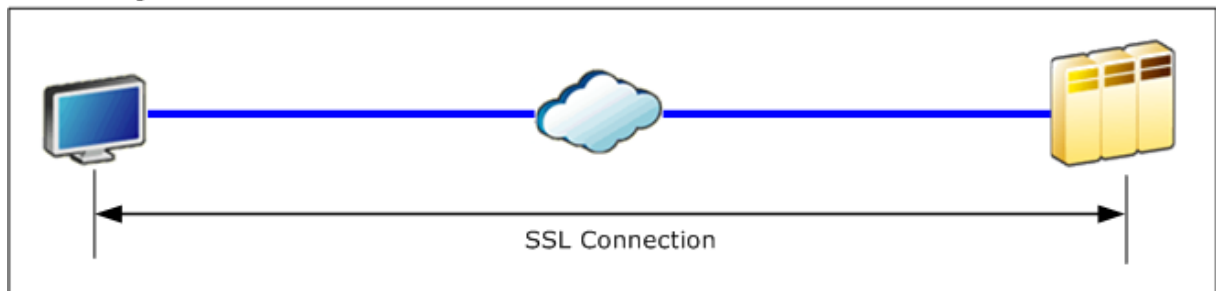
### **Hinweis**

Die SSL-Komprimierung erfordert eine sichere Peering-Verbindung (Signalisierung) zwischen den beiden Appliances an den Enden der beschleunigten Verbindung.

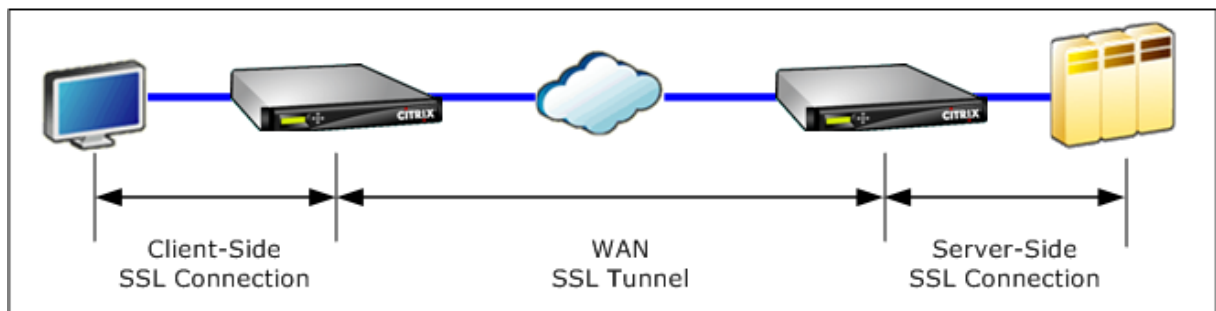
Die Verschlüsselung wird von Ende zu Ende aufrechterhalten, indem die Verbindung in drei verschlüsselte Segmente aufgeteilt wird: Client-zu-clientseitige Appliance, clientseitige Appliance zu serverseitige Appliance und serverseitige Appliance zu Server.



### Ordinary SSL Connection



### Accelerated SSL Connection



Achtung: SSL-Komprimierung entschlüsselt den verschlüsselten Datenstrom und, sofern nicht die Option Benutzerdatenverschlüsselung verwendet wird, behalten die Komprimierungsprotokolle beider Beschleunigungseinheiten Klartextdatensätze der entschlüsselten Daten bei. Stellen Sie sicher, dass Ihre Bereitstellung und Einstellungen mit den Sicherheitsrichtlinien Ihrer Organisation übereinstimmen. Citrix empfiehlt, dass Sie die Verschlüsselung des Komprimierungsverlaufs auf jeder Einheit aktivieren, wenn Sie die sichere Peering-Signalverbindung konfigurieren, die für die SSL-Beschleunigung erforderlich ist.

#### Hinweis

- Wenn Sie die SSL-Komprimierung aktivieren, hört die Appliance auf, eine Komprimierung mit anderen Appliances durchzuführen, mit denen sie keine sichere Peer-Beziehung hat (ob Citrix SD-WAN WANOP oder Citrix SD-WAN WANOP Plug-in). Diese Funktion eignet sich daher am besten für Netzwerke, in denen alle Appliances für die SSL-Komprimierung konfiguriert sind.
- Wenn die SSL-Komprimierung aktiviert ist, müssen Sie bei jedem Neustart der Appliance das Kennwort für den Schlüsselspeicher manuell eingeben.

## Funktionsweise der SSL-Komprimierung

April 19, 2021

Die SSL-Komprimierung hat Zugriff auf die Klartextdaten der Verbindung, da die serverseitige Appliance als *Sicherheitsdelegat* der Endpunktserver fungiert. Dieses Verhalten ist möglich, da die serverseitige Appliance mit Kopien der Sicherheitsanmeldeinformationen der Server (private Schlüssel und Zertifikate) konfiguriert ist, so dass sie im Namen des Servers handeln kann. Für den Client entspricht dieses Verhalten der direkten Kommunikation mit dem Endpunktserver.

Da die Appliance als Sicherheitsdelegat des Servers arbeitet, befindet sich die meiste Konfiguration auf der serverseitigen Appliance. Die clientseitige Appliance (oder Plug-in) fungiert als Satellit der serverseitigen Appliance und erfordert keine Konfiguration pro Server.

Die serverseitigen und clientseitigen Appliances teilen sich über eine *SSL-Signalverbindung* den Sitzungsstatus. Alle beschleunigten Verbindungen zwischen den beiden Appliances werden über *SSL-Datenverbindungen* gesendet, unabhängig davon, ob die ursprünglichen Verbindungen verschlüsselt wurden oder nicht.

Hinweis: Die SSL-Komprimierung verschlüsselt nicht unbedingt den gesamten Linkverkehr. Der ursprünglich verschlüsselte Datenverkehr bleibt verschlüsselt, der unverschlüsselte Datenverkehr wird jedoch nicht immer verschlüsselt. Die Appliances versuchen nicht, nicht beschleunigten Datenverkehr zu verschlüsseln. Da es keine absolute Garantie dafür gibt, dass eine bestimmte Verbindung beschleunigt wird (verschiedene Ereignisse verhindern eine Beschleunigung), gibt es keine Garantie, dass die Appliances eine bestimmte unverschlüsselte Verbindung verschlüsseln.

Die SSL-Komprimierung funktioniert in einem von zwei Modi: transparenter Proxy oder geteilter Proxy. Diese beiden Modi unterstützen geringfügig unterschiedliche SSL-Funktionen. Sie wählen den Modus aus, der die Funktionen bereitstellt, die eine bestimmte Anwendung benötigt.

**Welcher SSL-Proxy-Modus verwendet werden soll —Verwenden** Sie den transparenten SSL-Proxy-Modus *nur*, wenn Sie eine echte Client-Authentifizierung benötigen (d. h. eine Authentifizierung, die den einzelnen Endpunkt-Client korrekt identifiziert) *und* Sie keine Diffie-Hellman, Temp RSA, TLS-Sitzungstickets, SSL-Version 2 oder Sitzungsneuverhandlung. Verwenden Sie SSL-geteilten Proxy für alle anderen Bereitstellungen.

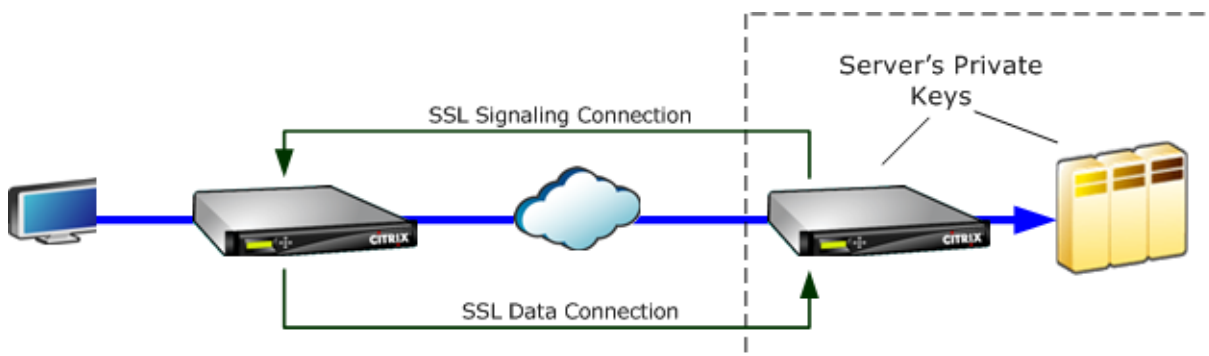
## Transparenter SSL-Proxy

Im *transparenten SSL-Proxy-Modus* (nicht zu verwechseln mit dem transparenten Modus des Citrix SD-WAN WANOP-Plug-ins) maskiert sich die serverseitige Appliance als Server. Die Anmeldeinformationen des Servers (Zertifikatschlüsselpaar) werden auf der serverseitigen Appliance installiert, sodass sie im Auftrag des Servers handeln kann. Die serverseitige Appliance konfiguriert dann die clientseitige Appliance, um das Client-Ende der Verbindung zu verarbeiten. Die Anmeldeinformationen des Servers sind nicht auf der clientseitigen Appliance installiert.

Echte Clientauthentifizierung wird in diesem Modus unterstützt, aber Temp RSA und Diffie-Hellman nicht. Der transparente SSL-Proxymodus eignet sich für Anwendungen, die eine Clientauthen-

tifizierung erfordern, jedoch nur, wenn keine der folgenden Funktionen erforderlich ist: Diffie-Hellman, Temp RSA, TLS-Sitzungstickets, SSL-Version 2. Außerdem darf keine Neuverhandlung der Sitzung durchgeführt werden, oder die Verbindung wird beendet.

Auf der clientseitigen Appliance ist keine Konfiguration erforderlich (außer der Konfiguration einer sicheren Peering-Beziehung mit der serverseitigen Appliance), und es ist keine Konfiguration auf dem Client erforderlich, die die Verbindung genau so behandelt, als ob sie direkt mit dem Server kommuniziert.



## SSL-geteilter Proxy

Der *SSL-geteilte Proxy-Modus* wird in den meisten Fällen bevorzugt, da er Temp RSA und Diffie-Hellman unterstützt, die viele Anwendungen benötigen. Im SSL-geteilten Proxymodus maskiert die serverseitige Appliance als Server für den Client und als Client für den Server. Sie installieren Serveranmeldeinformationen (ein Zertifikatschlüsselpaar) auf der serverseitigen Appliance, damit sie im Auftrag des Servers handeln kann.

Der geteilte Proxymodus unterstützt auch die Proxy-Clientauthentifizierung, wenn Sie optionale Clientanmeldeinformationen installieren, die der Endpunktserveranwendung angezeigt werden, wenn sie die Clientauthentifizierung anfordert. Diese Client-Anmeldeinformationen werden anstelle der tatsächlichen Anmeldeinformationen des Endpunkt-Clients angezeigt. (Verwenden Sie transparenten Proxy, wenn die Endpunkt-Client-Anmeldeinformationen für die Anwendung erforderlich sind.)

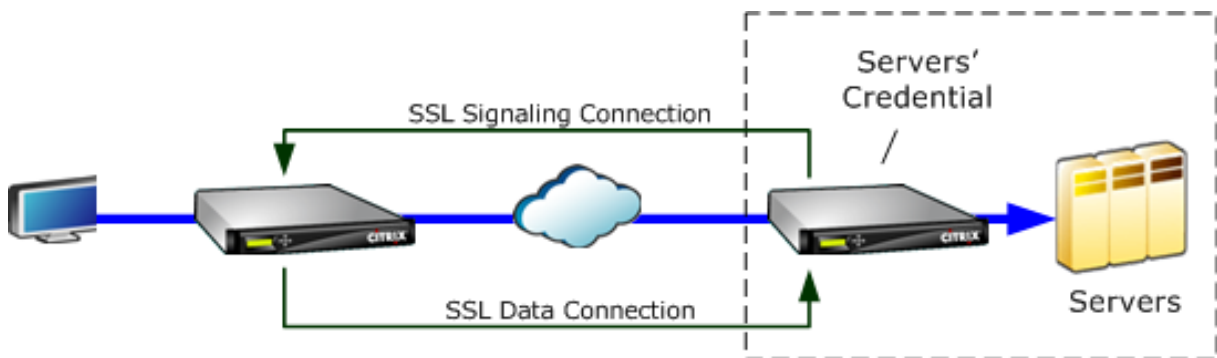
Da die echte Clientauthentifizierung in diesem Modus nicht unterstützt wird, kann der Server den tatsächlichen Endpunktclient nicht authentifizieren. Wenn die serverseitige Appliance nicht mit Clientanmeldeinformationen konfiguriert ist, schlagen alle Versuche der serverseitigen Anwendung bei der Clientauthentifizierung fehl. Wenn die serverseitige Appliance mit Clientanmeldeinformationen konfiguriert ist, werden alle Anforderungen für die Clientauthentifizierung mit diesen Anmeldeinformationen beantwortet, unabhängig von der Identität des tatsächlichen Clients.

Auf der clientseitigen Appliance ist keine Konfiguration erforderlich (außer der Konfiguration einer sicheren Peering-Beziehung mit der serverseitigen Appliance), und es ist keine Konfiguration auf dem

Client erforderlich, wodurch die Verbindung so behandelt wird, als ob sie direkt mit dem Server kommuniziert. Die Serveranmeldeinformationen auf der serverseitigen Appliance sind nicht auf der clientseitigen Appliance installiert.

Zur Unterstützung mehrerer Server können mehrere private Zertifikatschlüsselpaare auf der Appliance installiert werden, eines pro SSL-Profil. Spezielle SSL-Regeln in den Service-Klassendefinitionen stimmen Server mit SSL-Profilen und somit SSL-Profile mit Anmeldeinformationen überein.

Im SSL-geteilten Proxy-Modus müssen die Zertifizierungsstellenzertifikate und Zertifikatschlüsselpaare und Zertifizierungsstellenzertifikate tatsächlich nicht mit denen der Server übereinstimmen. Aufgrund der Art eines geteilten Proxys kann die serverseitige Appliance Anmeldeinformationen verwenden, die für die Clientanwendung akzeptabel sind (gültige Anmeldeinformationen, die von einer vertrauenswürdigen Behörde ausgestellt werden). Beachten Sie, dass Webbrowser bei HTTPS-Verbindungen eine Warnung ausgeben, wenn der allgemeine Name nicht mit dem Domännennamen in der URL übereinstimmt. Im Allgemeinen ist die Verwendung von Kopien der Anmeldeinformationen des Servers die problemlose Option.



## Konfigurieren der SSL-Komprimierung

April 19, 2021

Die Citrix SD-WAN WO SSL-Komprimierungsfunktion ermöglicht die Multisession-Komprimierung von SSL-Verbindungen (z. B. HTTPS-Verkehr) und bietet ein Komprimierungsverhältnis von bis zu 10.000:1. Weitere Informationen finden Sie unter [SSL-Komprimierung](#).

Damit die SSL-Komprimierung funktioniert, benötigt die Citrix SD-WAN WANOP-Appliance Zertifikate vom Server oder vom Client. Zur Unterstützung mehrerer Server können mehrere private Schlüssel auf der Appliance installiert werden, einer pro SSL-Profil. Spezielle SSL-Regeln in den Service-Klassendefinitionen stimmen Server mit SSL-Profilen und somit SSL-Profile mit privaten Schlüsseln überein.

SSL-Komprimierung funktioniert im geteilten Proxy oder transparenten Proxy-Modus, Sie können den

Modus nach Ihren Anforderungen wählen. Weitere Informationen finden Sie unter [Funktionsweise der SSL-Komprimierung](#).

#### Hinweis

Der transparente Proxy-Modus wird derzeit nicht unterstützt.

Um einen sicheren Zugriff mit SSL-Tunnel zu ermöglichen, wird das neueste SSL-Protokoll TLS 1.2 im SSL-Proxy verwendet. Sie können nur das TLS1.2-Protokoll verwenden oder die Protokolle TLS1.0, TLS1.1 und TLS1.2 verwenden.

#### Hinweis

SSL-Protokolle SSL v3 und SSL v2 werden nicht mehr unterstützt.

### So konfigurieren Sie die SSL-Komprimierung:

1. Erwerben Sie Kopien des CA-Zertifikats und des privaten Zertifikatschlüsselpaars Ihres Servers, und installieren Sie diese auf der serverseitigen Appliance. Diese Anmeldeinformationen sind wahrscheinlich anwendungsspezifisch. Das heißt, ein Server hat möglicherweise andere Anmeldeinformationen für einen Apache-Webserver als für einen Exchange Server, auf dem RPC über HTTPS ausgeführt wird.

2. Sie können ein gesplittetes Proxy-SSL-Profil oder ein transparentes Proxy-SSL-Profil erstellen.

Weitere Informationen zum Konfigurieren von Split Proxy SSL-Profilen finden Sie unter **Konfigurieren eines Split Proxy SSL-Profiles** unten.

Informationen zum Konfigurieren des transparenten Proxy-SSL-Profiles finden Sie im Abschnitt **Configuring Transparent Proxy SSL-Profile** weiter unten.

#### Hinweis

Transparentes Proxy-SSL-Profil wird derzeit nicht unterstützt.

3. Schließen Sie das SSL-Profil an eine Serviceklasse auf der serverseitigen Appliance an. Dies kann entweder durch Erstellen einer neuen Service-Klasse auf der Grundlage der Server-IP oder durch Ändern einer vorhandenen Service-Klasse erfolgen.

Weitere Informationen finden Sie unter **Erstellen oder Ändern der Service-Klasse** unten.

4. Festlegen von Serviceklassen auf der clientseitigen Appliance. SSL-Datenverkehr wird nur komprimiert, wenn er in eine Serviceklasse auf der clientseitigen Appliance fällt, die Beschleunigung und Komprimierung ermöglicht. Dies kann eine gewöhnliche Service-Class-Regel sein, keine SSL-Regel (nur die serverseitige Appliance benötigt SSL-Regeln), muss jedoch Beschleunigung und Komprimierung aktivieren. Der Datenverkehr fällt in eine vorhandene Dienstklasse, z. B. HTTPS oder Anderer TCP-Datenverkehr. Wenn die Richtlinie dieser Klasse Beschleunigung und Komprimierung ermöglicht, ist keine zusätzliche Konfiguration erforderlich.

- Überprüfen Sie den Betrieb der Regel. Senden Sie Datenverkehr, der SSL-Beschleunigung über die Appliances erhalten soll. Auf der serverseitigen Appliance sollte auf der Registerkarte Überwachung: Optimierung: Verbindungen: Beschleunigte Verbindungen die Spalte Dienstklasse mit der Dienstklasse übereinstimmen, die Sie für die sichere Beschleunigung eingerichtet haben, und die Spalte SSL-Proxy sollte True für entsprechende Verbindungen auflisten.

## Konfigurieren eines geteilten Proxy-SSL-Profiles

### So konfigurieren Sie ein geteiltes Proxy-SSL-Profil:

- Navigieren Sie in der serverseitigen Citrix SD-WAN WO-Appliance zu **Configuration > Secure Acceleration > SSL-Profil** und klicken Sie auf **Add Profile**.

#### Hinweis

Sie können entweder manuell ein SSL-Profil hinzufügen oder ein SSL-Profil importieren, das auf Ihrem lokalen Computer gespeichert ist.

- Geben Sie im Feld **Profilname** einen Namen für das SSL-Profil ein, und wählen Sie **Profil aktiviert** aus.
- Wenn Ihr SSL-Server mehr als einen virtuellen Hostnamen verwendet, geben Sie im Feld **Virtueller Hostname** den Namen des virtuellen Zielhosts ein. Dies ist der Hostname, der in den Anmeldeinformationen des Servers aufgeführt ist.

#### Hinweis

Um mehrere virtuelle Hosts zu unterstützen, erstellen Sie für jeden Hostnamen ein separates SSL-Profil.

- Wählen Sie Proxytyp **teilen**.
- Behalten Sie im Feld **Zertifikatüberprüfung** den Standardwert (Signatur/Ablauf) bei, sofern Ihre Richtlinien nichts anderes vorschreiben.

## 6. Serverseitige Proxykonfiguration ausführen:

Wählen Sie im Feld **Verifizierungsspeicher** eine vorhandene Serverzertifizierungsstelle aus, oder klicken Sie auf **+**, um eine Serverzertifizierungsstelle hochzuladen.

Wählen Sie **Authentifizierung erforderlich**, und wählen Sie im Feld **Zertifikat/Privatschlüssel** ein Zertifikatschlüsselpaar aus, oder klicken Sie auf **+**, um ein Zertifikatschlüsselpaar hochzuladen.

Wählen Sie im Feld **Protokollversion** die Protokolle aus, die Ihr Server akzeptiert.

**Hinweis**

Citrix SD-WAN WO unterstützt nur eine Kombination aus **TLS1.0, TLS1.1 oder TLS1.2** oder **TLS1.2**\*\*. SSL-Protokolle SSLv3 und SSLv2 werden nicht unterstützt.

Bearbeiten Sie bei Bedarf die Zeichenfolge **Cipher Specification** unter Verwendung der OpenSSL-Syntax.

Wählen Sie bei Bedarf den Typ der Neuverhandlung aus der Dropdown-Liste **Neuverhandlungstyp** aus, um die clientseitige SSL-Sitzungsneuverhandlung zuzulassen.

## 7. Clientseitige Proxy-Konfiguration ausführen:

Behalten Sie im Feld **Zertifikat/Privatschlüssel** den Standardwert bei.

Wählen Sie **Zertifikatkette erstellen**, damit die serverseitige Appliance die SSL-Zertifikatkette erstellen kann.

Wählen Sie ggf. einen Zertifizierungsstellenspeicher aus, der als Zertifikatkettenspeicher verwendet werden soll, oder laden Sie diesen hoch.

Wählen Sie im Feld **Protokollversion** die Protokollversionen aus, die Sie auf der Clientseite unterstützen möchten.

**Hinweis**

Citrix SD-WAN WO unterstützt nur eine Kombination aus **TLS1.0, TLS1.1 oder TLS1.2** oder

**TLS1.2**\*\*\* SSL-Protokolle SSLv3 und SSLv2 werden nicht unterstützt.

Bearbeiten Sie ggf. die clientseitige Verschlüsselungsspezifikation.

Wählen Sie bei Bedarf den Typ der Neuverhandlung aus der Dropdown-Liste **Neuverhandlungstyp** aus, um die clientseitige SSL-Sitzungsneuverhandlung zuzulassen.

Client-Side Proxy Configuration

Certificate/Private Key\*  
split

☐ Disable Session Re-use  
☒ Build Certificate Chain

Certificate Chain Store

Protocol Version\*  
TLS 1.0, TLS1.1 or TLS 1.2

Cipher Specification\*  
!ADH:HIGH:MEDIUM:@STRENGTH

Renegotiation Type\*  
Old Style Renegotiation Disabled

8. Klicken Sie auf **Erstellen**.

## Konfigurieren eines transparenten Proxy-SSL-Profiles

### So konfigurieren Sie ein transparentes Proxy-SSL-Profil:

1. Navigieren Sie in der serverseitigen Citrix SD-WAN WO-Appliance zu **Configuration > Secure Acceleration > SSL-Profil** und klicken Sie auf **Add Profile**.

#### Hinweis

Sie können entweder manuell ein SSL-Profil hinzufügen oder ein SSL-Profil importieren, das auf Ihrem lokalen Computer gespeichert ist.

2. Geben Sie im Feld **Profilname** einen Namen für das SSL-Profil ein, und wählen Sie **Profil aktiviert** aus.
3. Wenn Ihr SSL-Server mehr als einen virtuellen Hostnamen verwendet, geben Sie im Feld **Virtueller Hostname** den Namen des virtuellen Zielhosts ein. Dies ist der Hostname, der in den Anmeldeinformationen des Servers aufgeführt ist.

#### Hinweis

Um mehrere virtuelle Hosts zu unterstützen, erstellen Sie für jeden Hostnamen ein separates SSL-Profil.



4. Wählen Sie **Transparenter** Proxytyp.
5. Wählen Sie im Feld **Privater Schlüssel des SSL-Servers** den privaten Schlüssel aus dem Dropdownmenü aus, oder klicken Sie auf +, um einen neuen privaten Schlüssel hochzuladen.
6. Klicken Sie auf **Erstellen**.

## Erstellen oder Ändern der Serviceklasse

**So erstellen oder ändern Sie die Serviceklasse und fügen Sie das SSL-Profil hinzu:**

1. Navigieren Sie im Webinterface der Citrix SD-WAN WO Appliance zu **Configuration > Optimization Rules > Service Classes**, und klicken Sie auf **Hinzufügen**. Um eine vorhandene Serviceklasse zu bearbeiten, wählen Sie die entsprechende Serviceklasse aus, und klicken Sie auf **Bearbeiten**.
2. Geben Sie im Feld Name einen Namen für die neue Serviceklasse ein (z.B. Accelerated HTTPS).
3. Aktivieren Sie die Komprimierung, indem Sie die Beschleunigungsrichtlinie auf **Datenträger, Arbeitsspeicher** oder **Flusssteuerung** festlegen.
4. Klicken Sie im Abschnitt **Filterregeln** auf **Hinzufügen**.
5. Geben Sie im Feld **Ziel-IP-Adresse** die IP-Adresse des Servers ein (z. B. 172.16.0.1 oder äquivalent 172.16.0.1/32).
6. Legen Sie im Feld **Richtung** die Regel auf Unidirektional fest. SSL-Profile werden deaktiviert, wenn Bidirektional angegeben ist.
7. Wählen Sie im Abschnitt **SSL-Profil** das von Ihnen erstellte SSL-Profil aus, und verschieben Sie es in den Abschnitt **Konfiguriert**.
8. Klicken Sie auf **Erstellen**, um die Regel zu erstellen.
9. Klicken Sie auf **Erstellen**, um die Serviceklasse zu erstellen.

## Aktualisierter CLI-Befehl

Citrix SD-WAN WO 9.3 unterstützt das neueste TLS1.2 SSL-Protokoll. Sie können nur das TLS1.2-Protokoll oder eine beliebige Version von TLS-Protokollen verwenden. SSL-Protokolle SSL v3 und SSL v2 und transparente Proxy-SSL-Profilen werden nicht unterstützt. Die CLI-Befehle **add ssl-profile** und **set ssl-profile** werden aktualisiert, um diese Änderungen widerzuspiegeln.

### add ssl-profile:

```

1  *--name "profile-name"*
2
3  *\[--state {
4    enable, disable }
5    \]*
6
7  *--proxy-type split*
8
9  *\[--virtual-hostname "hostname"\]*
10
11 *--cert-key "cert-key-pair-name"*
12
13 *\[--build-cert-chain {
14   enable, disable }
15   \]*
16
17 *\[--cert-chain-store {
18   use-all-configured-CA-stores, "store-name" }
19   \]*
20
21 *\[--cert-verification {
22   none, Signature/Expiration, Signature/Expiration/*
23
24 *Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
25   \]*
26
27 *\[--verification-store {
28   use-all-configured-CA-stores, "store-name" }
29   \]*
30
31 *\[--server-side-protocol {
32   TLS-1.2, TLS-version-any }
33   \]*
34
35 *\[--server-side-ciphers "ciphers"\]*
36
37 *\[--server-side-authentication {
38   enable, disable }
39   \]*
40
41 *\[--server-side-cert-key "cert-key-pair-name"\]*
42
43 *\[--server-side-build-cert-chain {

```

```
44  enable, disable }
45  \]*
46
47  *\[--server-side-renegotiation {
48    disable-old-style, enable-old-style, new-style,*
49
50  *compatible }
51  \]*
52
53  *\[--client-side-protocol-version {
54    TLS-1.2, TLS-version-any }
55  \]*
56
57  *\[--client-side-ciphers "ciphers"\]*
58
59  *\[--client-side-renegotiation {
60    disable-old-style, enable-old-style, new-style,*
61
62  *compatible }
63  \]*
```

**set ssl-profile:**

```
1  *--name "profile-name" \[--state {
2    enable, disable }
3  \]*
4
5  *\[--proxy-type split\]*
6
7  *\[--virtual-hostname "hostname"\]*
8
9  *\[--cert-key "cert-key-pair-name"\]*
10
11 *\[--build-cert-chain {
12   enable, disable }
13 \]*
14
15 *\[--cert-chain-store {
16   use-all-configured-CA-stores, "store-name" }
17 \]*
18
19 *\[--cert-verification {
20   none, Signature/Expiration, Signature/Expiration/*
21
22 *Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
23 \]*
24
25 *\[--verification-store {
26   use-all-configured-CA-stores, "store-name" }
27 \]*
28
29 *\[--server-side-protocol {
30   TLS-1.2, TLS-version-any }
```

```
31  \]*
32
33  *\[ -server-side-ciphers "ciphers" \]*
34
35  *\[ -server-side-authentication {
36    enable, disable }
37  \]*
38
39  *\[ -server-side-cert-key "cert-key-pair-name" \]*
40
41  *\[ -server-side-build-cert-chain {
42    enable, disable }
43  \]*
44
45  *\[ -server-side-renegotiation {
46    disable-old-style, enable-old-style, new-style,*
47
48  *compatible }
49  \]*
50
51  *\[ -client-side-protocol-version {
52    TLS-1.2, TLS-version-any }
53  \]*
54
55  *\[ -client-side-ciphers "ciphers" \]*
56
57  *\[ -client-side-renegotiation {
58    disable-old-style, enable-old-style, new-style,*
59
60  *compatible }
61  \]*
```

## SSL-Komprimierung mit Citrix SD-WAN WANOP-Plug-in

April 19, 2021

Das Citrix SD-WAN WANOP Plug-in wird immer als clientseitige Einheit verwendet und erfordert daher keine zusätzliche SSL-Konfiguration außer der Installation von Anmeldeinformationen für die SSL-Signalverbindung (Secure Peering). Der Hauptunterschied zwischen der SSL-Komprimierung des Plug-ins und der Appliance besteht darin, dass das Plug-In die Benutzerdaten im datenträgerbasierten Komprimierungsverlauf nicht verschlüsseln kann.

**Achtung:** Da der festplattenbasierte Komprimierungsverlauf des Plug-ins nicht verschlüsselt ist, wird ein Klartextdatensatz potenziell sensibler und kurzlebheller verschlüsselter Kommunikation beibehalten

. Dieser Mangel an Verschlüsselung ist potenziell gefährlich auf Computern, für die der physische Zugriff nicht kontrolliert wird. Daher empfiehlt Citrix die folgenden Best Practices:

- Verwenden Sie keine **Zertifikatvalidierung: Keine** auf Ihren Appliances. (Beachten Sie, dass die Appliance in diesem Fall die Komprimierung mit Plug-Ins verweigert, die über keine entsprechenden Zertifikate verfügen.)
- Installieren Sie Zertifikate nur auf Systemen, die überprüft werden können, um die Anforderungen Ihrer Organisation für physische oder Datensicherheit zu erfüllen (z. B. Notebooks, die Vollfestplattenverschlüsselung verwenden).

Das Citrix SD-WAN WANOP Plug-in unterstützt sowohl SSL Split-Proxy als auch SSL-transparenten Proxy. Das Plug-in wird ohne Zertifikatschlüsselpaare für die SSL-Signalverbindung ausgeliefert. Falls gewünscht, können dieselben Anmeldeinformationen von allen Plug-Ins verwendet werden, oder jedes Plug-In kann seine eigenen Anmeldeinformationen haben.

Das Plug-In versucht keine SSL-Komprimierung, es sei denn, die Anmeldeinformationen wurden installiert.

Das Plug-In erbt seine Kryptolizenz von der Appliance.

## RPC über HTTP

April 19, 2021

Microsoft Exchange Server ist einer der gängigen E-Mail-Server, die in verschiedenen Organisationen verwendet werden. Aufgrund der jüngsten Verbesserungen in Microsoft Exchange Server können Sie eine sichere Verbindung mit diesem Server über das Internet herstellen. Abhängig von der verfügbaren Bandbreite kann es zu Latenz in der E-Mail kommen, die an den Outlook-Client gesendet wird. Zusätzlich zum MAPI-Protokoll unterstützt die Citrix SD-WAN WANOP-Appliance Remote Procedure Call over HTTPS (RPC über HTTPS), um den Microsoft Exchange-Datenverkehr zu optimieren. Dieses Feature wird auch als Outlook Anywhere bezeichnet.

RPC über HTTPS ist kein neues Protokoll, aber ab Microsoft Exchange 2013 ersetzt MAPI als Standardprotokoll. Der Hauptvorteil von RPC über HTTPS besteht darin, dass Clients eine sichere Verbindung zum Mailserver über das Internet herstellen können.

Wenn Sie RPC über HTTPS verwenden, muss der Microsoft Exchange-Server ein digitales Zertifikat und einen privaten Schlüssel verwenden, um sich am Outlook-Client zu authentifizieren. Die Kommunikation zwischen Client und Server verwendet HTTPS als Transportprotokoll.

Auf der Citrix SD-WAN WANOP-Appliance wird RPC über HTTPS für die folgenden Versionen von Microsoft Outlook und Exchange Server unterstützt:

- Microsoft Outlook
  - Microsoft Outlook 2007

- Microsoft Outlook 2010
- Microsoft Outlook 2013
- Microsoft Exchange Server
  - Microsoft Exchange Server 2007
  - Microsoft Exchange Server 2010
  - Microsoft Exchange Server 2013

Von diesen unterstützen alle Versionen außer Microsoft Exchange Server 2013 MAPI (über TCP) sowie RPC über HTTPS. Microsoft Exchange Server 2013 erzwingt jedoch Verbindungen, unabhängig von der verwendeten Microsoft Outlook-Version RPC über HTTPS zu verwenden, um eine Verbindung mit dem Exchange-Server herzustellen.

## Konfigurieren von RPC über HTTPS

Standardmäßig ist die Funktion RPC über HTTPS auf der Appliance aktiviert. Um die Appliance jedoch so zu konfigurieren, dass RPC über HTTPS beschleunigt wird, müssen Sie die folgenden zusätzlichen Aufgaben ausführen:

- Konfigurieren Sie verschlüsseltes MAPI.
- Konfigurieren Sie ein SSL-Profil mit einem Serverzertifikat.
- Erstellen Sie eine RPC über HTTPS-Dienstklasse und binden Sie das SSL-Profil daran.

## Verschlüsseltes MAPI konfigurieren

### Hinweis

Überspringen Sie diesen Abschnitt, wenn Sie bereits eine verschlüsselte MAPI-Beschleunigung auf der Appliance konfiguriert haben.

Microsoft Outlook verwendet MAPI-Verbindungen (Messaging Application Programming Interface) zwischen Outlook-Clients und dem Microsoft Exchange-Server. MAPI-Verbindungen verwenden RPCs, die von einer HTTP-Verbindung gekapselt sind. Bevor Sie RPC über HTTPS auf einer Citrix SD-WAN WANOP-Appliance konfigurieren, müssen Sie daher verschlüsseltes MAPI auf der Appliance konfigurieren.

### Voraussetzungen:

Bevor Sie verschlüsselte MAPI konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die Option Secure Peer sollte sowohl auf dem Client als auch auf der serverseitigen Appliance auf True festgelegt sein. Informationen zum Konfigurieren eines sicheren Partners finden Sie unter [Sicheres Peering](#).
- Die auf der serverseitigen Appliance konfigurierte DNS-IP-Adresse muss erreichbar sein.
- Die Datacenter-Appliance muss erfolgreich der Domäne beitreten.
- Ein Delegatbenutzer muss der Appliance im Datenzentrum hinzugefügt werden und sein Status sollte "Erfolg" sein.

Weitere Informationen finden Sie unter [Konfigurieren einer Citrix SD-WAN WANOP-Appliance zur Optimierung des sicheren Windows-Datenverkehrs](#).

### **Konfigurieren eines SSL-Profiles mit einem Serverzertifikat**

Die HTTPS-Verbindung, die die MAPI-Verbindung kapselt, wird durch SSL gesichert. Daher erfordert RPC über HTTPS eine Konnektivität über TCP-Port 443. Dieser Port ist HTTPS zugewiesen, die Web-Server-Administratoren in der Regel in der Firewall-Anwendung offen halten. Die Verwendung von SSL-geschützter Kommunikation hilft RPC über HTTPS, die Sicherheit aller Kommunikation aufrechtzuerhalten.

Um die RPC-über-HTTPS-Beschleunigung zu aktivieren, müssen Sie ein Serverzertifikat auf der Appliance installieren. Mit diesem Serverzertifikat können Sie ein SSL-Profil konfigurieren, das RPC über HTTPS für die sichere Kommunikation verwendet. Informationen zum Konfigurieren eines SSL-Profiles mit einem Exchange-Serverzertifikat finden Sie unter Installieren von Server- und Clientzertifikaten.

#### **Hinweis**

Sie müssen ein SSL-Profil nur auf der Datacenter-Appliance konfigurieren.

### **Erstellen Sie eine RPC-über-HTTPS-Dienstklasse und binden Sie das SSL-Profil daran**

Um die RPC-über-HTTP-Verbindungen zu optimieren, müssen Sie eine Dienstklasse erstellen, die HTTPS und alle MAPI-Anwendungen auflistet. Sie müssen die IP-Adresse des Microsoft Exchange-Servers als Ziel-IP-Adresse für diese Dienstklasse angeben und dann das von Ihnen erstellte SSL-Profil an diese Dienstklasse binden. Das Binden des Profils an die Dienstklasse stellt sicher, dass die Kommunikation zwischen dem Outlook-Client und dem Microsoft Exchange-Server mithilfe dieses Profils gesichert ist.

#### **Hinweis**

Sie müssen ein SSL-Profil nur auf der Datacenter-Appliance konfigurieren und an die Dienstklasse binden.

## Überprüfen beschleunigter RPC über HTTPS-Verbindungen

Nachdem Sie RPC über HTTPS auf der Appliance konfiguriert haben, können Sie auf der Seite Überwachung für MAPI überprüfen, ob die Appliance die RPC-über-HTTPS-Verbindung beschleunigt. Die beschleunigten RPC-über-HTTPS-Verbindungen werden auf der Registerkarte Beschleunigte MAPI-Sitzungen aufgeführt.

### Hinweis

Sie müssen RPC über HTTPS auf Ihren clientseitigen Appliances sowie auf Ihren serverseitigen Citrix SD-WAN WANOP-Appliances konfigurieren, um den RPC über HTTPS-Verbindungen zu beschleunigen.

So überprüfen Sie, ob RPC über HTTPS-Verbindungen beschleunigt werden

1. Navigieren Sie zu **Überwachung > Optimierung > Outlook (MAPI)**.
2. Überprüfen Sie auf der Registerkarte **Beschleunigte MAPI-Sitzungen**, ob RPC über HTTPS-Verbindungen beschleunigt werden.

TCP Connection Count	Client	Server	Bytes Sent	Bytes Received	User Name	Encrypted	Service Class
213	192.168.10.33	192.168.20.5	744.26 MB	2.70 GB	Administrator	True	HTTPS eMAPI

### Hinweis

Die Anwendung hat mögliche Werte für: HTTPS eAPI, HTTP eAPI, HTTPS MAPI und HTTP MAPI.

## TCP-Durchflusskontrollbeschleunigung

April 19, 2021

Gewöhnliche WANs haben eine sehr schlechte Reaktionsfähigkeit bei hoher Link-Auslastung und bei langen Entfernungen. Eine weit verbreitete Faustregel für gewöhnliche, nicht beschleunigte WAN-Verbindungen lautet: Sobald die Link-Auslastung 40% erreicht, ist es an der Zeit, mehr Bandbreite hinzuzufügen, da Leistung und Zuverlässigkeit bis zu dem Punkt verschlechtert sind, an dem die Verbindung weitgehend unbrauchbar ist. Interaktive Leistung leidet, was es den Menschen



schwer macht, Arbeit zu erledigen, und Verbindungen oft Timeout. Beschleunigte Links haben dieses Problem nicht. Eine Verbindung mit 95% Auslastung ist immer noch perfekt nutzbar.

Citrix SD-WAN WANOP-Appliances werden zu virtuellen Gateways, die den TCP-Verkehr auf der WAN-Verbindung steuern. Gewöhnliche TCP wird pro Verbindung von den Endpunktgeräten gesteuert. Eine optimale Steuerung des Link-Datenverkehrs ist schwierig, da weder die Endpunktgeräte noch einzelne Verbindungen über die Verbindungsgeschwindigkeit oder die Menge des konkurrierenden Datenverkehrs Bescheid wissen. Ein Gateway hingegen ist in einer idealen Position, um den Linkverkehr zu überwachen und zu steuern. Gewöhnliche Gateways verschwenden diese Chance, da sie die Flow-Kontrolle, die TCP fehlt, nicht bereitstellen können. Die Citrix SD-WAN WANOP-Technologie fügt die Intelligenz hinzu, die in den Netzwerkgeräten und den TCP-Verbindungen fehlt. Das Ergebnis ist eine stark verbesserte WAN-Leistung, auch unter rauen Bedingungen wie hohen Verlusten oder extremen Entfernungen.

Die Citrix SD-WAN WANOP-Flow-Steuerung ist verlustfrei und transparent und implementiert ein breites Spektrum von Geschwindigkeitsoptimierungen. Aufgrund der automatischen Erkennung und der automatischen Konfiguration ist keine Konfiguration erforderlich. Möglicherweise müssen Sie Ihre Firewalls jedoch optimieren, wenn sie die TCP-Optionen blockieren, die von den Beschleunigungsalgorithmen verwendet werden.

## **Verlustfreie und transparente Durchflussregelung**

April 19, 2021

Die Beschleunigung funktioniert auf jeder TCP-Verbindung, die über zwei Appliances (eine am sendenden Standort und eine am empfangenden Standort) oder eine Citrix SD-WAN WANOP-Appliance und ein Citrix SD-WAN WANOP Plug-in läuft. Obwohl die obige Abbildung ein Netzwerk von zwei Appliances zeigt, kann jede Appliance die Verbindungen zwischen einer beliebigen Anzahl von anderen mit der Appliance ausgestatteten Standorten gleichzeitig beschleunigen. Auf diese Weise kann eine einzelne Appliance pro Standort anstelle von zwei pro Link verwendet werden.

Wie jedes Gateway verwendet die Citrix SD-WAN WANOP-Appliance Pakete auf dem Link. Im Gegensatz zu gewöhnlichen Gateways wird jedoch für jedes Linksegment eine transparente, verlustfreie Flusssteuerung auferlegt, einschließlich:

- Das LAN-Segment zwischen dem Absender und der sendenden Appliance
- Das WAN-Segment zwischen den sendenden und empfangenden Einheiten
- Das LAN-Segment zwischen der empfangenden Appliance und dem Empfänger

Die Durchflusssteuerung kann für jedes dieser drei Segmente unabhängig verwaltet werden. Die Segmente sind teilweise entkoppelt, so dass jeder seine Geschwindigkeit unabhängig gesteuert werden

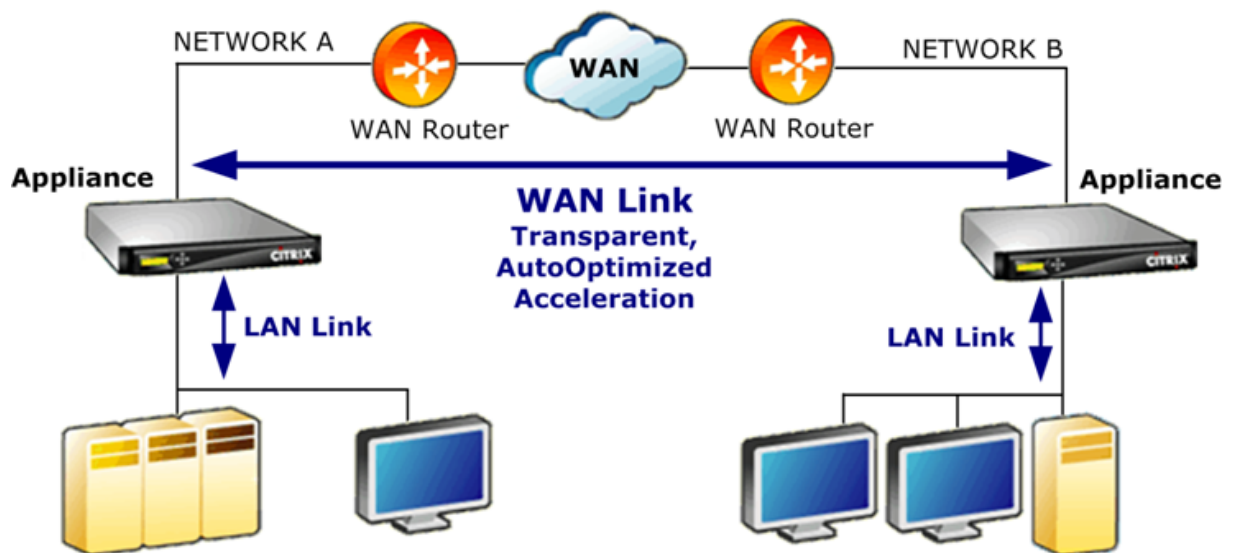
kann. Dies ist wichtig, wenn die Geschwindigkeit einer Verbindung schnell auf ihre faire Bandbreitenfreigabe hoch- oder heruntergefahren werden muss, und ist auch wichtig, um erweiterte WAN-Algorithmen und -Komprimierung zu unterstützen.

Das TCP-Protokoll soll jede TCP-Verbindung versuchen, ihre Bandbreitenauslastung kontinuierlich zu erhöhen. Die Verbindungsbandbreite ist jedoch begrenzt. Das Ergebnis ist, dass die Links überlaufen werden. Die Citrix SD-WAN WANOP-Flusssteuerung sorgt dafür, dass die TCP-Verbindungen genau mit der richtigen Geschwindigkeit fließen. Der Link ist gefüllt, wird aber nie überlaufen, so dass Warteschlangenlatenz und Paketverluste minimiert werden, während der Durchsatz maximiert wird.

Bei gewöhnlichem TCP neigen lange laufende Verbindungen (die Zeit hatten, die die gesamte Bandbreite zu nutzen) dazu, kurzlaufende Verbindungen auszuquetschen. Dieses Problem, das die interaktive Reaktionsfähigkeit ruiniert, tritt bei der Flusssteuerung nicht auf.

Die Flusskontrolle ist eine Standardfunktion für alle Appliances der Citrix SD-WAN WANOP-Familie.

Abbildung 1. Beschleunigung verbessert die Leistung transparent



## Geschwindigkeitsoptimierung

April 19, 2021

Die meisten TCP-Implementierungen funktionieren nicht weit über WAN-Verbindungen. Um nur zwei Probleme zu nennen, sind die standardmäßigen TCP-Weiterübertragungsalgorithmen (Selective Acknowledgments und TCP Fast Recovery) für Verbindungen mit hohen Verlustraten unzureichend und berücksichtigen nicht die Anforderungen kurzlebiger Transaktionsverbindungen.

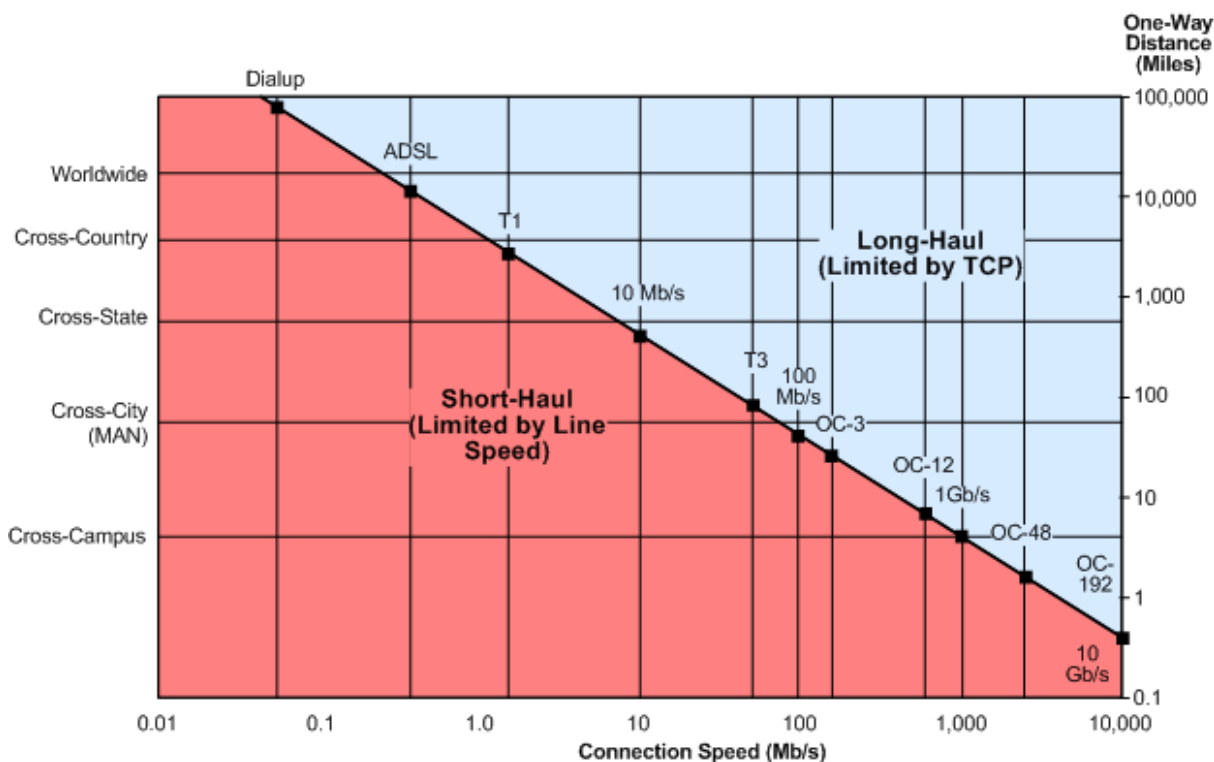
Citrix SD-WAN WANOP implementiert ein breites Spektrum von WAN-Optimierungen, um die Daten unter allen Arten von widrigen Bedingungen am Laufen zu halten. Diese Optimierungen arbeiten transparent, um sicherzustellen, dass die Daten so schnell wie möglich am Ziel ankommen.

Die WAN-Optimierung funktioniert transparent und erfordert keine Konfiguration.

Die WAN-Optimierung ist eine Standardfunktion für alle Citrix SD-WAN WANOP-Appliances.

Die folgende Abbildung zeigt die Übertragungsgeschwindigkeiten, die in verschiedenen Entfernungen ohne Beschleunigung möglich sind, wenn die Endpunkte Standard TCP (TCP Reno) verwenden. Zum Beispiel sind Gigabit-Durchsätze ohne Beschleunigung innerhalb eines Radius von wenigen Meilen möglich, 100 Mbit/s sind auf weniger als 100 Meilen erreichbar, und der Durchsatz auf einer weltweiten Verbindung ist auf weniger als 1 Mbit/s begrenzt, unabhängig von der tatsächlichen Geschwindigkeit der Verbindung. Mit der Beschleunigung stehen jedoch die Geschwindigkeiten oberhalb der Diagonallinie für Anwendungen zur Verfügung. Entfernung ist kein begrenzender Faktor mehr.

Abbildung 1. Nicht beschleunigte TCP-Leistung stürzt mit Abstand



#### Hinweis

Ohne Citrix Beschleunigung ist der TCP-Durchsatz umgekehrt proportional zur Entfernung, wodurch es unmöglich ist, die volle Bandbreite von Hochgeschwindigkeitsverbindungen mit Fernstrecken zu extrahieren. Mit Beschleunigung verschwindet der Entfernungsfaktor, und die volle Geschwindigkeit einer Verbindung kann in jeder Entfernung verwendet werden. (Diagramm basiert auf dem Modell von Mathis, *et al*, Pittsburgh Supercomputer Center.)

Die beschleunigte Übertragungsleistung entspricht ungefähr der Verbindungsbandbreite. Die Übertragungsgeschwindigkeit ist nicht nur höher als bei nicht beschleunigtem TCP, sondern ist auch angesichts der sich ändernden Netzwerkbedingungen viel konstant. Der Effekt besteht darin, dass sich entfernte Verbindungen so verhalten, als wären sie lokal. Vom Benutzer wahrgenommene Reaktionsfähigkeit bleibt unabhängig von der Link-Auslastung konstant. Im Gegensatz zu normalem TCP, bei dem ein WAN mit 90% Auslastung für interaktive Aufgaben nutzlos ist, hat eine beschleunigte Verbindung bei 90% Link-Auslastung die gleiche Reaktionsfähigkeit wie bei 10%.

Bei Kurzstreckenverbindungen (diejenigen, die unter die diagonale Linie in der obigen Abbildung fallen) erfolgt wenig oder keine Beschleunigung unter guten Netzwerkbedingungen, aber wenn sich aber die Netzwerksituation verschlechtert, sinkt die Leistung viel langsamer ab als bei gewöhnlichem TCP.

Nicht-TCP-Datenverkehr, wie UDP, wird nicht beschleunigt. Es wird jedoch immer noch vom Traffic Shaper verwaltet.

## Beispiel

Ein Beispiel für erweiterte TCP-Optimierungen ist eine Weiterübertragungsoptimierung, der *Transaktionsmodus* genannt wird. Eine Besonderheit von TCP ist, dass, wenn das letzte Paket in einer Transaktion gelöscht wird, der Verlust nicht vom Sender bemerkt wird, bis ein Receiver Timeout (RTO) Zeitraum abgelaufen ist. Diese Verzögerung, die immer mindestens eine Sekunde lang und oft länger ist, ist die Ursache für die Verzögerungen in mehreren Sekunden bei verlustbehafteten Links-Verzögerungen, die interaktive Sitzungen unangenehm oder unmöglich machen.

Der Transaktionsmodus löst dieses Problem, indem das endgültige Paket einer Transaktion nach einer kurzen Verzögerung automatisch erneut übertragen wird. Daher erfolgt eine RTO nur, wenn beide Kopien gelöscht werden, was unwahrscheinlich ist.

Eine Massenübertragung ist im Grunde eine einzige enorme Transaktion, so dass die zusätzliche Bandbreite, die vom Transaktionsmodus für eine Massenübertragung verwendet wird, nur ein Paket pro Datei betragen kann. Interaktiver Datenverkehr, wie Tastendruck oder Mausbewegungen, weist jedoch kleine Transaktionen auf. Eine Transaktion kann aus einem einzelnen unterdimensionierten Paket bestehen. Das Doppelte Senden solcher Pakete hat eine bescheidene Bandbreitenanforderung. Tatsächlich bietet der Transaktionsmodus eine Forward-Fehlerkorrektur (FEC) für interaktiven Datenverkehr und bietet einen RTO Schutz für das Ende der Transaktion für anderen Datenverkehr.

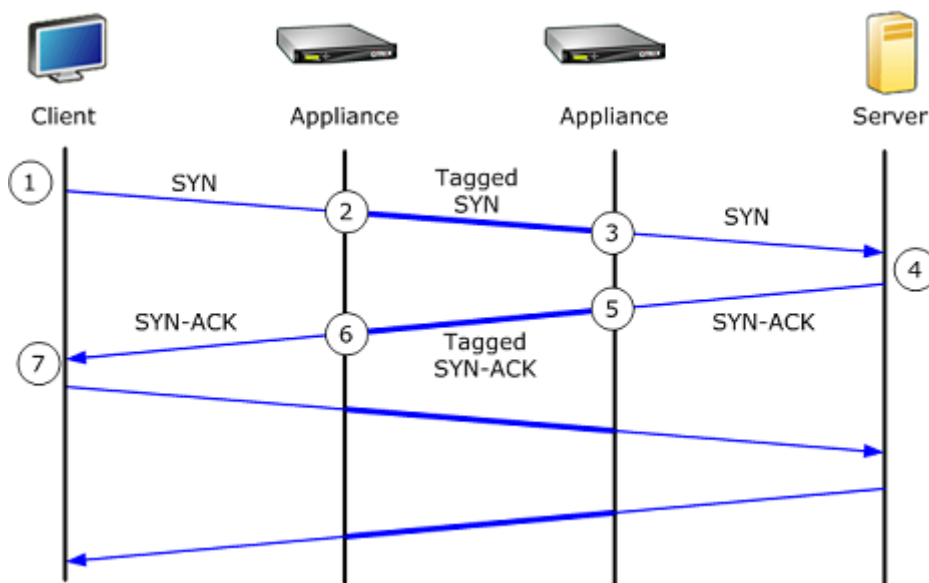
## Automatische Erkennung und automatische Konfiguration

April 19, 2021

Im Prozess, der Autodiscovery genannt wird, erkennen Citrix SD-WAN WANOP-Einheiten die Anwesenheit des anderen automatisch. Die Appliances hängen TCP-Header-Optionen an die ersten Pakete in jeder Verbindung an: das SYN-Paket (vom Client an den Server gesendet, um die Verbindung zu öffnen) und das SYN-ACK-Paket (vom Server an den Client gesendet, um anzuzeigen, dass die Verbindung akzeptiert wurde). Durch das Taggen der SYN-Pakete und das Abhören von getaggten SYN- und SYN-ACK-Paketen können die Appliances die Anwesenheit des anderen in Echtzeit erkennen.

Der Hauptvorteil der automatischen Erkennung besteht darin, dass Sie nicht jedes Mal neu konfigurieren müssen, wenn Sie Ihrem Netzwerk eine neue Appliances hinzufügen. Sie finden sich automatisch. Darüber hinaus ermöglicht der gleiche Prozess die automatische Konfiguration. Die beiden Appliances verwenden die TCP-Header-Optionen, um Betriebsparameter auszutauschen, einschließlich der Bandbreitengrenzen (sowohl in der Sende- als auch Empfangsanweisung), des grundlegenden Beschleunigungsmodus (hardboost oder softboost) und der akzeptablen Komprimierungsmodi (disk, memory oder none). Alle Informationen, die jede Appliance über ihren Partner benötigt, werden mit jeder Verbindung ausgetauscht, so dass Variationen pro Verbindung möglich sind (z. B. Variationen pro Service-Klasse in den zulässigen Komprimierungstypen).

Abbildung 1. Funktionsweise der Autodiscovery



Der AutoDiscovery-Prozess funktioniert wie folgt:

1. Der Client öffnet wie gewohnt eine TCP-Verbindung zum Server, indem er ihm ein TCP SYN-Paket sendet.
2. Die erste Appliance leitet das SYN-Paket durch, nachdem sie eine Reihe von anwendungsspezifischen TCP-Header-Optionen hinzugefügt und deren Fenstergröße angepasst hat.
3. Die zweite Appliance liest die TCP-Optionen, entfernt sie aus dem Paket und leitet sie an den Server weiter.

4. Der Server akzeptiert die Verbindung, indem er wie gewohnt mit einem TCP SYN-ACK-Paket reagiert.
5. Die zweite Appliance merkt sich, dass diese Verbindung ein Kandidat für die Beschleunigung ist und fügt ihre eigenen Beschleunigungsoptionen an den SYN-ACK-Header an.
6. Die erste Appliance liest die von der zweiten Appliance hinzugefügten Optionen, entfernt sie aus dem Paketheader und leitet das Paket an den Client weiter. Die Verbindung wird nun beschleunigt. Die beiden Appliances haben die notwendigen Parameter über die Optionswerte ausgetauscht und speichern sie für die Dauer der Verbindung im Speicher.

Die Verbindung wird beschleunigt und die Beschleunigung ist für Client, Server, Router und Firewalls transparent.

## TCP-Strömungssteuerungsmodi

April 19, 2021

TCP-Flusssteuerung hat zwei Modi: Softboost und Hardboost.

Softboost verwendet einen ratenbasierten Absender, der beschleunigten Datenverkehr mit Geschwindigkeiten bis zur Bandbreite der Verbindung sendet. Wenn das Bandbreitenlimit etwas niedriger als die Verbindungsgeschwindigkeit festgelegt ist, werden Paketverlust und Latenz minimiert, während die Link-Auslastung maximiert wird. Interaktive Anwendungen sehen schnelle Reaktionszeiten, während Massenübertragungsanwendungen eine hohe Bandbreite aufweisen. Softboost teilt das Netzwerk mit anderen Anwendungen in jeder Topologie und arbeitet mit QoS-Systemen von Drittanbietern zusammen.

Hardboost ist aggressiver als Softboost. Durch das Ignorieren von Paketverlusten und anderen sogenannten Staus Signalen funktioniert es sehr gut bei Verbindungen, die mit schweren, nicht überlastenden Verlusten wie Satellitenverbindungen geplagt sind. Es eignet sich auch hervorragend für Langstreckenverbindungen mit einem hohen Hintergrund-Paketverlust, wie viele Übersee-Links. Hardboost wird nur für Punkt-zu-Punkt-Links empfohlen, die mit Softboost keine ausreichende Leistung erzielen.

Softboost ist der Standardmodus und wird in den meisten Fällen empfohlen.

### Hinweis

- Hardboost sollte nur für Punkt-zu-Punkt-Verbindungen mit fester Geschwindigkeit oder Hub-and-Spoke-Bereitstellungen verwendet werden, bei denen die Hubbandbreite mindestens gleich der Summe der beschleunigten Spoke-Bandbreiten ist.

- Softboost und Hardboost schließen sich gegenseitig aus, was bedeutet, dass alle Appliances, die miteinander kommunizieren müssen, gleich gesetzt werden müssen. Wenn eine Einheit auf Hardboost und die andere auf Softboost eingestellt ist, findet keine Beschleunigung statt.

### So wählen Sie den Softboost Modus aus:

Softboost ist der Standardmodus und wird in den meisten Fällen empfohlen.

1. Navigieren Sie zu **Konfiguration > Links > Hardboost/ Softboost** und klicken Sie auf Bearbeiten.
2. Wählen Sie **Softboost** als **WAN-Boost-Modus**.

The screenshot shows the 'Link Settings' dialog box. Under 'WAN Boost Mode', the 'Softboost' radio button is selected. Below it, the 'WAN Bandwidth Receive Limit' is set to '1' in the input field, and 'gbps' is selected in the dropdown menu. At the bottom, there are 'Save' and 'Cancel' buttons.

3. Klicken Sie auf **Speichern**

### So wählen Sie den Hardboost Modus aus:

Wählen Sie den Hardboost Modus nur bei Punkt-zu-Punkt-Verbindungen mit fester Geschwindigkeit oder Hub-and-Spoke-Verbindungen, bei denen die Hubbandbreite größer oder gleich der beschleunigten Spoke-Verbindungen ist.

1. Navigieren Sie zu **Konfiguration > Links > Hardboost/ Softboost** und klicken Sie auf Bearbeiten.
2. Wählen Sie **Hardboost** als **WAN-Boost-Modus**.
3. Stellen Sie das **Empfangslimit für WAN-Bandbreite** auf 95% der Verbindungsgeschwindigkeit ein.
4. Klicken Sie auf **Save**.

## Überlegungen zu Firewalls

April 19, 2021

Die Verwendung von TCP-Optionen durch die Citrix SD-WAN Appliance gefährdet den beschleunigten Datenverkehr durch Firewalls, die aggressive Regeln für die Verweigerung von Diensten für Verbindungen mit weniger häufigen TCP-Optionen haben.

Einige Firewalls entfernen die unbekannten Optionen und leiten dann das Paket weiter. Diese Aktion verhindert Beschleunigung, beeinträchtigt aber nicht die Konnektivität.

Andere Firewalls verweigern den Dienst für Verbindungen mit unbekannten Optionen. Das heißt, die SYN-Pakete mit Citrix SD-WAN WANOP-Optionen werden von der Firewall verworfen. Wenn die Appliance wiederholte Verbindungsversuchsfehler erkennt, wird es ohne die Optionen wiederholt. Dies stellt die Konnektivität nach einer Verzögerung mit variabler Länge wieder her, normalerweise im Bereich von 20-60 Sekunden, jedoch ohne Beschleunigung.

Jede Firewall, die Citrix SD-WAN WANOP-Optionen nicht über unverändert weitergibt, muss neu konfiguriert werden, um TCP-Optionen im Bereich von 24 bis 31 (Dezimal) zu akzeptieren.

Die meisten Firewalls blockieren diese Optionen nicht. Allerdings können Cisco ASA und PIX Firewalls (und vielleicht andere) mit Version 7.x-Firmware dies standardmäßig tun.

Die Firewalls an beiden Enden des Links sollten untersucht werden, da beide Optionen für ausgehende Verbindungen zulassen, aber sie bei eingehenden Verbindungen blockieren können.

Das folgende Beispiel sollte mit Cisco ASA 55x0 Firewalls mit 7.x Firmware funktionieren. Da es global Optionen im Bereich von 24-31 erlaubt, gibt es keine benutzerdefinierte Konfiguration pro Schnittstelle oder pro Einheit:

```

1  =====
2  CONFIGURATION FOR CISCO ASA 55X0 WITH 7.X CODE TO ALLOW TCP OPTIONS
3  =====
4  hostname(config)# tcp-map WSOptions
5  hostname(config-tcp-map)# tcp-options range 24 31 allow
6  hostname(config-tcp-map)# class-map WSOptions-class
7  hostname(config-cmap)# match any
8  hostname(config-cmap)# policy-map WSOptions
9  hostname(config-pmap)# class WSOptions-Class
10 hostname(config-pmap-c)# set connection advanced-options WSOptions
11 hostname(config-pmap-c)# service-policy WSOptions global
12 <!--NeedCopy-->

```

Die Konfiguration für eine PIX Firewall ist ähnlich:

```

1  =====
2  POLICY MAP TO ALLOW APPLIANCE TCP OPTIONS TO PASS (PIX 7.x)
3  =====
4  pixfirewall(config)#access-list tcpmap extended permit tcp any any
5  pixfirewall(config)# tcp-map tcpmap
6  pixfirewall(config-tcp-map)# tcp-opt range 24 31 allow
7  pixfirewall(config-tcp-map)# exit
8  pixfirewall(config)# class-map tcpmap
9  pixfirewall(config-cmap)# match access-list tcpmap
10 pixfirewall(config-cmap)# exit
11 pixfirewall(config)# policy-map global_policy
12 pixfirewall(config-pmap)# class tcpmap
13 pixfirewall(config-pmap-c)# set connection advanced-options tcpmap
14 <!--NeedCopy-->

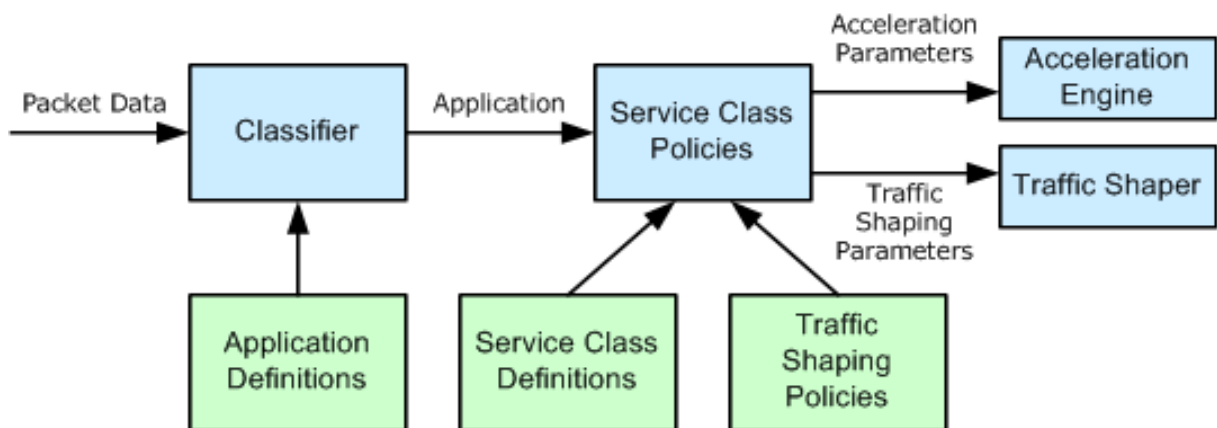
```



## Verkehrsklassifizierung

April 19, 2021

Die beiden Hauptfunktionen einer Citrix SD-WAN WANOP-Appliance sind Traffic Shaping, die die Link-Nutzung für alle Arten von Datenverkehr maximiert, und Beschleunigung, die Komprimierung und verschiedene Optimierungen zur Beschleunigung des TCP-Datenverkehrs anwendet. Zwei grundlegende Komponenten der Traffic Shaping und Beschleunigung sind der Application-Classifizierung Mechanismus und der Service-Class-Mechanismus. Ersteres identifiziert die Art des Datenverkehrs, so dass letztere den Datenverkehr einer Service-Klasse zuweisen kann. Jede Dienstklasse verfügt über eine Traffic Shaping-Richtlinie und eine Beschleunigungsrichtlinie.



## Anwendungsklassifizierer

April 19, 2021

Der Anwendungsklassifizierer verwendet Anwendungsdefinitionen, um den Datenverkehr nach Protokoll und Anwendung zu kategorisieren. Diese Informationen werden zum Erstellen von Berichten und vom Service-Class-Mechanismus verwendet. Viele Anwendungen sind bereits definiert, und Sie können bei Bedarf mehr definieren.

### Protokoll- und Portspezifikationen in Anwendungsdefinitionen

Der Anwendungsklassifizierer verwendet das offizielle Protokoll und die Portspezifikationen der Internet Assigned Numbers Authority (IANA) <http://www.iana.org>. Manchmal verwenden andere Anwendungen als die offiziellen einen Port. Der Klassifikator kann eine solche Verwendung im Allgemeinen nicht erkennen. Wenn Ihr Netzwerk solche Anwendungen verwendet, können Sie dieses Problem

normalerweise beheben, indem Sie die Anwendung im Anwendungsklassifizierer umbenennen, um die tatsächliche Anwendung anzugeben, die diesen Port im Netzwerk verwendet. Wenn Sie beispielsweise Port 3128 nicht für die Standardverwendung für einen Squid-Webcache verwenden, sondern für einen SOCKS-Proxy, können Sie die Anwendung Squid (TCP) in SOCKS (Port 3128) umbenennen.

Anwendungen dürfen keine überlappenden Definitionen aufweisen. Wenn beispielsweise eine Anwendung im Netzwerk TCP-Ports 3120 und 3128 verwendet und eine andere Anwendung Port 3120 verwendet, kann nur eine Citrix SD-WAN WANOP-Anwendungsdefinition Port 3120 enthalten.

## Anwendungsdefinitionen konfigurieren

- Dynamisches TCP, für Anwendungen mit dynamischen Portzuweisungen
- Ether-Typ, für Ethernet-Pakettypen
- Veröffentlichte ICA-Apps für Virtual Apps/Virtual Desktops-Anwendungen
- IP, für IP-Protokolle wie ICMP oder GRE
- TCP, für TCP-Anwendungen
- UDP, für UDP-Anwendungen
- Webadresse für bestimmte Websites oder Domänen.

So konfigurieren Sie eine Anwendungsdefinition:

1. Navigieren Sie zu **Konfiguration>Optimierungsregeln>Anwendungsklassifizierer** und klicken Sie auf **Hinzufügen**.

The screenshot shows the 'Create Application' form in the Citrix SD-WAN WANOP interface. The form is divided into several sections:

- Name\***: A text input field containing 'Viber'.
- Description**: A text input field containing 'messaging'.
- Application Group\***: A section with two panels. The left panel, titled 'Available (25)', lists various application groups with expand/collapse icons. The right panel, titled 'Configured (2)', shows the selected groups: 'Email and Collaboration' and 'Custom'.
- Classification Type\***: A dropdown menu set to 'TCP'.
- Port\***: A text input field containing '5243'.
- Buttons**: 'Create' and 'Close' buttons at the bottom left.

2. Legen Sie auf der Seite „**Anwendung erstellen**“ die folgenden Parameter fest:

- **Name** - Name des Anwendungsklassifizierers. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (\_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstrich, Hash (#), Punkt (.), Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Maximale Länge: 31 Zeichen.
- **Beschreibung** - Beschreibung des Anwendungsklassifizierers.
- **Anwendungsgruppe** - Der Anwendungsklassifizierer gehört zu dieser Anwendungsgruppe. Anwendungsgruppen sind eine Gruppe vordefinierter Anwendungsgruppen, die auf der Grundlage ihrer Funktionalität kategorisiert werden.
- **Klassifizierungsart** - Die Klassifizierung auf hoher Ebene, die Sie für diesen Anwendungsklassifikator verwenden möchten. Die High-Level-Klassifizierung erfolgt meist auf der Grundlage des Ports, den eine Anwendung verwendet.
- **Port** —Die zu verwendende Portnummer. Sie können einen Bereich, eine Liste oder eine Zahl zwischen 0 und 65535 eingeben.

### 3. Klicken Sie auf **Erstellen**.

Auf der Seite **Anwendungsklassifizierer** werden alle Anwendungen aufgelistet, die vom SD-WANOP-Klassifikator erkannt werden.

Die Seite **Application Classifiers** listet alle Anwendungen auf, die vom SD-WAN WANOP-Klassifikator erkannt werden.

#### **Tipp**

Klicken Sie auf **Auto Discover**, damit alle veröffentlichten Citrix Anwendungen, die im Datenstrom angezeigt werden, automatisch zur Anwendungsliste hinzugefügt werden. Sobald sie entdeckt wurden, werden sie in Berichten angezeigt und können für Traffic-Forming-Richtlinien verwendet werden.

## Serviceklassen

April 19, 2021

Dienstklassen werden Traffic-Shaping-Richtlinien und Beschleunigungsrichtlinien zugewiesen, die für alle Verbindungen verwendet werden, die der Service-Class-Definition entsprechen. Serviceklassen können auf folgenden Parametern basieren:

- Anwendungen
- IP- oder VLAN-Adressen

- DSCP Bits
- SSL-Profile

Als Ausgangspunkt werden die standardmäßigen Service-Class-Definitionen empfohlen. Ändern Sie sie, wenn sie sich als unzureichend für Ihre Links erweisen.

Die Serviceklassen werden in einer geordneten Liste definiert. Die erste Definition, die dem verarbeiteten Datenverkehr entspricht, wird zur Dienstklasse für den Datenverkehr.

## **Unterschiede zwischen Beschleunigungsentscheidungen und Traffic Shaping Policies**

Um eine Beschleunigungsentscheidung zu treffen, untersucht die Citrix SD-WAN WANOP-Appliance das anfängliche SYN-Paket jeder TCP-Verbindung, um festzustellen, ob die Verbindung ein Kandidat für die Beschleunigung ist. Das SYN-Paket enthält keine Payload, nur Header. Daher muss die Beschleunigungsentscheidung auf dem Inhalt der Kopfzeilen des SYN-Pakets basieren, z. B. dem Zielport oder der Ziel-IP-Adresse der Verbindung. Die Beschleunigung dauert, sobald sie angewendet wird, für die Dauer der Verbindung.

Im Gegensatz zu Beschleunigungsentscheidungen können Traffic-Forming-Richtlinien auf dem Inhalt des Datenstroms der Verbindung basieren. Je nachdem, wie lange es dauert, bis der Anwendungsklassifikator genügend Daten für eine endgültige Klassifizierung erhält, kann eine Verbindung während seiner Lebensdauer neu klassifiziert werden.

Beispielsweise ist das erste Paket in einer HTTP-Verbindung zu <http://www.example.com> ein SYN-Paket, das einen Header, aber keine Nutzlast enthält. Der Header verfügt über einen IP-Zielport von 80, der mit der Definition der HTTP: Internet-Service-Klasse übereinstimmt. Daher basiert die Acceleration-Engine ihre Beschleunigungsentscheidung, in diesem Fall keine (keine Beschleunigung) auf diese Serviceklasse.

Der Traffic Shaper verwendet die Traffic-Shaping-Richtlinie der Dienstklasse HTTP: Internet, aber diese Entscheidung ist vorübergehend. Das erste Payload-Paket enthält die Zeichenfolge GET <http://www.example.com>, die der Beispiel-Anwendungsdefinition im Anwendungsklassifizierer entspricht. Die Serviceklasse, die die Beispielanwendung enthält, wird vom Traffic-Shaper ausgewählt, stattdessen von der Serviceklasse, die HTTP: Internet enthält, und der Traffic-Shaper verwendet die in dieser Service-Class-Definition benannte Dienstleistungsklassenrichtlinie.

### **Hinweis**

Unabhängig von der Serviceklassenrichtlinie verfolgt die Berichtsfunktion die Verwendung der Beispielanwendung.

### **Wichtig**

Der gesamte Datenverkehr ist mit einer Anwendung und einer Serviceklasse verknüpft, und alle

Serviceklassen haben eine Traffic-Shaping-Richtlinie, aber nur TCP-Verbindungen haben eine andere Beschleunigungsrichtlinie als keine.

## Konfigurieren von Service-Klassendefinitionen

Da Service-Class-Definitionen eine geordnete Liste sind, muss eine Definition, die eine Ausnahme für einen allgemeinen Fall darstellt, der allgemeineren Definition auf der Seite Service-Klasse vorausgehen. Die erste Definition, deren Regel mit dem Datenverkehr übereinstimmt, ist die, die angewendet wird. Beispiel:

- Dienstklassen, die auf URLs basieren, müssen vor den HTTP-Dienstklassen in der Dienstklassenliste stehen, da jede URL-basierte Regel auch mit der HTTP-Dienstklasse übereinstimmt. Daher würde das Setzen der HTTP-Dienstklasse verhindern, dass die URL-basierten Regeln oder veröffentlichten anwendungsbasierten Regeln jemals verwendet werden.
- Genauso müssen Dienstklassen, die auf ICA-veröffentlichten Anwendungen (Virtual Apps/Virtual Desktops) basieren, vor der Citrix Serviceklasse stehen.

Da alle URL-basierten Regeln mit der HTTP-Dienstklasse übereinstimmen, würde das Übersetzen der HTTP-Dienstklasse dazu führen, dass die URL-basierten Regeln oder veröffentlichten anwendungsbasierten Regeln niemals verwendet werden.

Configuration Overview > Optimization Rules > Service Classes					
<div> Add Edit Delete Update Order Filter Rules </div> <div>Show User Modified Service Classes Only</div>					
Order	Name	Status	Acceleration Policy	Traffic Shaping Policy	Appflow Reporting Status
1	ICA	Enabled	disk	ICA Priorities	Enabled
2	Web (Private)	Enabled	disk	Default Policy	Enabled
3	Web (Private-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
4	Web (Internet)	Enabled	disk	Default Policy	Enabled
5	Web (Internet-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
6	CIFS	Enabled	disk	Default Policy	Enabled
7	NFS	Enabled	disk	Default Policy	Enabled
8	Microsoft Exchange (MAPI)	Enabled	disk	Default Policy	Enabled
9	Mail (Other)	Enabled	disk	Default Policy	Enabled
10	VOIP and Multimedia	Enabled	None	VOIP Traffic	Enabled
11	VOIP Webcam	Enabled	None	High Priority Traffic	Enabled
12	FTP Data	Enabled	disk	Low Priority Traffic	Enabled
13	FTP Control	Enabled	Flow Control Only	Default Policy	Enabled
14	Instant Messaging	Enabled	disk	Default Policy	Enabled
15	Session Applications	Enabled	Flow Control Only	Default Policy	Enabled
16	Directory and Security	Enabled	Flow Control Only	Default Policy	Enabled
17	Database Applications	Enabled	Flow Control Only	Default Policy	Enabled
18	Secure Applications	Enabled	Flow Control Only	Default Policy	Enabled
19	Iperf	Enabled	Flow Control Only	Low Priority Traffic	Enabled
20	NetApp SnapMirror	Enabled	memory	Default Policy	Enabled
21	Other TCP Traffic	Enabled	None	Default Policy	Enabled
22	Unclassified Traffic	Enabled	None	Default Policy	Enabled

So erstellen Sie eine RPC-über-HTTP-Dienstklasse und binden das SSL-Profil daran:

1. Navigieren Sie zu **Konfiguration>Optimierungsregeln>Serviceklassen** und klicken Sie auf **Hinzufügen**.

Dashboard Monitoring **Configuration** Downloads Notifications (6)

← Back

### Create Service Classes

Name\*  
RPC over HTTP

☒ Enabled

Acceleration Policy\*  
disk

Traffic Shaping Policy  
☒ Single Policy ☐ Per Link Policy

☒ Enable AppFlow Reporting  
☐ Exclude from SSL Tunnel

Default Policy

Filter Rules

Add Edit Delete

Application	Source IP Address	Destination IP Address	VLANs	DiffServ DSCP Bits	Direction	SSL Profiles
No items						

Create Close

- Geben Sie im Feld **Name** einen Namen für die Serviceklasse ein.
- Stellen Sie sicher, dass die Option **Aktiviert** ausgewählt ist.
- Wählen Sie in der Liste **Beschleunigungsrichtlinie** eine Beschleunigungsrichtlinie aus. **Speicher** und **Datenträger** sind die besten Wahl, da die Appliance automatisch Datenträger oder Speicher auswählt, je nachdem, was für den Datenverkehr besser geeignet ist. **Der Speicher** gibt nur den Speicher an. Wählen Sie **Nur Flow Control**, um die Komprimierung zu deaktivieren, aber die Beschleunigung der Flusststeuerung zu aktivieren. Wählen Sie diese Option für immer verschlüsselte Dienste und für den FTP-Steuerkanal aus. **Keiner** wird nur für nicht komprimierbaren verschlüsselten Datenverkehr und Echtzeit-Video verwendet.
- Wählen Sie **AppFlow Reporting** aktivieren, um AppFlow-Berichte für diese Service Class zu aktivieren. Informationen aus dieser Serviceklasse sind in AppFlow Berichten enthalten. AppFlow ist ein Industriestandard für die Entsperrung von Anwendungstransaktionsdaten, die von der Netzwerkinfrastruktur verarbeitet werden. Die WAN Optimization AppFlow-Schnittstelle funktioniert mit jedem AppFlow-Kollektor, um Berichte zu generieren. Der Kollektor erhält detaillierte Informationen von der Appliance unter Verwendung des offenen AppFlow Standards.
- Wählen Sie **Aus dem SSL-Tunnel** ausschließen, um den mit der Serviceklasse verbundenen Datenverkehr vom SSL-Tunneling auszuschließen.
- Stellen Sie in der Liste der Traffic Shaping-Richtlinien sicher, dass die Option **Standardrichtlinie** ausgewählt ist. Traffic Shaping-Richtlinien haben eine gewichtete Priorität und andere Attribute, die bestimmen, wie übereinstimmender Datenverkehr im Verhältnis zu anderem Datenverkehr behandelt wird. Die meisten Dienstklassen sind auf Standardrichtlinie festgelegt, aber Datenverkehr mit höherer Priorität kann eine Richtlinie für Traffic Shaping mit höherer Priorität zugewiesen werden, und Datenverkehr mit niedrigerer Priorität kann eine Richtlinie mit

geringerer Priorität zugewiesen werden.

8. Klicken Sie im Abschnitt Filterregeln auf **Hinzufügen**, um eine Filterregel zu erstellen, die Any als Standardwert für alle Parameter hat. Wenn eine Regel für eine bestimmte Verbindung als TRUE ausgewertet wird, wird die Verbindung dieser Serviceklasse zugewiesen. Filterregeln für die meisten Dienstklassen bestehen ausschließlich aus einer Liste von Anwendungen, aber Regeln können auch IP-Adressen, VLAN-Tags, DSCP-Werte und SSL-Profilnamen enthalten. Alle Felder in einer Regel sind standardmäßig Beliebig (ein Platzhalter). Felder innerhalb einer Regel werden mit einem logischen UND verbunden.
9. Klicken Sie auf **Hinzufügen**, um Filterregeln hinzuzufügen.

**Filter Rules**

Application Group\*  
Email and Collaboration

Application Classifiers\*

Available (27) Select All

NNTP	+
Novell Groupwise	+
POP3 (secure)	+
POP3 Kerberos	+
SMTP (clear)	+

Configured (2) Remove All

POP3 (clear)	-
Biff	-

Source IP Address  
10.102.29.230

Direction\*  
Unidirectional

Destination IP Address

VLANs

DiffServ DSCP Bits\*  
Best Effort

10. Wählen Sie in der Liste **Anwendungsgruppe** die Option **E-Mail und Zusammenarbeit** aus.
11. Wählen Sie aus der Liste **Verfügbar** die erforderlichen Anwendungen aus.
12. Verschieben Sie die ausgewählten Anwendungen in die Liste **Konfiguriert**.
13. Fügen Sie im Feld **Quell-IP-Adressen** die Client-IP-Adressen hinzu.
14. Wählen Sie **in der Liste Richtung** die Richtung des Datenverkehrs aus.
15. Wählen Sie in der Liste **SSL-Profil** das von Ihnen erstellte SSL-Profil aus.
16. Klicken Sie auf **Erstellen**.



**Hinweis**

- Sie müssen ein SSL-Profil nur auf der Datencenter-Appliance konfigurieren und an die Dienstklasse binden.
- Nur die Dienstklassen, deren Filterregelrichtung unidirektional festgelegt ist, können SSL-Profilen zugeordnet werden.

## Traffic Shaping

April 19, 2021

18. April 2018

Traffic Shaping ermöglicht es Ihnen, den Netzwerkdatenverkehr zu regulieren, um ein gewisses Maß an Servicequalität (QoS) zu gewährleisten. Sie können den Fluss von Paketen in ein Netzwerk (Bandbreitendrosselung) oder aus einem Netzwerk (Ratenbegrenzung) regulieren.

Mithilfe von Traffic Shaping Policies können Sie die Priorität des unterschiedlichen Link-Datenverkehrs festlegen und den Datenverkehr mit einer Geschwindigkeit in der Nähe, aber nicht höher als der Verbindungsgeschwindigkeit an die Verbindung senden. Im Gegensatz zu Beschleunigung, die nur für TCP/IP-Datenverkehr gilt, verarbeitet der Traffic Shaper den gesamten Datenverkehr auf der Verbindung.

Sie können eine hohe Bandbreite für Datenverkehrsflüsse festlegen, die wichtiger als die restlichen Verkehrsflüsse sind, sodass Sie die knappen Link-Ressourcen optimal nutzen können.

Die Traffic Shaping basiert auf gewichteter Fair Queuing, die jeder Serviceklasse ihren fairen Anteil an der Verbindungsbandbreite gibt. Wenn der Link im Leerlauf ist, kann jede Verbindung (in jeder Serviceklasse) den gesamten Link verwenden. Wenn mehrere Verbindungen um die Verbindungsbandbreite konkurrieren, wendet der Traffic Shaper Traffic Shaping-Richtlinien an, um die richtige Mischung aus Datenverkehr zu bestimmen.

Weitere Informationen zur gewichteten Fair Queuing finden Sie unter [Gewichtete Fair Queuing](#).

### So konfigurieren Sie Traffic Shaping:

1. Konfigurieren Sie die Linkdefinition.

Die Linkdefinition wird vom Traffic Shaper verwendet, um die Sende- und Empfangsgeschwindigkeit sowie andere verknüpfungsbezogene Informationen zu bestimmen. Weitere Informationen darüber, wie Traffic Shaper Link-Definition verwendet und wie Linkdefinitionen konfiguriert werden, finden Sie unter [Verknüpfungsdefinitionen](#).

2. Konfigurieren Sie die Anwendungsdefinition.

Der Datenverkehr, der durch die Verknüpfung fließt, wird vom Anwendungsklassifizierer untersucht, um zu welcher Anwendung er gehört, und dann wird die Anwendung in der Dienstklassenliste nachgeschlagen, um zu welcher Dienstklasse sie gehört. Weitere Informationen zur Anwendungsklassifizierung und zum Konfigurieren der Anwendungsdefinition finden Sie unter [Traffic-Klassifikation](#).

3. Erstellen Sie eine Traffic Shaping-Richtlinie.

Sie können die standardmäßigen Traffic Shaping-Richtlinien verwenden oder eine neue Richtlinie erstellen, um die gewichtete Priorität und andere Parameter gemäß Ihren Netzwerkanforderungen festzulegen. Hinweise zum Erstellen von Traffic Shaping Policy finden Sie unter [Traffic Shaping-Richtlinien](#).

4. Konfigurieren Sie eine Dienstklassendefinition, und ordnen Sie die Traffic Shaping-Richtlinie der Dienstklasse zu.

Hinweise zum Konfigurieren der Service-Klassendefinition finden Sie unter [Serviceklassen](#).

Einige Highlights des Traffic Shaper:

- Der gesamte WAN-Datenverkehr unterliegt der Traffic Shaping: beschleunigte Verbindungen, nicht beschleunigte Verbindungen und Nicht-TCP-Datenverkehr wie UDP-Flows und GRE-Streams.
- Der Algorithmus ist gewichtete Fair Queuing, in der der Administrator jeder Service-Klasse eine Priorität zuweist. Jede Serviceklasse stellt einen Bandbreitenpool dar, der auf einen Mindestanteil der Verbindungsgeschwindigkeit berechtigt ist, gleich  $(\text{my\_priority} / \text{sum\_of\_all\_priorities})$ . Eine Serviceklasse mit einer gewichteten Priorität von 100 erhält doppelt so viel Bandbreite wie eine Serviceklasse mit einer gewichteten Priorität von 50. Sie können Gewichte von 1 bis 256 zuweisen.
- Jede Verbindung innerhalb einer Dienstklasse erhält einen gleichen Anteil an der Bandbreite, die dieser Dienstklasse zugewiesen ist.
- Jede Verbindung erhält ihren fairen Anteil an der Verbindungsbandbreite, da nach der Komprimierung Prioritäten auf die tatsächlich übertragenen WAN-Daten angewendet werden. Wenn Sie beispielsweise über zwei Datenströme mit derselben Priorität verfügen, wobei einer die Komprimierung 10:1 und der andere eine Komprimierung 2:1 erreicht, sehen die Benutzer einen Unterschied im Durchsatz von 5:1, obwohl die WAN-Link-Nutzung der beiden Verbindungen identisch ist. In der Praxis ist diese Disparität wünschenswert, da WAN-Bandbreite und nicht Anwendungsbandbreite die knappe Ressource ist, die verwaltet werden muss.
- Traffic Shaping Policies gelten gleichermaßen für beschleunigten und nicht beschleunigten Datenverkehr. Beispiel: Eine beschleunigte Virtual Apps-Verbindung und eine unkonzertierte

Virtual Apps-Verbindung empfangen Traffic Shaping und haben daher im Vergleich zum Massendatenverkehr erhöhte Priorität. Ein weiteres Beispiel kann zeitbezogene Nicht-TCP-Datenverkehr wie VoIP (das UDP-Protokoll verwendet) beschleunigt werden.

- Traffic Shaping wird sowohl in den Sende- als auch Empfangsanweisungen auf die WAN-Link sowohl für beschleunigten als auch für nicht beschleunigten Datenverkehr angewendet. Diese Funktion verhindert Überlastung und erhöhte Latenz, selbst wenn die andere Seite der Verbindung nicht mit einer Citrix SD-WAN WANOP-Appliance ausgestattet ist. Beispielsweise können Internet-Downloads priorisiert und verwaltet werden.
- Die Traffic-Forming-Richtlinie für eine Service-Klasse kann auf Basis pro Link angegeben werden, falls gewünscht.
- Zusätzlich zur direkten Gestaltung des Datenverkehrs kann sich der Traffic Shaper indirekt auf ihn auswirken, indem das Feld Differentiated Services Code Point (DSCP) festgelegt wird, um nachgeschaltete Router über die Art des Datenverkehrs zu informieren, der jedes Paket benötigt.

## Gewichtete Fair Queuing

April 19, 2021

In jedem Link bestimmt das Engpassgateway die Warteschlangendisziplin, da Daten in den Nicht-Engpassgateways nicht sichern. Ohne ausstehende Daten in den Warteschlangen ist das Warteschlangenprotokoll irrelevant.

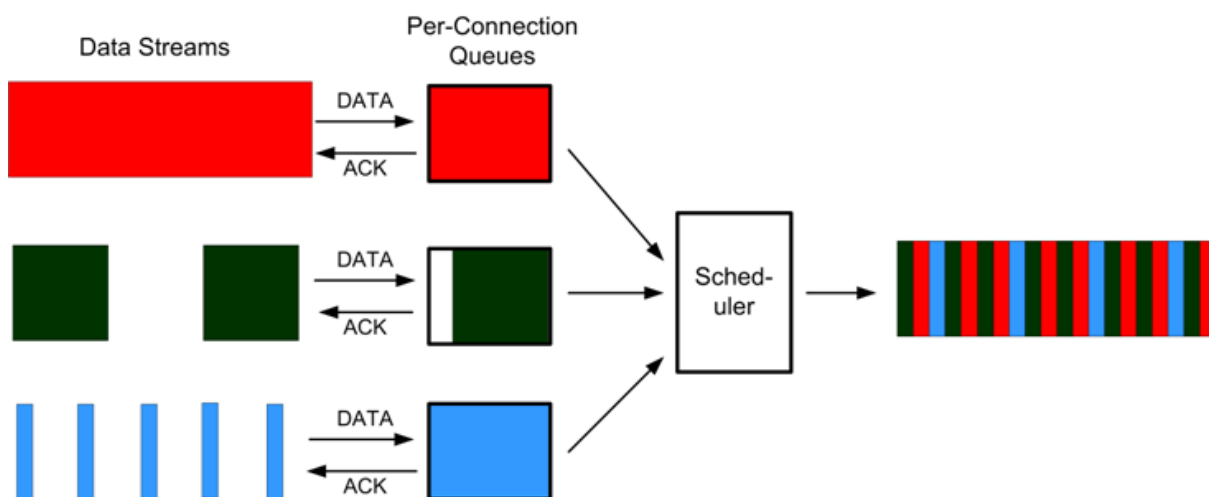
Die meisten IP-Netzwerke verwenden tiefe FIFO-Warteschlangen. Wenn der Datenverkehr schneller als die Engpassgeschwindigkeit eintrifft, füllen sich die Warteschlangen aus und alle Pakete erleiden erhöhte Warteschlangenzeiten. Manchmal ist der Verkehr in ein paar verschiedene Klassen mit separaten FIFOs unterteilt, aber das Problem bleibt bestehen. Eine einzelne Verbindung, die zu viele Daten sendet, kann zu großen Verzögerungen, Paketverlusten oder beides für alle anderen Verbindungen in ihrer Klasse führen.

Eine Citrix SD-WAN WANOP-Appliance verwendet *gewichtete Fair Queuing*, die eine separate Warteschlange für jede Verbindung bereitstellt. Mit Fair Queuing kann eine zu schnelle Verbindung nur ihre eigene Warteschlange überlaufen. Es hat keine Auswirkungen auf andere Verbindungen. Aber wegen der verlustfreien Flusssteuerung gibt es keine zu schnelle Verbindung und Warteschlangen überlaufen nicht.

Das Ergebnis ist, dass jede Verbindung ihren Traffic in die Verbindung gemessen hat und die Verbindung als Ganzes ein optimales Bandbreiten- und Latenzprofil aufweist.

Die folgende Abbildung zeigt die Wirkung von Fair Queuing. Eine Verbindung, die weniger als ihren fairen Anteil an Bandbreite (die untere Verbindung) benötigt, erhält so viel Bandbreite, wie sie zu verwenden versucht. Darüber hinaus hat es nur sehr geringe Warteschlangenlatenz. Verbindungen, die versuchen, mehr als ihren fairen Anteil zu nutzen, erhalten ihren fairen Anteil und jede Bandbreite, die von Verbindungen übrig bleibt, die weniger als ihren fairen Anteil verwenden.

Abbildung 1. Fair Queuing in Aktion



Das optimale Latenzprofil bietet Benutzern interaktiver und transaktionaler Anwendungen optimale Leistung, selbst wenn sie die Verbindung mit mehreren Massenübertragungen teilen. Die Kombination aus verlustfreier, transparenter Flow Control und Fair Queuing ermöglicht es Ihnen, alle Arten von Traffic über die gleiche Verbindung sicher und transparent zu kombinieren.

Der Unterschied zwischen gewichtetem Fair Queuing und ungewichtetem Fair Queuing besteht darin, dass gewichtetes Fair Queuing die Option beinhaltet, einigem Datenverkehr eine höhere Priorität (Gewichtung) zu geben. Traffic mit einem Gewicht von zwei erhält die doppelte Bandbreite des Traffic mit einem Gewicht von eins. In einer Citrix SD-WAN WANOP-Konfiguration werden die Gewichtungen in Traffic-Shaping-Richtlinien zugewiesen.

## Traffic Shaping-Richtlinien

April 19, 2021

Jede Service-Klassendefinition ist einer Traffic Shaping-Richtlinie zugeordnet, die Parameter für den Datenverkehr der zugeordneten Dienstklasse festlegt. Sie können Traffic Shaping-Richtlinien für Websites mit besonderen Anforderungen erstellen und konfigurieren, aber die Standardrichtlinieneinstellungen funktionieren für die meisten Installationen einwandfrei und bieten die folgenden Vorteile:

- Erhöhte Reaktionszeit für interaktiven Datenverkehr, z. B. Citrix Virtual Apps and Desktops.

- Schutz des latenz- und jitter-sensitiven VoIP-Datenverkehrs.
- Kein Aufschlagen der Wand in Spitzenzeiten. Sie erhalten eine nutzbare Leistung auch bei extremer Belastung.
- Die Bandbreitenauslastung wurde verbessert, da Massenübertragungen die Verbindung mit der Bandbreite füllen können, die von interaktiven Aufgaben übrig bleibt.
- Erweiterung der Vorteile von Fair Queuing auf den gesamten Traffic

Eine Citrix SD-WAN WANOP-Appliance wird mit werkseitig standardmäßigen Traffic Shaping-Richtlinien ausgeliefert, die eine Vielzahl von Prioritäten umfassen. Diese Richtlinien sind auf der Seite **Traffic Shaping Policies** aufgeführt. Abgesehen von der **Standardrichtlinie** können die anderen Werksstandardrichtlinien nicht bearbeitet oder gelöscht werden. Der Grund ist, sicherzustellen, dass sie auf allen Geräten die gleiche Bedeutung haben. Um Änderungen vorzunehmen, erstellen Sie eine neue Traffic-Forming-Richtlinie mit den neuen Parametern und ändern Sie die entsprechenden Service-Class-Definitionen, um auf die neue Traffic-Forming-Richtlinie zu verweisen.

### So erstellen Sie eine Traffic Shaping-Richtlinie:

1. Navigieren Sie in der SD-WANOP-Verwaltungsschnittstelle zu **Konfiguration > Optimierungsgesetze > Traffic Shaping-Richtlinien**, und klicken Sie auf **Hinzufügen**.

Name	Very High (Priority 256)	Voice Optimized	DiffServ/TOS	Maximum Incoming Bandwidth	Maximum Outgoing Bandwidth
VOIP Traffic	Very High (Priority 256)	✓	Expedited Forward...	75 %	75 %
Very High Priority Traffic	Very High (Priority 256)	✗	Disabled	0	0
High Priority Traffic	High (Priority 128)	✗	Disabled	0	0
Medium High Priority Traffic	Medium High (Priority 64)	✗	Disabled	0	0
Medium Priority Traffic	Medium (Priority 32)	✗	Disabled	0	0
Medium Low Priority Traffic	Medium Low (Priority 16)	✗	Disabled	0	0
Low Priority Traffic	Low (Priority 8)	✗	Disabled	0	0
Very Low Priority Traffic	Very Low (Priority 4)	✗	Disabled	0	0
ICA Priorities	Very High (Priority 256)	✗	Disabled	0	0
Default Policy	Medium (Priority 32)	✗	Disabled	0	0
TSP1	High (Priority 128)	✗	Disabled	10 %	10 %

2. Geben Sie auf der Seite **Traffic Shaping Policy erstellen** Werte für die folgenden Parameter ein:

- **Name**—Der Name der neuen Richtlinie. Muss einzigartig sein.
- **Gewichtete Priorität** —Sie können einen vorhandenen Prioritätswert auswählen oder einen benutzerdefinierten Wert zwischen 1 und 256 auswählen. Eine Verbindung mit einer Priorität von 256 erhält das 256-fache der Bandbreitenfreigabe als Verbindung mit der Priorität 1.
- **Voice optimieren**—Wenn diese Option ausgewählt ist, hat diese Richtlinie eine unendliche Priorität. Dies ist für den meisten Datenverkehr höchst unerwünscht, da es

ein wirkungsvolles Traffic Shaping verhindert und Engpässe für anderen Datenverkehr verursacht, wenn genügend für Voice optimierter Datenverkehr vorhanden ist, um die Verbindung auszufüllen. Nur für VoIP verwenden und immer in Verbindung mit einem Bandbreitenlimit für die Richtlinie verwenden (z. B. 50% der Verbindungsgeschwindigkeit)

### Hinweis

Die Sprachoptimierung kann nicht konfiguriert werden, während die ICA-Prioritäten festgelegt sind.

The screenshot shows the 'Create Traffic Shaping Policy' form in the Citrix SD-WAN WANOP 10.2 Configuration page. The form includes the following fields and options:

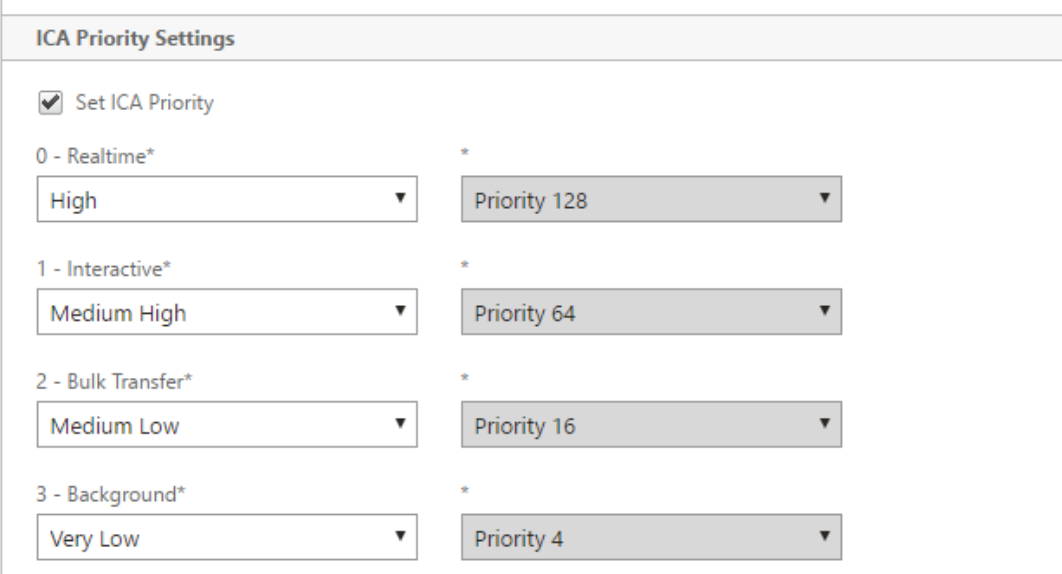
- Name\***: TSP1
- Weighted Priority\***: Very Low (dropdown)
- Priority**: Priority 4 (dropdown)
- Optimize for Voice**: ☒ (checked)
- DiffServ/TOS\***: AF12 - Silver (dropdown)
- DSCP**: DSCP 12 (binary: 001100) (dropdown)
- Bandwidth Limit\***: By Percentage of Link Bandwidth (dropdown)
- Maximum Incoming Bandwidth Rate (%)**: 50
- Maximum Outgoing Bandwidth Rate (%)**: 50
- ICA Priority Settings**: ☐ Set ICA Priority. ICA priorities cannot be configured while Optimize for Voice is enabled.
- ICA DiffServ/TOS Settings**: ☐ Set ICA DiffServ/TOS
- Less** (link)
- Add** (button)
- Cancel** (button)

- **DiffServ/TOS**—Legt die DSCP-Bits für Ausgabepakete auf den ausgewählten Wert fest. Wird verwendet, um nachgeschaltete Router zu steuern.
- **Bandbreitenbegrenzung** —Verhindert, dass der Datenverkehr, der diese Richtlinie verwendet, die angegebene Bandbreite überschreitet, die entweder als Prozentsatz der Verbindungsgeschwindigkeit oder als absoluter Wert angegeben wird. Citrix empfiehlt, einen Prozentsatz anzugeben, damit die gleiche Definition für Verknüpfungen unterschiedlicher Geschwindigkeiten gelten kann. Diese Funktion kann die Bandbreite ungenutzt lassen. Beispielsweise lässt eine Richtlinie, die auf 50% der Verbindungsgeschwindigkeit festgelegt ist, dem betroffenen Datenverkehr nicht mehr als 50% der Verbindung zu, selbst wenn die Verbindung ansonsten im Leerlauf ist. Die Einschränkung des Datenverkehrs auf diese Weise ist nicht mit der maximalen Leistung konsistent, daher wird diese Funktion nur selten verwendet, außer bei VoIP-Datenverkehr mit der Einstellung Voice optimieren.

**Hinweis**

Das Konfigurieren von **Bandbreitenlimit** gilt nur für Citrix SD-WAN WANOP Edition. Für Citrix SD-WAN PE Edition ist der Parameter **Bandwidth Limit** standardmäßig deaktiviert.

- **ICA-Priorität festlegen:** Wenn diese Richtlinie für den Citrix Virtual Apps-/Virtual Desktops-Datenverkehr verwendet wird, wird die interne Priorität des Datenverkehrs für Echtzeit-, interaktiven, Massenübertragungs- und Hintergrunddatenverkehr mit der hier festgelegten Priorität überschrieben.



ICA Priority Settings	
<input checked="" type="checkbox"/> Set ICA Priority	
0 - Realtime*	*
High	Priority 128
1 - Interactive*	*
Medium High	Priority 64
2 - Bulk Transfer*	*
Medium Low	Priority 16
3 - Background*	*
Very Low	Priority 4

- **Legen Sie ICA DiffServ/TOS fest:** Für den ICA-Datenverkehr (Virtual Apps/Virtual Desktops) kann jeder der vier ICA-Prioritätswerte mit einem anderen DSCP-Wert markiert werden. Diese Funktion ist besonders für das neue Multistream-ICA-Feature nützlich, in dem der Virtual Apps- oder Virtual Desktops-Client unterschiedliche Verbindungen für verschiedene Prioritätsebenen verwendet.

ICA DiffServ/TOS Settings	
<input checked="" type="checkbox"/> Set ICA DiffServ/TOS	
Multi-Stream (0 - Realtime)*	*
AF11 - Gold	DSCP 10 (binary: 001010)
Multi-Stream (1 - Interactive)*	*
AF21 - Gold	DSCP 18 (binary: 0010010)
Multi-Stream (2 - Bulk Transfer)*	*
AF12 - Silver	DSCP 12 (binary: 001100)
Multi-Stream (3 - Background)*	*
AF13 - Bronze	DSCP 14 (binary: 001110)
Single-Stream (All priorities)*	*
AF33 - Bronze	DSCP 30 (binary: 0011110)

- Klicken Sie auf **Hinzufügen**. Die neu erstellte Traffic Shaping Policy ist in der Liste Traffic Shaping Policies aufgeführt.

Sie können die Traffic Shaping-Richtlinie nun einer Dienstklasse zuordnen. Weitere Informationen finden Sie unter [Serviceklassen](#).

## Video-Caching

April 19, 2021

Viele Organisationen verwenden Videos für Kommunikation, die nicht zeitabhängig sind (z. B. Schulungen und vorab aufgezeichnete Nachrichten an Mitarbeiter). Die Kommunikation von Nachrichten über Videos ist nicht nur kostengünstig, sondern auch praktisch, wenn das Publikum über Zeitzone verteilt ist. Videos verbrauchen jedoch viel Bandbreite, wenn sie über das Internet abgespielt werden. Unzureichende Bandbreite verursacht Latenz, was sich auf die Benutzererfahrung auswirkt und die Auswirkungen der Videokommunikation beeinträchtigt.

Video-Caching verbessert die Anzeigeerfahrung für HTTP-Videostreams, insbesondere bei langsameren Links. Der Video-Cache wird auf der lokalen Citrix SD-WAN WANOP-Appliance verwaltet. Wenn ein lokaler Benutzer ein Video ansieht, das bereits zwischengespeichert wurde, kann die Appliance die zwischengespeicherte Kopie mit voller LAN-Geschwindigkeit bereitstellen.



Nachdem Sie die Appliance zum Zwischenspeichern von Videos konfiguriert haben, werden die von Ihren Benutzern angezeigten Videos zwischengespeichert. Sie können auch die Option Vorbevölkerung verwenden, um ausgewählte Videos vom lokalen Videoserver abzurufen, wenn Sie eine spätere Verwendung voraussetzen.

Die Video-Caching-Funktion verwendet einen abfänglichen Proxy-Cache, um alle HTTP-Anforderungen zu untersuchen. Anforderungen, die die unten aufgeführten Anforderungen erfüllen, werden zwischengespeichert. Videos werden nur aus dem Cache bereitgestellt, wenn sie von der Cache-Engine als frisch ausgewertet werden. Andernfalls werden sie erneut für den Viewer abgerufen, und die zuvor zwischengespeicherte Version wird überschrieben.

Aktueller Inhalt garantiert. Jedes Mal, wenn ein Video angezeigt wird, überprüft der Cache den Ursprungsserver. Wenn sich das Video geändert hat, wird der zwischengespeicherte Inhalt verworfen und der neue Inhalt wird heruntergeladen.

### **Hinweis**

Caching ist jetzt transparent. Das heißt, die IP-Adresse des Clients und des Servers werden End-to-End beibehalten. In früheren Versionen wurde die IP-Adresse der Citrix SD-WAN WANOP-Appliance als Quelladresse angezeigt.

Ein Video wird zwischengespeichert, wenn alle folgenden Kriterien erfüllt sind:

- Das Protokoll, das zum Streamen des Videos verwendet wird, ist HTTP. Standardmäßig ist Port 80 für Video-Caching konfiguriert. Wenn Sie jedoch einen anderen Port konfiguriert haben, z. B. 8080 für einen Webserver, müssen Sie diesen Port für das Zwischenspeichern von Videos angeben.
- Sie haben Videoquellen hinzugefügt, von denen Sie Videos zwischenspeichern möchten. Standardmäßig werden der Appliance YouTube, Vimeo, Youku, Dailymotion und Metacafe Videoquellen hinzugefügt, aber nur YouTube und Vimeo sind aktiviert. Wenn Sie Videos von einer der anderen Standardquellen zwischenspeichern möchten, müssen Sie diese aktivieren. Wenn Sie neue Videoquellen hinzufügen, können Sie diese beim Hinzufügen aktivieren.
- Neben YouTube, Vimeo, Metacafe, Dailymotion und Youku können Sie zusätzliche Websites, IP-Adressen oder Subnetze als Videoquellen angeben. Beachten Sie, dass diese Websites keine Vermeidungsmechanismen haben sollten, z. B. das Hinzufügen von zufälligen Zeichen zu einer URL.
- Das Video muss sich in einem der anerkannten Videoformate befinden und die folgende Dateierweiterungen haben: .3gp, .avi, .dat, .divx, .dvv, .dv-avi, .flv, .fmv, .h264, .hdmov, .m15, .m1v, .m21, .m2a, .m2v, .m4e, .m4v, .m75, .moov, .mov, .movie, .mp21, .mp2v, .mp4, .mp4v, .mpe, .mpeg, .mpeg4, .mpg, .mpeg2, .mpv, .mts, .ogg, .ogv, .qt, .qtm, .ra, .rm, .ram, .rmd, .rms, .rmvb, .rp, .rv, .swf, .ts, .vfw, .vob, .webm, .wm, .wma, .wmv, and .wtv.

## Unterstützte Plattformen

Die Video-Caching-Funktion wird von den folgenden Appliances unterstützt:

- SD-WAN WANOP 600 Appliance mit 1 Mbit/s und 2 Mbit/s Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 800 Appliance mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 1000 Appliance mit Windows Server, mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 2000 Appliance mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 2000 Appliance mit Windows Server, mit allen Bandbreitenlizenzenmodellen.
- SD-WAN WANOP 3000 Appliance mit allen Modellen der Bandbreitenlizenz.
- SD-WAN WANOP VPX und SD-WAN WANOP VPX für Amazon

## Unterstützte Videoserver

Die Video-Caching-Funktion wird von Adobe Flash Media Server 4.5 oder höher unterstützt. Darüber hinaus wird jeder Videoserver, der Videos über HTTP als statische Links dient, für Video-Caching unterstützt.

## Unterstützte Bereitstellungsmodi

Video-Caching wird in Inline, Inline innerhalb von VLAN-Trunk-Ports, Virtual Inline und WCCP-Bereitstellungsmodi unterstützt.

## Überlegungen zur Verwendung der Video-Caching-Funktion

Im Folgenden sind einige Punkte zu beachten, wenn Sie die Video-Caching-Funktion verwenden.

- Wenn eine der unterstützten Websites die Darstellung von Inhalten ändert, wird der Vorteil für die Videozwischenspeicherung für diese Websites möglicherweise erst erreicht, wenn die Richtliniendatei für Videozwischenspeicherung aktualisiert wurde. Für solche gelegentlichen Änderungen stellt Citrix eine aktualisierte Videocaching-Richtliniendatei bereit. Informationen zur Verwendung finden Sie unter Aktualisieren der Richtliniendatei für Videozwischenspeicherung.
- Einige Videowebsites verwenden möglicherweise unterschiedliche Dateiformate für dasselbe Video, je nach Betriebssystem oder Browser, der für den Zugriff auf das Video verwendet wird. Dies kann zu einem Cache-Fehlern führen.

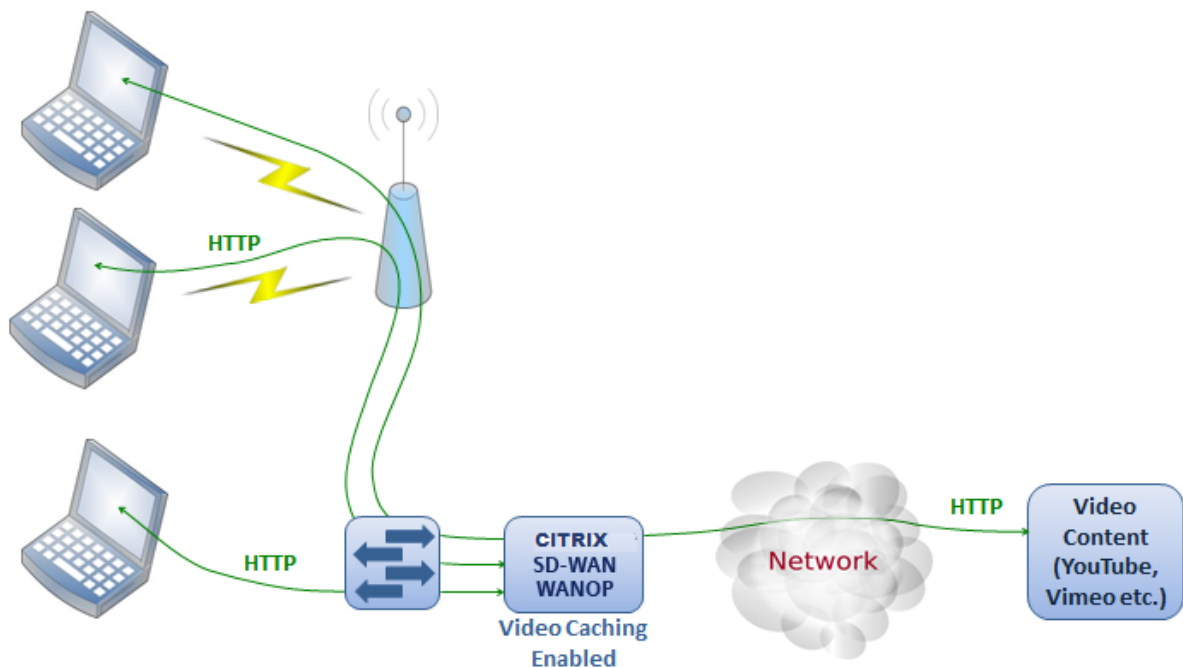
- Einige Videowebsites wie YouTube passen sich den Netzwerkbedingungen an. Die Qualität eines Videos kann daher von den Netzwerkbedingungen zum Zeitpunkt des Zwischenspeichers abhängen.

## Video-Caching-Szenarien

April 19, 2021

Sie können Video-Caching auf Citrix SD-WAN WANOP Appliance in den folgenden Szenarien bereitstellen:

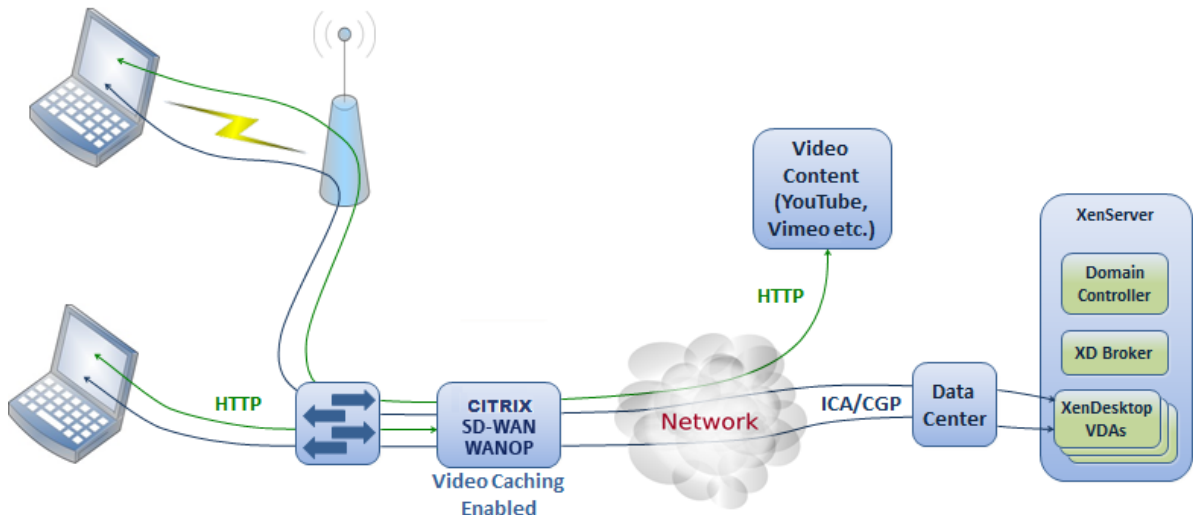
### Zugang zu Zweigstellen



In diesem Anwendungsfall greifen Benutzer über die Webbrowser auf ihren Computern auf das Internet zu. Diese Anfragen, die Videoinhalte von einer aktivierten Site wie Vimeo betreffen, werden auf der lokalen Citrix SD-WAN WANOP-Appliance zwischengespeichert. Jeder nachfolgende Zugriff auf dasselbe Video führt zu Cache-Treffern auf der lokalen Appliance, sodass das Video mit LAN-Geschwindigkeit und ohne Wartezeiten auf den Remoteserver übertragen werden kann.

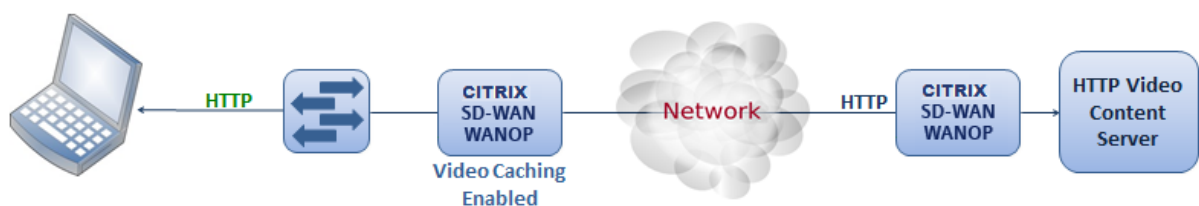
Im Gegensatz zu anderen Citrix SD-WAN WANOP-Funktionen, die den Datenverkehr zwischen gepaarten Geräten beschleunigen, ist diese Funktion eine Single-Ended-Operation, die nur die lokale Appliance mit Zugriff auf die Video-Website benötigt.

## Zweigstelle mit Citrix Virtual Apps and Desktops Benutzern, die HDX MediaStream Flash-Umleitung verwenden



HDX-Flash-Umleitung ist ein Feature der Citrix Virtual Apps and Desktops. Anstatt das Video auf den remoten virtuellen Desktops, die im Internet des Servers oder im Datacenter angezeigt werden, wiederzugeben, werden Flash-Videos über dieses Feature in das lokale System getunnelt. Das Video wird auf den eigentlichen Client-Computer gestreamt und auf dem eigentlichen Client über das Internet der Zweigstelle gerendert. Die Aktivierung der Video-Caching-Funktion auf der branchenseitigen Citrix SD-WAN WANOP-Appliance kann Benutzern ein deutlich verbessertes Seherlebnis bieten. Darüber hinaus verringert die Aktivierung der Funktion den Bandbreitenbedarf für Streaming-Videos.

## Enterprise HTTP-Videowebserver



In diesem Anwendungsfall greifen Benutzer über das Rechenzentrum auf die Videowebserver zu. Wenn Sie die Video-Caching-Funktion auf der branchenseitigen Citrix SD-WAN WANOP-Appliance aktivieren, wird die Benutzeranfrage aus dem Cache der branchenseitigen Citrix SD-WAN WANOP-Appliance bedient. Dies trägt dazu bei, den Netzwerkverkehr zum Rechenzentrum Citrix SD-WAN WANOP Appliance zu reduzieren. Infolgedessen kann die Bandbreite des Rechenzentrums Citrix SD-WAN WANOP Appliance verwendet werden, um den Datenverkehr für andere Branchen zu

bedienen.

## Konfigurieren der Videozwischenspeicherung

April 19, 2021

Sie können die Video-Caching-Funktion entweder über die grafische Benutzeroberfläche von Citrix SD-WAN WANOP oder über die Befehlszeilenschnittstelle konfigurieren. Standardmäßig ist die Appliance so konfiguriert, dass Videos von YouTube und Vimeo zwischengespeichert werden. Youku, Metacafe und Dailymotion sind standardmäßig auf der Appliance konfiguriert. Alles, was Sie tun müssen, ist sie zu aktivieren. Sie können Videowebsites hinzufügen, z. B. eine interne Website mit Video-Tutorials oder andere Informationen.

### Hinweis

Videozwischenspeicherung einer optionalen Funktion, die standardmäßig nicht aktiviert ist. Sie müssen es nur aktivieren, wenn Sie über einen beträchtlichen HTTP-Videoverkehr verfügen.

## Voraussetzungen

Um die Videozwischenspeicherung auf der Appliance zu konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie haben die entsprechende IP-Adresse für den beschleunigten Bridge-Port konfiguriert, den Sie für die Videozwischenspeicherung verwenden möchten.
- Sie können das APA/APB-Gateway von der Appliance aus pingen.
- Die Details des DNS-Servers sind korrekt.
- Die Appliance kann den DNS-Namen `www.citrix.com` auflösen.
- Die Citrix SD-WAN WANOP apX IP-Adresse hat einen HTTP-Zugang in Ihrem Unternehmensnetzwerk.
- Wenn die Appliance zwischen den Trunk-Ports von zwei Netzwerkgeräten bereitgestellt wird, müssen Sie auf der Seite Netzwerkkonfiguration die VLAN-ID mit der IP-Adresse angeben, die die Appliance zum Senden von HTTP-Anforderungen verwendet.
- Für **Dienstklassen** Web (Internet) und **Web (Privat)** sollte die Einstellung **Acceleration Policy** nicht auf **None** festgelegt sein.

## Video-Caching-Funktion aktivieren

Bevor Sie die Video-Caching-Funktion verwenden können, müssen Sie sie aktivieren.

So aktivieren Sie das Video-Caching:

### 1. Navigieren Sie zu **Konfiguration**

**Appliance-Einstellungen > Netzwerkkadapter**, überprüfen Sie im Abschnitt **Verwaltungseinstellungen**, und stellen Sie sicher, dass die Details des primären DNS-Servers korrekt sind und die Appliance den DNS-Namen `www.Citrix.com` auflösen kann. Klicken Sie auf das Symbol **Bearbeiten**, um die Einstellungen zu ändern.

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN WANOP 10.2 interface. The left sidebar lists various settings, with 'Network Adapters' selected. The main content area is titled 'Network Adapters' and contains two sections: 'Management Settings' and 'Network Adapters'.

**Management Settings:**

- Host Name\*: `vpx-175`
- ☐ DHCP for DNS
- Primary DNS Server: `10.102.29.16`
- Secondary DNS Server: `10.102.29.70` (with a help icon)
- Buttons: **Save**, **Cancel**

**Network Adapters:**

Below the 'Edit' button is a table listing the configured network adapters.

Name	Status	DHCP	IPv4 Address	IPv4 Gateway	IPv6 Address	IPv6 Gateway	SSH	Web	VLAN	VLAN Group
apA	Enabled	Disabled	192.168.10.20/24	192.168.10.1	::	::	Enabled	Enabled	Disabled	0
Primary	Enabled	Disabled	10.102.203.175/24	10.102.203.1	::	::	Enabled	Enabled	Disabled	0

### 2. Navigieren Sie zu **Konfiguration > Einheiteninstellungen > Netzwerkkadapter**. Wählen Sie im Abschnitt **Netzwerkkadapter** ein Beschleunigungspaar (zum Beispiel APA) aus und klicken Sie auf **Bearbeiten**.

Stellen Sie sicher, dass die für das beschleunigte Paar angegebenen IP-Adressen, Netzwerkmaske und Standard-Gateway -IP-Adressen korrekt sind.

**Modify Adapter**

**Modify Adapter**

Name

apA

☒ Enabled

☐ DHCP for IPv4 Address

IPv4 Address/MaskBits\*

10.102.29.88/32

IPv4 Gateway

10.102.29.1

IPv6 Address/Prefixlength

::

IPv6 Gateway

::

**Management Access**

☒ SSH

☒ Web

**VLAN**

☐ VLAN

Save

Close

3. Navigieren Sie zur Seite **Konfiguration > Einheiteneinstellungen > Features**, und aktivieren Sie die Funktion **Videozwischenspeicherung**.

Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Ja**.

Name	State	Status
Traffic Processing	Disabled	License is not available
Traffic Acceleration	Enabled	Disabled - due to disabled traffic processing
Traffic Shaping	Enabled	Disabled - due to disabled traffic processing
Traffic Bridging	Enabled	Enabled
IPv6 Acceleration	Enabled	Disabled - due to disabled traffic processing
AppFlow	Enabled	Enabled
RPC Over HTTP	Enabled	Disabled - due to disabled traffic processing
Native Mapi	Enabled	Disabled - due to disabled traffic processing
ICA Multi-stream	Disabled	Disabled
MAPI Cross Protocol Optimization	Disabled	Disabled
SCPS	Disabled	Disabled
Secure Partner	Disabled	Disabled
SNMP	Enabled	Enabled
SSH Access	Enabled	Enabled
SSL Optimization	Enabled	Disabled - due to disabled traffic processing
Syslog	Enabled	Enabled
User Data Store Encryption	Disabled	Disabled
<b>Video Caching</b>	<b>Disabled</b>	<b>Disabled</b>
NetScaler SD-WAN WANOP Client	Enabled	Disabled - Requires IP configuration
WCCP	Enabled	Disabled - due to disabled traffic processing
CIFS Protocol Optimization	Disabled	Disabled - due to disabled traffic processing

### Hinweis

Der Dienst wird neu gestartet und eine neue Zwischenspeicherpartition wird erstellt. Wenn Sie das Feature zum ersten Mal auf der Appliance aktivieren, wird eine neue Partition erstellt, indem der Speicherplatz, der einer anderen festplattenbasierten Komprimierung zugewiesen ist, reduziert wird. Der datenträgerbasierte Komprimierungsverlauf wird zurückgesetzt und vorhandene Verbindungen werden beendet.

4. Alternativ können Sie zu **Konfiguration > Optimierungsregeln > Video-Caching** navigieren und auf **Aktivieren** klicken.

### Hinzufügen von Videowebsites

Die Appliance ist so konfiguriert, dass sie Videos von YouTube und Vimeo zwischenspeichert und teilweise so konfiguriert ist, dass sie Videos von Youku, Metacafe und Dailymotion zwischenspeichert. Um Videos von einer der drei letztgenannten Sites zwischenzuspeichern, müssen Sie die Site aktivieren.



Ein Video von einer aktivierten Website wird zwischengespeichert, sobald ein Benutzer darauf zugreift. Sie können zusätzliche Videowebsites konfigurieren, für die keine URL-Umschreibung erforderlich ist, indem Sie ihre Hostnamen oder IP-Adressen zur Liste Videoquellen auf der Appliance hinzufügen. Sie können auch benutzerdefinierte Sites einschließen, die keine Cache-Vermeidungsmechanismen aufweisen.

Sie müssen diese Videoquellen aktivieren, bevor die Appliance Videos von ihnen zwischenspeichern kann.

Die Videozwischenspeicherung verwendet Videoquellen für den Konfigurationsworkflow. Wenn Sie eine der Videoquellen mit einem Hostnamen oder einem Website/Hostnamen konfigurieren, führt die Appliance den gesamten HTTP-Datenverkehr durch, der durch die Appliance fließt. Wenn Sie jedoch alle Videoquellen nur mit IP-Adressen konfigurieren, wird von der Appliance nur diese IP-Adressen proxys und zwischengespeichert. Unabhängig davon, ob Sie Hostnamen oder IP-Adressen verwenden, stellen Sie sicher, dass Sie diese Videoquellen deaktivieren, wenn Ihre Organisation den Zugriff auf die YouTube-, Vimeo-, Dailymotion-, Metacafe- und Youku-Websites nicht zulässt.

#### So aktivieren Sie eine Videoquelle:

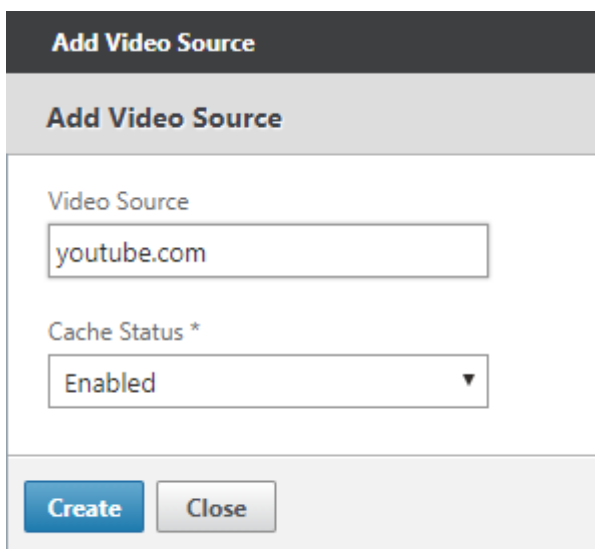
1. Navigieren Sie zu **Konfiguration > Optimierungsregeln > Videozwischenspeicherung > Videoquellen**.
2. Wählen Sie eine Videoquelle aus der Liste aus, klicken Sie auf **Ändern**.

3. Wählen Sie im Dropdown-Feld **Cache-Status** die Option **Aktivieren** aus, und klicken Sie auf **Speichern**.

#### So fügen Sie eine Videoquelle hinzu:

1. Navigieren Sie zu **Konfiguration\*\*> Optimierungsregeln\*\*Video-CachingVideoquellen\*\*** und klicken Sie auf **\*\*Hinzufügen**.

2. Geben Sie im Feld **Videoquelle** den Website-Namen oder die IP-Adresse des Webserver ein, den Sie der Videoquellliste hinzufügen möchten.
3. Stellen Sie in der Liste **Cachestatus** sicher, dass **Aktiviert** ausgewählt ist. Sie können in dieser Liste **Deaktiviert** auswählen, wenn Sie die Videozwischenspeicherung für diese Site zu einem späteren Zeitpunkt aktivieren möchten.



The screenshot shows a web-based dialog box titled "Add Video Source". Inside the dialog, there is a section with the same title. Below this, there are two input fields. The first is labeled "Video Source" and contains the text "youtube.com". The second is labeled "Cache Status \*" and is a dropdown menu currently showing "Enabled". At the bottom of the dialog, there are two buttons: a blue "Create" button and a grey "Close" button.

4. Klicken Sie auf **Erstellen**.

Um eine Videoquelle zu löschen, wählen Sie sie in der Liste **Videoquellen** aus und klicken Sie auf **Löschen**.

## Video Vorbevölkerung

April 19, 2021

Eine Citrix SD-WAN WANOP-Appliance kann Videos von Ihrem internen Videoserver herunterladen und zwischenspeichern, bevor sie von jedem Benutzer angezeigt werden. Diese Funktion ist nützlich, wenn Sie sicherstellen möchten, dass alle Benutzer die gleichen Vorteile haben (z. B. bei der Wiedergabe eines Selbsttrainings-Videos, das zu einem bestimmten Zeitpunkt geplant ist). Sie können statische URLs planen, von denen Sie Videos abrufen möchten.

Die abgerufenen Videos werden im Video-Cache gespeichert. Sobald ein Benutzer eine Anfrage für die URL sendet, wird das Video aus dem Cache bereitgestellt, selbst für den ersten Zugriff auf das Video.

**Um Videos im Voraus abzurufen, können Sie folgende Aufgaben ausführen:**

- Geben Sie eine URL an, von der Sie Videos im Voraus zwischenspeichern möchten.
- Planen Sie Datum und Uhrzeit, zu dem die Videos zwischengespeichert werden sollen.
- Planen Sie ein Intervall, in dem Sie die Videos zwischenspeichern möchten.
- Verwalten Sie die Einträge, die Sie der Liste hinzugefügt haben.

Um ein Video im Voraus herunterzuladen und zwischenzuspeichern, müssen Sie den absoluten Pfad für die URL eines bestimmten Videos oder eines Videoordners angeben, in dem die Verzeichnisindizierung aktiviert ist.

#### **Hinweis**

Wenn Sie nur einen Eintrag zu den Videovorbevölkerungsaufgaben hinzufügen, wird das zugehörige Video heruntergeladen und zwischengespeichert. Wenn ein Client jedoch auf das Video zugreift, wird es vom Videoserver bedient und erhält keine Caching-Vorteile. Um sicherzustellen, dass der Client Vorteile für die Zwischenspeicherung erhält, müssen Sie den Videoserver oder die IP-Adresse, die in der Vorbevölkerungsaufgabe verwendet wird, der Liste der Videoquellen hinzufügen.

#### **So fügen Sie eine URL hinzu, um Videos im Voraus zwischenzuspeichern:**

1. Navigieren Sie zu **Konfiguration > Video-Caching > Vorausfüllen**, und klicken Sie auf **Hinzufügen**.

**Add Prepopulation Entry**

**Add Prepopulation Entry**

Name\*

Example

URL\*

http://example.com/ ?

Interface\*

apA ▼

State

☒ Enable ☐ Disable

Schedule

☒ Now ☐ Later

Repeat\*

Only Once ▼

Create Close

2. Geben Sie im Feld **Name** einen Namen an, mit dem Sie den Eintrag für das Vorauffüllen identifizieren können.
3. Geben Sie im Feld **URL** die URL an, von der Sie ein oder mehrere Videos zwischenspeichern möchten. Die URL kann für ein bestimmtes Video oder einen Videosever sein. Stellen Sie sicher, dass Sie eine vollständige URL oder einen Videoordner angeben.
4. Wählen Sie im Feld **Schnittstelle** den beschleunigten Bridgeport aus, um Videos von der URL herunterzuladen.
5. Setzen Sie **Status** auf **Aktivieren**, um Statusinformationen zu erhalten. Die verschiedenen Zustände und ihre Beschreibung sind in der folgenden Tabelle dargestellt.
6. Sie können Videos von der URL direkt auf die Appliance herunterladen und zwischenspeichern oder sie zu einem geplanten Zeitpunkt herunterladen.
7. Klicken Sie auf **Erstellen**.

In der folgenden Tabelle werden die Statusmeldungen beschrieben:

Status	Beschreibung
Konfiguriert	Abrufen von Video zum Zwischenspeichern, bevor die erste Ansicht für die URL konfiguriert ist und eine neue Aufgabe hinzugefügt wird.
Verbindungszeitüberschreitungsfehler	Die Verbindung zum Server hat ein Zeitlimit überschritten, und es gibt keine Antwort vom Server.
Fehler 301 - Permanent verschoben	Das heruntergeladene und zwischengespeicherte Video wurde dauerhaft an einen anderen Speicherort verschoben.
Fehler 403 - Verboten	Der Zugriff auf das Video, das heruntergeladen und zwischengespeichert werden soll, wird verweigert.
Fehler 404 - Nicht gefunden	Das heruntergeladene und zwischengespeicherte Video steht unter dem bereitgestellten Link nicht zur Verfügung.
Fehler 504: Server nicht erreichbar	Die angegebene URL ist nicht erreichbar.
x Datei(en) erfolgreich heruntergeladen	Download erfolgreich für die URL, und x Anzahl der Mediendateien werden in den Cache heruntergeladen.
Fehler beim Herunterladen von x von y Dateien	Download fehlgeschlagen für einige der Mediendateien von der URL.
Fehler beim Herunterladen von x Dateien	Es konnte keine Mediendatei von der URL heruntergeladen werden.
Download abgeschlossen	Die Verarbeitung aller URLs für diesen Eintrag ist abgeschlossen.
Ausführen von Download	Der Download wird ausgeführt.
Beginn	Die Appliance hat mit dem Herunterladen von Mediendateien von der URL begonnen.
Diesen Eintrag löschen	Der Eintrag wird aus der Liste der URLs gelöscht.
Verzeichnisliste konnte nicht abrufen	Die Auflistung aus dem angegebenen Remoteverzeichnis konnte nicht abrufen.
Eintrag durch Löschen des Cache-Vorgangs entfernt	Der Eintrag wurde durch den Cache-Vorgang gelöscht.
Aktualisierungsstatus	Die Appliance aktualisiert den Status des Eintrags.

Status	Beschreibung
Verstrichene Planzeit	Der geplante Zeitpunkt, zu dem das entfernte Objekt heruntergeladen werden soll, ist vorbei.
x / y Dateien im Cache	Beim Aktualisieren des Status eines Eintrags hat die Appliance festgestellt, dass x -Anzahl der Dateien außerhalb der y -Anzahl im Cache vorhanden ist.
Schnittstellen-AP x für Video-Caching deaktiviert	Die Bridge-Schnittstelle AP x ist für Video-Caching nicht aktiviert.
Aktualisierungsstatus	Der Status des Eintrags wird aktualisiert.
Fehler 0	Beim Herunterladen der Videos ist ein unbekannter Fehler aufgetreten. Wenden Sie sich an das Citrix Technical Support-Team, um das Problem zu beheben.

## Verwalten der Video-Caching-Vorbevölkerung

Sie können die Video-Caching-Vorbevölkerung verwalten, um zu steuern, wie Sie Videos von den URLs herunterladen und zwischenspeichern möchten. Sie können die folgenden Aufgaben ausführen, um die Vorbevölkerung der Videozwischenspeicherung zu verwalten:

- Starten Sie das Herunterladen von Videos vor oder nach dem geplanten Datum und der Uhrzeit.
- Aktualisieren Sie die URL eines Eintrags.
- Deaktivieren Sie das Zwischenspeichern von Videos aus einem URL-Eintrag.
- Planen Sie das Zwischenspeichern von Videos aus einem URL-Eintrag.
- Aktualisieren Sie eine Schnittstelle für einen URL-Eintrag.
- Aktualisieren Sie den Status eines URL-Eintrags.
- Löschen Sie einen URL-Eintrag.

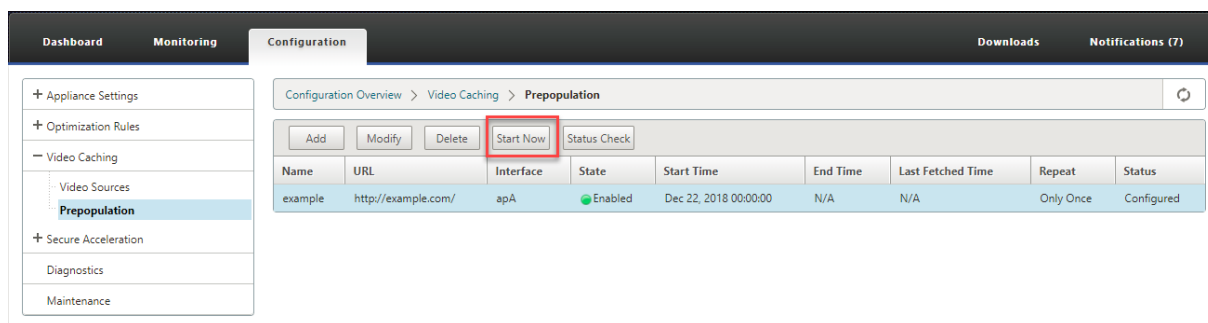
Das folgende Flussdiagramm zeigt die Flusssteuerung der Prozesse, die beim Verwalten verschiedener Aktivitäten der Video-Vorbestückungsfunktion gefolgt sind.



## Videos herunterladen

Wenn technische Probleme mit einer Website oder der von Ihnen hinzugefügten URL das geplante Herunterladen und Zwischenspeichern beeinträchtigen, können Sie jederzeit mit dem Herunterladen und Zwischenspeichern von Videos beginnen.

Um ein Video sofort herunterzuladen und zu cachern, navigieren Sie zu **Konfiguration > Video-Caching > Prepopulation**. Wählen Sie den Eintrag für das Video aus, das Sie zwischenspeichern möchten, und klicken Sie dann auf **Jetzt starten**. Das Aktualisieren des Status des Videos dauert ungefähr eine Minute.



Nachdem Sie auf Jetzt starten geklickt haben, zeigt die Spalte Status den Status der Video-Downloads von der URL an.

### Aktualisieren der URL eines Eintrags vor der Grundgesamtheit

Nachdem Sie im Voraus eine URL hinzugefügt haben, von der Sie Videos herunterladen und zwischenspeichern können, können Sie die URL für optimale Ergebnisse optimieren, z. B. die Neukonfiguration der URL, wenn sich der Speicherort von Videos ändert oder der Name der Mediendatei in der Quelle geändert wird.

#### So aktualisieren Sie eine URL:

1. Navigieren Sie zur Seite **Konfiguration > Video-Caching > Vorbevölkerung**.
2. Wählen Sie den Eintrag aus, den Sie aktualisieren möchten, und klicken Sie auf **Ändern**.
3. Geben Sie im Feld URL die neue URL an.
4. Klicken Sie auf **OK**.

### Deaktivieren der Zwischenspeicherung von Videos von einer URL in einem Eintrag für die Vorbevölkerung

Wenn Sie den Cache regelmäßig mit Videos von einer bestimmten URL vorfüllen möchten, müssen Sie den Eintrag nicht löschen. Sie können es deaktivieren und dann bei Bedarf aktivieren.

#### So deaktivieren Sie einen Eintrag:

1. Navigieren Sie zu **Konfiguration > Video-Caching > Vorausfüllen**.
2. Wählen Sie den Eintrag aus, den Sie aktualisieren möchten, und klicken Sie auf **Ändern**.
3. Wählen Sie unter Status die Option **Deaktivieren** aus.
4. Klicken Sie auf **OK**.



## Planen der Zwischenspeicherung von Videos von einer URL in einem Eintrag für die Vorbevölkerung

Sie können das Datum und die Uhrzeit planen, zu der Sie Videos von der URL auf die Appliance herunterladen und zwischenspeichern möchten. Beispielsweise sollten Sie Videos abrufen, bevor Sie erwarten, dass Benutzer auf sie zugreifen. Das spart nicht nur Speicherplatz, sondern setzt auch die neuesten Versionen der Videos in den Cache.

**So planen Sie das Caching von einer URL aus:**

1. Navigieren Sie zu **Konfiguration > Video-Caching > Vorausfüllen**.
2. Wählen Sie den Eintrag aus, den Sie aktualisieren möchten, und klicken Sie auf **Ändern**.
3. Wählen Sie unter **Zeitplan** die Option **Später** aus.
4. Geben Sie im Feld **Start** das Datum und die Uhrzeit an, zu der Videos von der URL heruntergeladen werden sollen. Das Format für Datum und Uhrzeit ist JJJ-MM-TT HH:MM:SS.
5. Wählen Sie in der Liste **Wiederholen** die Häufigkeit des Herunterladens und Cachens der Videos aus. Es gibt folgende Optionen:
  - **Nur einmal:** Videos von der URL nur einmal herunterladen, zum geplanten Datum und Uhrzeit.
  - **Täglich:** Videos täglich von der URL herunterladen, beginnend mit dem geplanten Datum und der Uhrzeit. Der Download startet jeden Tag zur angegebenen Startzeit.
  - **Wöchentlich:** Laden Sie Videos von der URL einmal pro Woche herunter, beginnend mit dem geplanten Datum und der Uhrzeit. Der Download startet jede Woche an dem Tag und der Uhrzeit, die Sie angeben.
  - **Monatlich:** Laden Sie Videos von der URL einmal im Monat herunter, beginnend mit dem geplanten Datum und der Uhrzeit. Der Download startet jeden Monat an dem Tag und der Uhrzeit, die Sie angeben.
6. Klicken Sie auf **OK**.

## Aktualisieren einer Schnittstelle in einem URL-Eintrag

Wenn Sie mehrere Links im Netzwerk konfiguriert haben, sollten Sie aufgrund der besseren Netzwerkkonnektivität möglicherweise einen bestimmten Link zum Herunterladen von Videos verwenden. Um mehrere Links zu konfigurieren, verwenden Sie die verfügbaren Bridge-Ports, wie APA und aPb Bridged Ports. Sie können diese Ports verwenden, um Videos für einen URL-Eintrag herunterzuladen.

**So aktualisieren Sie eine Schnittstelle für einen URL-Eintrag:**

1. Navigieren Sie zu **Konfiguration > Video-Caching > Prepopulation**.
2. Wählen Sie den Eintrag aus, den Sie aktualisieren möchten. Klicken Sie dann auf **Ändern**.
3. Wählen Sie in der Liste **Schnittstelle** die Schnittstelle aus, die Sie für den URL-Eintrag verwenden möchten. In der Liste werden die Schnittstellen angezeigt, die auf der Appliance verfügbar und konfiguriert sind.
4. Klicken Sie auf **OK**.

### Aktualisieren des Status eines URL-Eintrags

Im Laufe der Zeit kann sich der Status der zwischengespeicherten Videos ändern. Wenn Sie den Status des Eintrags regelmäßig überprüfen, wird sichergestellt, dass Benutzer beim Zugriff auf Videos keine unerwarteten Ergebnisse erhalten.

**So überprüfen Sie den neuesten Status der Videos, die über eine URL zwischengespeichert wurden:**

1. Navigieren Sie zu **Konfiguration > Video-Caching > Prepopulation**.
2. Wählen Sie den Eintrag aus, für den Sie den Status zwischengespeicherter Videos aktualisieren möchten.
3. Klicken Sie auf **Statusüberprüfung**.

### Löschen eines URL-Eintrags

Wenn Sie keinen URL-Eintrag benötigen, können Sie ihn aus der Liste löschen. Um einen URL-Eintrag zu löschen, wählen Sie den Eintrag aus und klicken Sie auf **Löschen**.

#### Hinweis

Wenn Sie eine Videovorbevölkerungsaufgabe aus der Liste löschen, werden auch die zugehörigen Videoobjekte aus dem Cache entfernt.

## Überprüfen der Videozwischenspeicherung

April 19, 2021

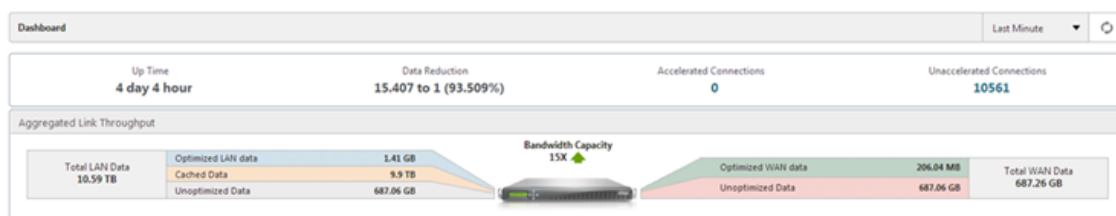
Diagramme und Daten auf der Seite Überwachung, Dashboard und Nutzung helfen Ihnen, die Vorteile Ihrer Videozwischenspeicherkonfiguration zu bewerten. Das Datenreduktionsverhältnis, das sich aus der Videozwischenspeicherung ergibt (ähnlich dem gesamten Komprimierungsverhältnis),

wird im Dashboard, auf der Überwachungsseite des Videocaches und auf der Seite Nutzungsdiagramm angezeigt. Beim Bewegen des Mauszeigers über das Datenreduktionsverhältnis auf der Seite Dashboard wird der Prozentsatz des Caching-Vorteils zusammen mit dem Prozentsatz der Komprimierungsvorteile auf den unterstützten Plattformen angezeigt.

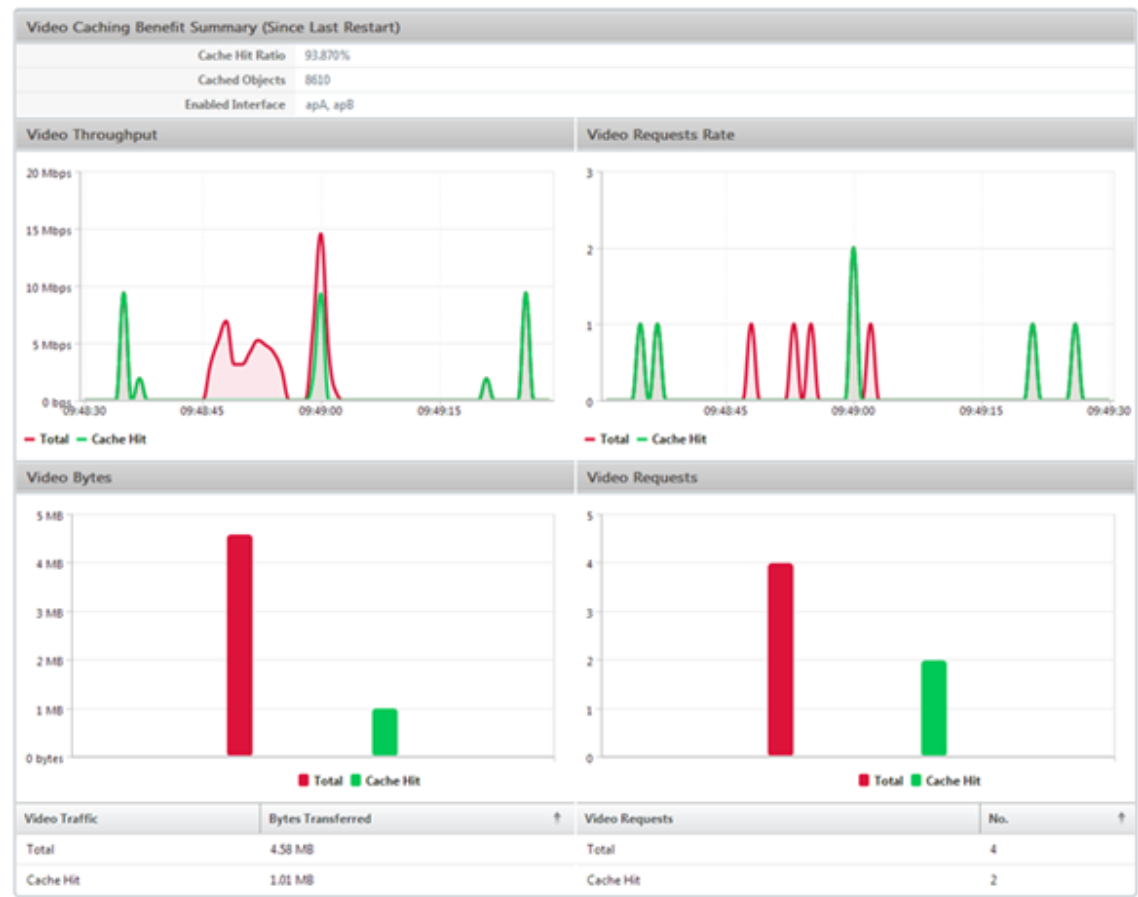
Der Zweck der Zwischenspeicherung besteht nicht nur darin, Bandbreite zu sparen, sondern auch die Leistung zu erhöhen, die Belastung der Videosever zu verringern und die Auswirkungen von Netzwerküberlastung zu verringern.

Die geschätzten WAN-Bandbreiteneinsparungen, die sich aus dem Video-Caching ergeben, werden wie folgt angezeigt:

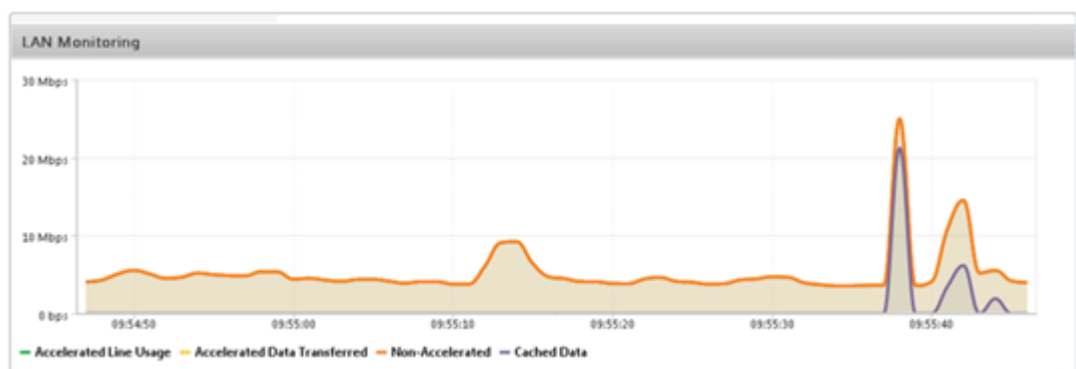
- Auf der Seite Dashboard können Sie den Caching-Vorteil als Prozentsatz anzeigen, indem Sie den Cursor über das Feld Datenreduktion im Dashboard bewegen. Sie können auch die aus dem Cache bereitgestellten Bytes (Cached Data) unter Aggregated Link Throughput anzeigen.



- Auf der Seite **Überwachung > Video-Caching** können Sie die Anzahl der zwischengespeicherten Objekte und die Cache-Trefferquote (in Prozent) anzeigen. Der Balken und die Zeitdiagramme zeigen die Anzahl der Anfragen und Bytes an, die aus dem Cache über 1 Minute, 1 Stunde, 1 Tag, 1 Woche und 1 Monat bereitgestellt werden. Diese Daten werden auch in tabellarischer Form unterhalb des Graphen angezeigt.



- Auf der Seite **Überwachung > Optimierung > Nutzungsdiagramm** können Sie die zwischengespeicherten Daten im Diagramm LAN-Überwachung anzeigen.



- Auf der Seite **Monitoring > Video Caching > \*\*HTTP-Stateliste\*\*** können Sie das verbesserte Cache-Verhalten überwachen. Auf dieser Seite wird der Status von HTTP-Verbindungen in Bezug auf Video-Caching gemeldet.
- Auf der Seite **Überwachung > Optimierung > Verbindungen** können Sie die zwischengespeicherten Verbindungen auf der Registerkarte Beschleunigte Verbindungen anzeigen. Hier werden sowohl Cache-Treffer als auch Cache-Misses angezeigt. Die Cache-Verbindungen

werden hier angezeigt, auch wenn sie nicht beschleunigt werden. Das heißt, die zwischengespeicherten Verbindungen werden hier angezeigt, auch wenn ein Partner Citrix SD-WAN WANOP Appliance nicht an der Verbindung beteiligt ist. Die Spalte **Bandbreiteneinsparungen (%)** zeigt ein Balkendiagramm darüber, wie viel WAN-Bandbreite durch die Transaktion eingespart wurde, sei es durch Caching oder Komprimierung. Das Ziel von Caching und Komprimierung ist zwar die Erhöhung der Geschwindigkeit und Benutzerfreundlichkeit und nicht die Verringerung der Bandbreitenauslastung, aber die Erhöhung der Geschwindigkeit und Benutzerfreundlichkeit sind oft mit der Reduzierung der Bandbreite verbunden. Das heißt, eine 90% ige Bandbreiteneinsparung impliziert eine 10-fache Erhöhung der Geschwindigkeit.

Monitoring > Optimization > Connections > Accelerated Connections

Accelerated ConnectionsUnaccelerated Connections

Action

Details	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)
	172.16.0.50 : 56501	192.229.163.33 : 80	0m 45s	0m 21s	504.95 KB	169.8 to 1 (Disk)	<div><div></div></div> 95.8
	172.16.0.193 : 1060	77.234.41.64 : 80	2h 52m 51s	2m 8s	393.43 KB	1.3 to 1 (Disk)	<div><div></div></div> 15.6
	172.16.0.58 : 55987	104.20.12.86 : 80	18m 23s	0m 5s	327.75 KB	N/A (None)	<div><div></div></div> 0
	172.16.0.50 : 56074	192.229.163.33 : 80	1m 10s	0m 22s	289.83 KB	91.2 to 1 (Disk)	<div><div></div></div> 95.2
	172.16.0.50 : 56092	216.58.216.130 : 80	1m 8s	0m 6s	241.33 KB	90.4 to 1 (Disk)	<div><div></div></div> 94.9
	172.16.0.50 : 56558	31.13.76.100 : 80	0m 42s	0m 3s	156.73 KB	2.8 to 1 (Disk)	<div><div></div></div> 60.6
	172.16.0.50 : 56335	216.58.216.130 : 80	1m 2s	0m 2s	96.65 KB	85.8 to 1 (Disk)	<div><div></div></div> 95.4
	172.16.0.50 : 56559	31.13.76.100 : 80	0m 42s	0m 6s	86.77 KB	2.9 to 1 (Disk)	<div><div></div></div> 62.7

Verwalten von Videozwischenspeicherquellen

April 19, 2021

Sie können Ihre Videoquellen entweder global verwalten, indem Sie globale Einstellungen konfigurieren oder einzeln, indem Sie den Status einer Videoquelle ändern.

Konfigurieren globaler Einstellungen

Globale Einstellungen ermöglichen es Ihnen, die Funktion auf Appliance-Ebene zu konfigurieren. Unabhängig von den hinzugefügten Videoquellen gelten diese Einstellungen für die gesamte Videozwischenspeicherung der Appliance. Sie haben folgende Möglichkeiten:

- Konfigurieren der maximalen Größe der zwischengespeicherten Objekte
- Konfigurieren eines DNS-Suffixes

- Caching-Ports konfigurieren
- Aktualisieren der Videocaching-Richtliniendatei

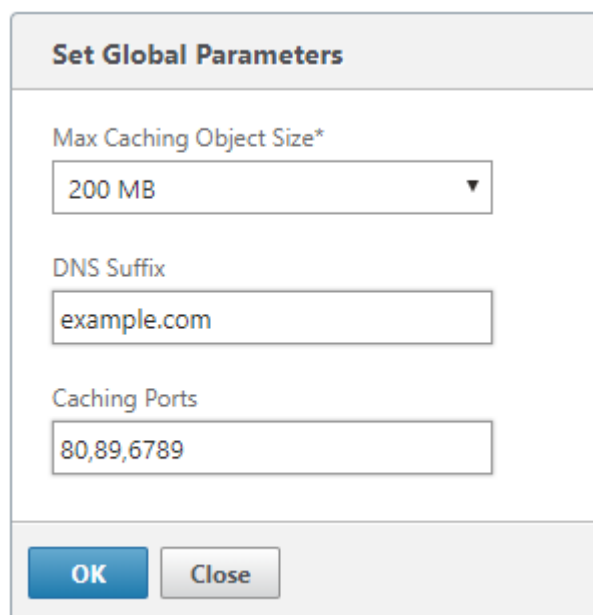
Sie können eine maximale Größe für zwischengespeicherte Objekte konfigurieren. Ein Objekt, das größer als dieser Grenzwert ist, wird nicht zwischengespeichert. Standardmäßig beträgt die maximale Größe des Caching-Objekts 100 MB.

Für URLs, die keine vollständigen Domännennamen enthalten und Domännennamensuffixe zum Hostnamen des Videoservers hinzufügen müssen, ist das Anhängen eines Standarddomännennamens erforderlich, um eine Antwort vom Server zu entnehmen. Wenn Sie z. B. auf das `http://training/CitrixSD-WANWANOP\_VideoCaching.mp4` Video zugreifen, wird davon ausgegangen, dass die Appliance die URL in übersetzt `http://training.example.com/CitrixSD-WANWANOP\_VideoCaching.mp4`. In diesem Fall müssen Sie `example.com` als Domännennamensuffix angeben.

Die Videozwischenspeicherung erfordert eine Portnummer für den HTTP-Video-Server. Der Standardwert ist Port 80. Wenn Ihr HTTP-Video-Server einen anderen Port als diesen bekannten HTTP-Port verwendet, müssen Sie die Portnummer der Liste der Caching-Ports hinzufügen.

#### So konfigurieren Sie globale Einstellungen für Video-Caching:

1. Navigieren Sie zu **Konfiguration > Video-Caching > Globale Parameter festlegen**.



The screenshot shows a dialog box titled "Set Global Parameters". It contains three configuration fields: "Max Caching Object Size\*" with a dropdown menu currently showing "200 MB", "DNS Suffix" with a text input field containing "example.com", and "Caching Ports" with a text input field containing "80,89,6789". At the bottom of the dialog are two buttons: "OK" and "Close".

2. Legen Sie im Feld **MaxCaching-Objektgröße** die maximale Größe für zwischengespeicherte Objekte fest.

Wählen Sie einen Wert aus den verfügbaren Grenzwerten aus. Ein Objekt, das größer als dieses Limit ist, wird nicht zwischengespeichert.

3. Geben Sie im Feld **DNS-Suffix** einen Domännennamen ein, der an URLs angehängt werden soll, die keine vollständigen Domännennamen enthalten und erfordern, dass dem Hostnamen des Videoservers Domännennamensuffixe hinzugefügt werden müssen.
4. Geben Sie im Feld **Caching-Ports** den Port des HTTP-Videoservers ein, um ihn der Liste der Caching-Ports hinzuzufügen. Optional können Sie mehrere Portnummern durch Kommas getrennt hinzufügen.
5. Klicken Sie auf **OK**.

Die Appliance verwendet 10% des zugewiesenen Festplattenspeichers für Verwaltungszwecke. Wenn die Festplattenbelegung 90% des zugewiesenen Festplattenspeichers erreicht, ist dies ein Hinweis darauf, dass der Datenträger voll ist. Um weitere Videoobjekte zwischenspeichern, entfernt die Appliance die am wenigsten verwendeten Objekte aus dem Video-Cache. Sie müssen den Cache nur löschen, wenn der Cache veraltete Videoobjekte bereitstellt.

Um den Videocache zu löschen, navigieren Sie zu **Konfiguration > Video-Caching**, und klicken Sie auf **Video-Cache löschen**.

## WAN-Einsicht

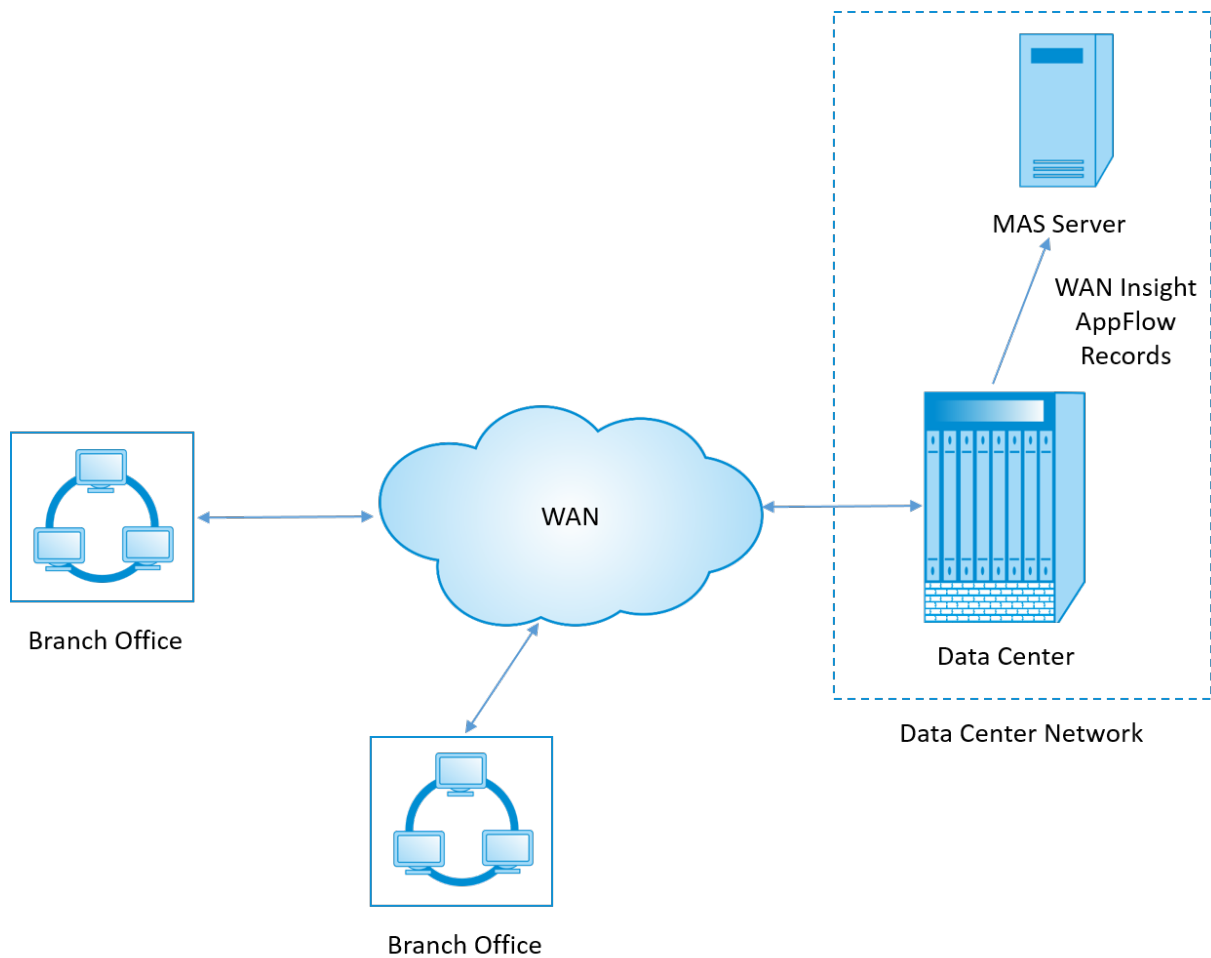
December 14, 2022

Die Citrix SD-WAN WANOP-Appliances optimieren die Bereitstellung einer großen Anzahl von Anwendungen über das WAN, indem sie die Effizienz des Datenflusses über das Netzwerk zwischen dem Rechenzentrum und den Zweigstellen verbessern. WAN-Insight-Analysen ermöglichen Administratoren die einfache Überwachung des beschleunigten und nicht beschleunigten WAN-Datenverkehrs, der zwischen dem Rechenzentrum und den Zweigstellen WAN-Optimierungs-Appliances fließt. WAN Insight bietet Einblick in Clients, Anwendungen und Zweigstellen im Netzwerk, um Netzwerkprobleme effektiv zu beheben. Live- und Verlaufsberichte ermöglichen es Ihnen, Probleme, falls vorhanden, proaktiv anzugehen.

Durch die Aktivierung von Analysen auf der WAN-Optimierungs-Appliance des Rechenzentrums kann Citrix Application Delivery Management (ADM) Daten sammeln und Berichte und Statistiken für das Rechenzentrum und die WAN-Optimierungs-Appliances für Zweigstellen bereitstellen.

### Hinweis

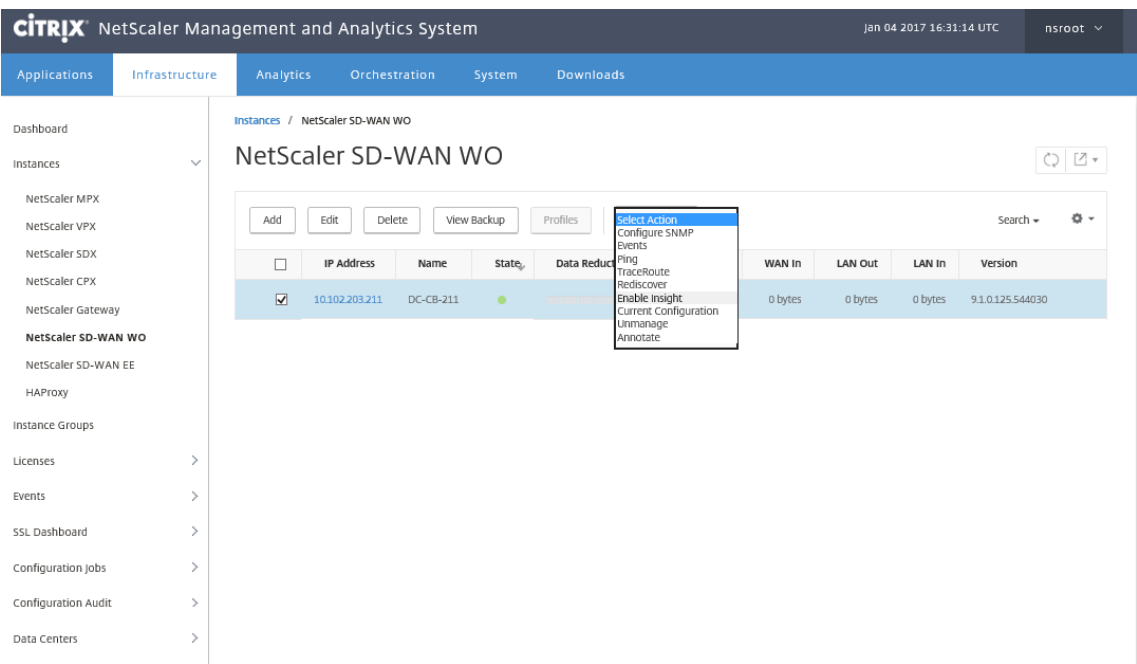
Hinweise zum Hinzufügen einer Instanz finden Sie unter [Hinzufügen von Instanzen zu Citrix ADM](#).



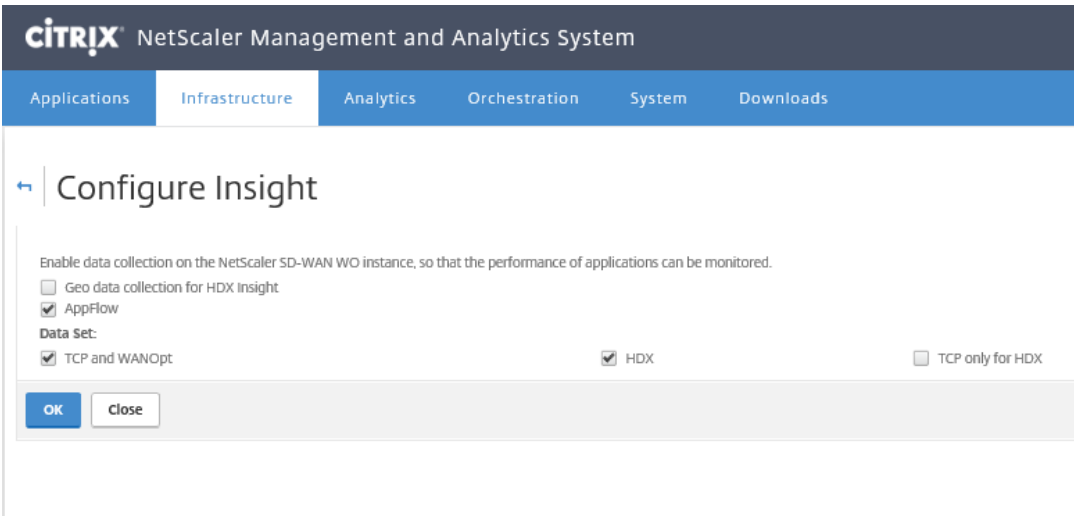
#### Aktivieren von Analysedaten auf dem WAN-Optimierungsgerät:

1. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADM ein (z. B. <http://192.168.100.1>).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldedaten ein.
3. Navigieren Sie zu **Infrastruktur > Instanzen > Citrix SD-WAN WO**, und wählen Sie die WAN-Optimierungs-Appliance für Rechenzentren aus.





4. Klicken Sie in der Dropdown-Option “Aktion” auf “**Enable Insight**”.
5. Wählen Sie die folgenden Parameter nach Bedarf aus:
  - **Geo-Datenerfassung für HDX Insight:** Freigabe der Client-IP-Adresse mit der Google Geo API.
  - **AppFlow:** Beginnt das Sammeln von Daten aus WAN-Optimierungsinstanzen.
  - **TCP und WANOpt:** Bietet TCP- und WANOpt Insight-Berichte.
  - **HDX:** Bietet HDX Insight Berichte.
  - **TCP nur für HDX:** Bietet TCP nur für HDX Insight Berichte.



6. Klicken Sie auf **OK**.

**So zeigen Sie WAN Insight-Berichte an:**

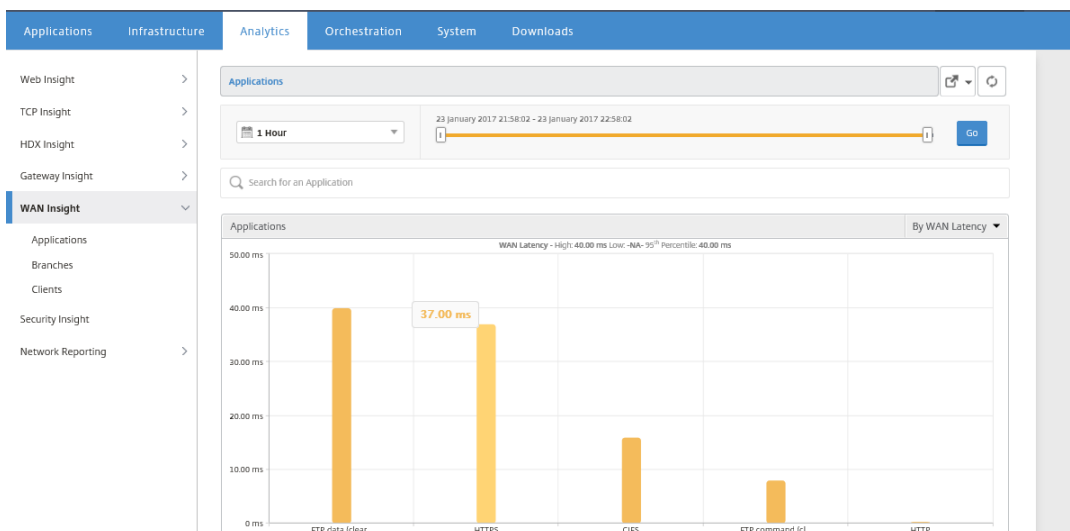
1. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADM ein (z. B. <http://192.168.100.1>).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldedaten ein.
3. Navigieren Sie zu **Analytics > WAN Insight**.

**Hinweis**

Die Option WAN Insight ist erst sichtbar, nachdem Sie Citrix ADM eine SD-WAN-WO-Instanz hinzugefügt haben.

Sie können die folgenden Berichte anzeigen:

- **Anwendungen** - Zeigt die Nutzungs- und Leistungsstatistiken aller Anwendungen für die ausgewählte Dauer an.
- **Branches** - Zeigt die Nutzungs- und Leistungsstatistiken aller WAN-Optimierungs-Branch Appliances an.
- **Clients** - Zeigt die Nutzungs- und Leistungsstatistiken aller Clients an, die auf die WAN-Optimierungsgeräte in jeder Zweigstelle zugreifen.



Die folgenden Metriken werden angezeigt:

| **\*\*Metrik\*\*** | **\*\*Beschreibung\*\*** |

| ———— | ———— |

| Aktive beschleunigte Verbindungen | Anzahl der aktiven WAN-Verbindungen, die beschleunigt werden. |

| Aktive nicht beschleunigte Verbindungen | Anzahl der aktiven WAN-Verbindungen, die nicht beschleunigt werden. |

| WAN-Latenz | Verzögerung in Millisekunden, die der Benutzer während der Interaktion

mit einer Anwendung auftritt. |

| Komprimierungsverhältnis | Verhältnis der Datenkomprimierung zwischen Zweigstelle und Rechenzentrum-Appliances für die ausgewählte Dauer. |

| Gesendete Pakete | Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer über das Netzwerk gesendet hat. |

| Empfangene Pakete | Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer vom Netzwerk empfangen hat. |

| Über WAN gesendete Bytes | Anzahl der Bytes, die die Citrix WAN-Optimierungs-Appliance für die ausgewählte Dauer über das WAN gesendet hat. |

| Über WAN empfangene Bytes | Anzahl der Bytes, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer vom WAN empfangen hat. |

| LAN RTO | Anzahl der Zeitüberschreitungen für die WAN-Optimierungs-Appliance bei der erneuten Übertragung an das LAN für die ausgewählte Dauer. |

| WAN RTO | Anzahl der Zeitüberschreitungen für die WAN-Optimierungs-Appliance bei der erneuten Übertragung an das WAN für die ausgewählte Dauer. |

| Neu übertragene Pakete (LAN) | Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer erneut an das LAN-Netzwerk übertragen hat. |

| Neu übertragene Pakete (WAN) | Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer erneut an das WAN-Netzwerk übertragen hat. |

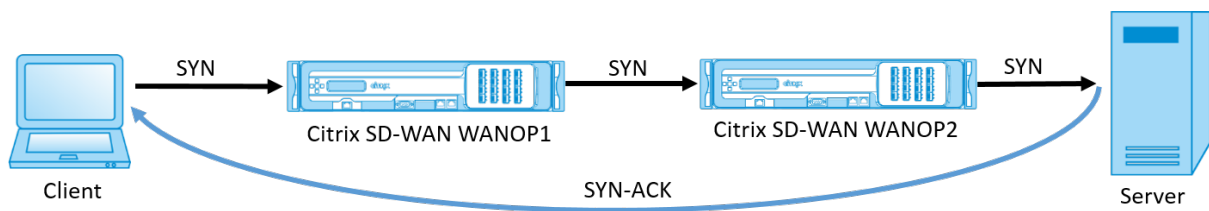
## Asymmetrisches Routing

April 19, 2021

Im Citrix SD-WAN WANOP-Netzwerk erfolgt ein asymmetrisches Routing, wenn Pakete, die für dieselbe TCP-Verbindung von Client zu Server oder Server zum Client fließen, nicht über eine oder beide Client- und serverseitige WANOP-Appliances übergeben werden. Die folgenden Fälle von Asymmetrie werden beobachtet.

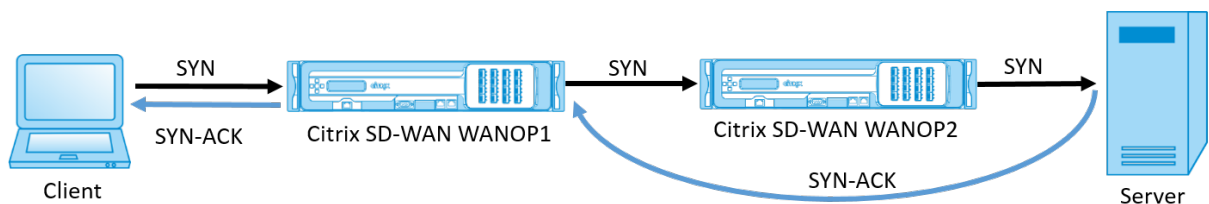
### **Vollständige Asymmetrie:**

Vollständige Asymmetrie tritt auf, wenn Pakete von einem Client zum Server über die clientseitigen und serverseitigen Citrix SD-WAN WANOP-Appliances fließen. Auf dem Rückgabepfad vom Server zum Client nehmen die Pakete jedoch eine andere Route unter Umgehung der Citrix SD-WAN WANOP-Appliances.



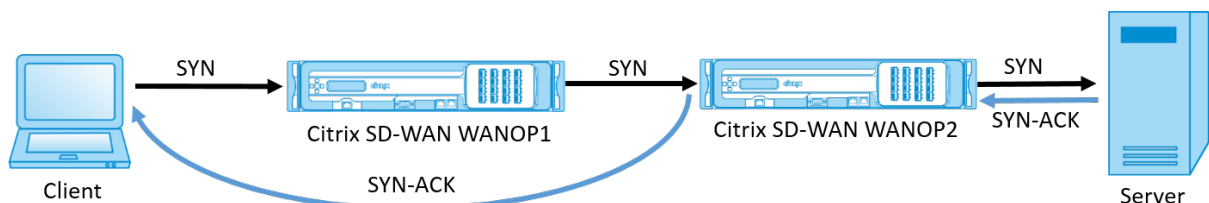
### Serverseitige Asymmetrie:

Serverseitige Asymmetrie tritt auf, wenn Pakete von einem Client zum Server über die clientseitigen und serverseitigen Citrix SD-WAN WANOP-Appliances fließen. Auf dem Rückgabepfad umgehen die Pakete jedoch die serverseitige Citrix SD-WAN WANOP-Appliance, durchlaufen aber die clientseitige Citrix SD-WAN WANOP-Appliance.



### Client-seitige Asymmetrie:

clientseitige Asymmetrie tritt auf, wenn Pakete von einem Client zum Server über die clientseitigen und serverseitigen Citrix SD-WAN WANOP-Appliances fließen. Auf dem Rückgabepfad durchlaufen die Pakete jedoch die serverseitige Citrix SD-WAN WANOP-Appliance, umgehen aber die clientseitige Citrix SD-WAN WANOP-Appliance.



## Asymmetrie im Citrix SD-WAN WANOP-Netzwerk behandeln

Im Citrix SD-WAN WANOP-Netzwerk wird bei vollständiger Asymmetrie die TCP-Verbindung zurückgesetzt. Um TCP-Verbindungsunterbrechungen zu vermeiden und weiterhin nicht beschleunigten Datenverkehr zu senden, wird eine asymmetrische Verbindungsliste in SD-WAN WANOP 10.1 eingeführt. Diese Funktion ist standardmäßig deaktiviert. Sie können diese Funktion sowohl auf den clientseitigen als auch auf den serverseitigen SD-WAN WANOP-Appliances aktivieren.

Beim ersten Erkennen einer asymmetrischen Verbindung wird die TCP-Verbindung zwischen Client und Server zurückgesetzt und ein Eintrag des Tupel wird in der asymmetrischen Verbindungsliste vorgenommen. Das Tupel besteht aus der Client-IP-Adresse und Server-IP-Adresse. Nachfolgende

Verbindungen aus dem Tupel passieren nicht beschleunigt. Das Verbindungstupel verbleibt in der asymmetrischen Verbindungsliste für einen Standardzeitüberschreitungszeitraum von vier Stunden oder bis Symmetrie erkannt wird. Der nicht beschleunigte Pass-Through ist wirksam, bis das Timeout eintritt oder bis die Appliance dynamisch erkennt, dass die Asymmetrie nicht mehr vorhanden ist.

Wenn clientseitige Asymmetrie oder serverseitige Asymmetrie erkannt wird, wird die TCP-Verbindung beibehalten und die Pakete werden standardmäßig nicht beschleunigt durch die Citrix SD-WAN WANOP-Appliance geleitet.

So aktivieren Sie die asymmetrische Verbindungsliste für Citrix SD-WAN WANOP-Appliances:

1. Greifen Sie auf die WANOP CLI-Eingabeaufforderung (WANOP Accelerator/Broker IP) zu.
2. Melden Sie sich mit den folgenden Anmeldeinformationen an:

**Login als:** *cli*\*\*

**Login:** \*\* *admin* \*\*

**Passwort:** \*\* *nsroot* \*\*

#### Hinweis

Das Standardkennwort für admin ist *nsroot*. Wenn Sie das Kennwort geändert haben, verwenden Sie das richtige.

3. Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste.

*Festlegen des Parameters `assyMetricConnectionList.Enable` auf*

#### Hinweis

Sie können den Timeout-Zeitraum gemäß Ihrer Netzwerkanforderung mit dem Befehl *`AssyMetricConnectionList.AutoFlushDuration`* konfigurieren.

Es stehen mehrere Parameter mit Asymmetrieliste zur Verfügung, die basierend auf Ihrer Netzwerkkumgebung auf Anforderung optimiert werden können. Weitere Informationen erhalten Sie von Citrix Customer Support.

## Citrix SD-WAN WANOP-Client-Plug-in

April 19, 2021

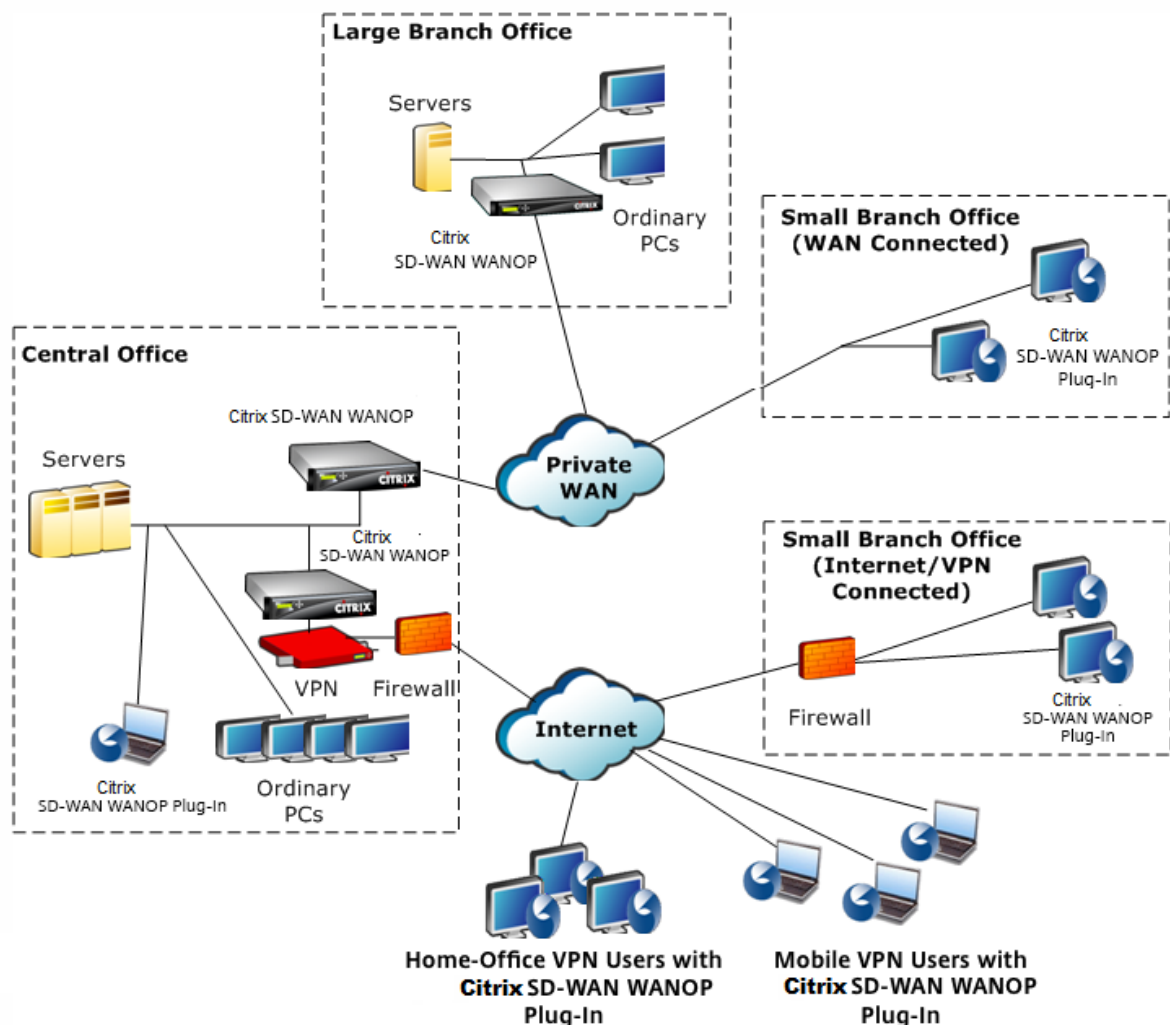
Das Citrix WANOP Client-Plug-in ist ein softwarebasierter Netzwerkbeschleuniger, der auf Windows-Laptops und -Workstations ausgeführt wird und die Beschleunigung überall ermöglicht, nicht nur in

Büros mit WANOP Client-Plug-in-Appliances. Sie verbindet sich mit einer Citrix WANOP-Appliance am anderen Ende der Verbindung.

Die Prinzipien des WANOP Client-Plug-in-Betriebs sind im Allgemeinen identisch mit denen einer WANOP Client-Plug-in-Appliance. Themen, die nicht in der Plug-In-Dokumentation enthalten sind, finden Sie im größeren Dokumentationssatz.

Das Plug-In wird als Standard-Microsoft-Installationsdatei (MSI) verteilt. Die Plug-In-Bereitstellung erfordert eine Plug-in-spezifische Konfiguration der WANOP-Appliances an den anderen Enden der Links. Wenn Sie die MSI-Datei mit den DNS- oder IP-Adressen der WANOP-Appliances und einigen anderen Parametern anpassen, müssen die Benutzer bei der Installation des Plug-Ins auf ihren Windows-Computern keine Konfigurationsinformationen eingeben.

Abbildung 1. Typisches WANOP-Client-Plug-In-Netzwerk, das das WANOP-Client-Plug-In anzeigt



### **Hinweis**

Das Plug-In wird von Citrix Receiver 1.2 oder höher unterstützt und kann von Citrix Receiver verteilt und verwaltet werden.

## **Hardware- und Softwareanforderungen**

April 19, 2021

Auf der Client-Seite der beschleunigten Verbindung wird das WANOP Client-Plug-in auf Windows-Desktop- und Laptop-Systemen unterstützt, aber nicht auf Netbooks oder Thin Clients. Citrix empfiehlt die folgenden Hardwarespezifikationen für den Computer, auf dem das

WANOP Client-Plug-In ausgeführt wird:

- Pentium 4-Klasse CPU
- 2 GB RAM
- 2 GB freier Festplattenspeicher

Das WANOP Client-Plug-In wird auf der Windows 10-Plattform unterstützt und benötigt folgende Systemanforderungen:

- 4 GB RAM
- 10 GB freier Festplattenspeicher

Das WANOP Client-Plug-In wird unter den folgenden Betriebssystemen unterstützt:

- Windows XP-Startseite
- Windows XP Professional
- Windows Vista (alle 32-Bit-Versionen von Home Basic, Home Premium, Business, Enterprise und Ultimate)
- Windows 7 (alle 32-Bit- und 64-Bit-Versionen von Home Basic, Home Premium, Professional, Enterprise und Ultimate)
- Windows 8 (32-Bit- und 64-Bit-Versionen von Enterprise Edition)
- Windows 10 (32-Bit- und 64-Bit-Versionen von Enterprise Edition)

Serverseitig unterstützen derzeit die folgenden Appliances WANOP Client-Plug-in-Bereitstellungen:

- WANOP Client Plug-in VPX
- WANOP Client-Plug-In 2000
- WANOP Client-Plug-In 3000
- WANOP Client-Plug-In 4000
- WANOP Client-Plug-in 5000

## Funktionsweise des WANOP-Plug-ins

April 19, 2021

WANOP Client Plug-in-Produkte verwenden Ihre bestehende WAN/VPN-Infrastruktur. Ein Computer, auf dem das Plug-In installiert ist, greift weiterhin wie vor der Installation des Plug-Ins auf LAN, WAN und Internet zu. Es sind keine Änderungen an Routingtabellen, Netzwerkeinstellungen, Clientanwendungen oder Serveranwendungen erforderlich.

Citrix Access Gateway-VPNs erfordern eine geringe Menge an WANOP Client-Plug-In-spezifischen Konfigurationen.

Es gibt zwei Varianten der Art und Weise, wie Verbindungen durch das Plug-In und die Appliance verarbeitet werden: den

*transparenten Modus* und den

*Redirector-Modus*. Redirector ist ein Legacy-Modus, der für neue Bereitstellungen nicht empfohlen wird.

- **Der transparente Modus** für die Beschleunigung von Plug-in-zu-Appliance ist der Beschleunigung von Appliance-zu-Appliance sehr ähnlich. Die WANOP Client-Plug-In-Appliance muss sich im Pfad befinden, der von den Paketen übernommen wird, wenn sie zwischen dem Plug-In und dem Server unterwegs sind. Wie bei der Appliance-zu-Appliance-Beschleunigung arbeitet der transparente Modus als transparenter Proxy, wobei die Quell- und Ziel-IP-Adresse sowie die Portnummern von einem Ende der Verbindung zum anderen beibehalten werden.
- **Der Umleitungsmodus** (nicht empfohlen) verwendet einen expliziten Proxy. Das Plug-In setzt ausgehende Pakete an die Redirector-IP-Adresse der Appliance um. Die Appliance wiederum liest die Pakete an den Server, während die Rücksendeadresse so geändert wird, dass sie auf sich selbst anstatt auf das Plug-In verweist. In diesem Modus muss die Appliance nicht physisch mit dem Pfad zwischen der WAN-Schnittstelle und dem Server verbunden sein (dies ist die ideale Bereitstellung).

Best Practice: Verwenden Sie den transparenten Modus, wenn Sie können, und den Umleitungsmodus, wenn Sie müssen.

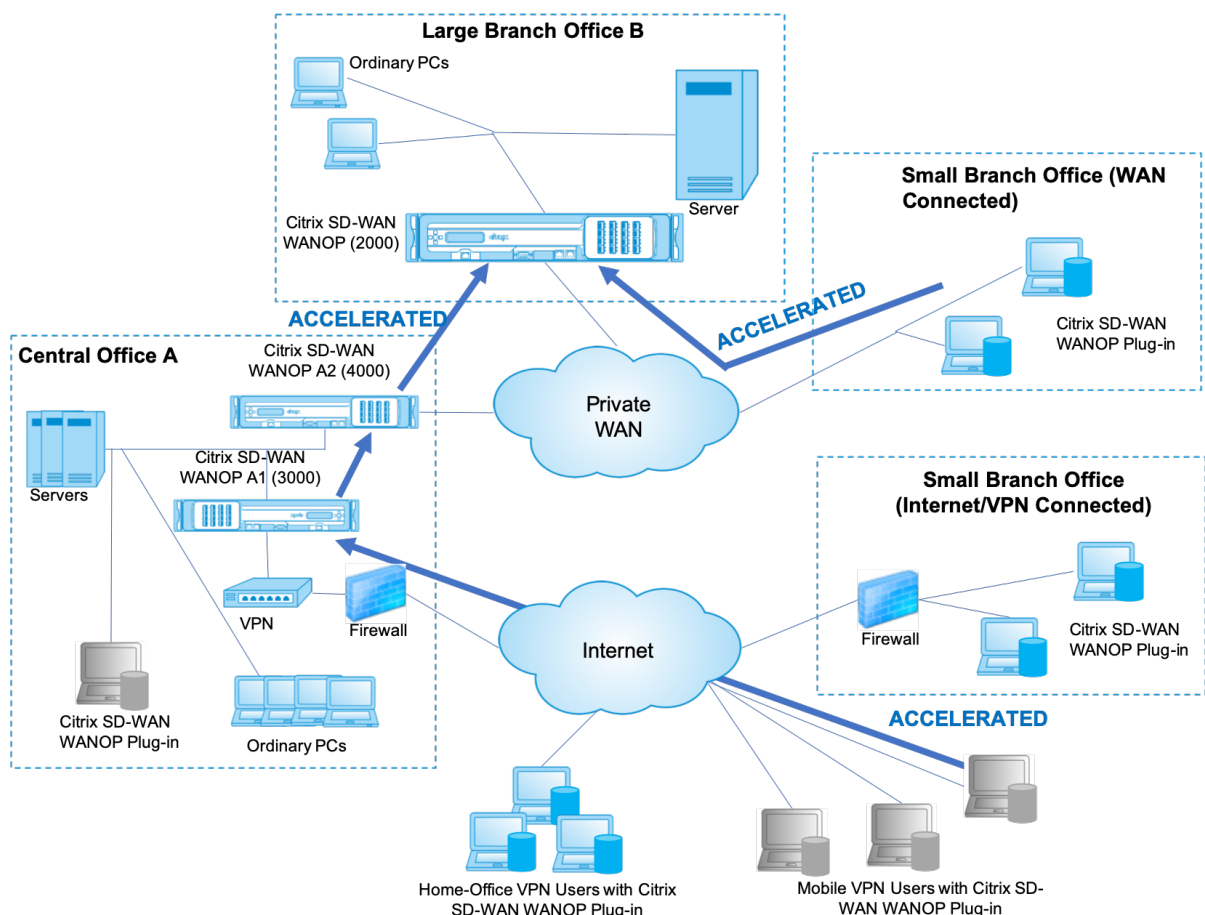


## Transparenter Modus

Im transparenten Modus müssen die Pakete für beschleunigte Verbindungen die Ziel-Appliance passieren, genau wie bei der Beschleunigung von Appliance zu Appliance.

Das Plug-In ist mit einer Liste der Appliances konfiguriert, die für die Beschleunigung verfügbar sind. Es versucht, jede Appliance zu kontaktieren und eine Signalverbindung zu öffnen. Wenn die Signalverbindung erfolgreich ist, lädt das Plug-In die Beschleunigungsregeln von der Appliance herunter, die die Zieladressen für Verbindungen sendet, die die Appliance beschleunigen kann.

Abbildung 1. Transparenter Modus, Hervorhebung von drei Beschleunigungspfaden



### Hinweis

- **Traffic Flow** —Der transparente Modus beschleunigt Verbindungen zwischen einem Citrix WANOP Client Plug-in und einer Plug-in-fähigen Appliance.
- **Lizenzierung** —Appliances benötigen eine Lizenz, um die gewünschte Anzahl von Plug-Ins zu unterstützen. In dem Diagramm muss Citrix SD-WAN WANOP A2 nicht für Plug-in-Beschleunigung lizenziert werden, da Citrix SD-WAN WANOP A1 bietet die Plug-in-Beschleunigung für Standort A.

- **Daisy-Chaining:** Wenn die Verbindung auf dem Weg zur Ziel-Appliance mehrere Appliances durchläuft, muss für die Appliances in der Mitte Daisy-Chaining aktiviert sein, oder die Beschleunigung wird blockiert. In dem Diagramm wird der Datenverkehr von Home-Office- und mobilen VPN-Benutzern, die für große Zweigstellen B bestimmt sind, von Citrix SD-WAN WANOP B beschleunigt. Damit dies funktioniert, müssen Citrix SD-WAN WANOP A1 und A2 über Daisy-Chaining aktiviert sein.

Wenn das Plug-In eine neue Verbindung öffnet, werden die Beschleunigungsregeln konsultiert. Wenn die Zieladresse einer der Regeln entspricht, versucht das Plug-In, die Verbindung zu beschleunigen, indem Beschleunigungsoptionen an das anfängliche Paket in der Verbindung (das SYN-Paket) angefügt werden. Wenn eine dem Plug-In bekannte Appliance Beschleunigungsoptionen an das SYN-ACK-Antwortpaket anfügt, wird eine beschleunigte Verbindung mit dieser Appliance hergestellt.

Die Anwendung und der Server wissen nicht, dass die beschleunigte Verbindung hergestellt wurde. Nur die Plug-In-Software und die Appliance wissen, dass eine Beschleunigung stattfindet.

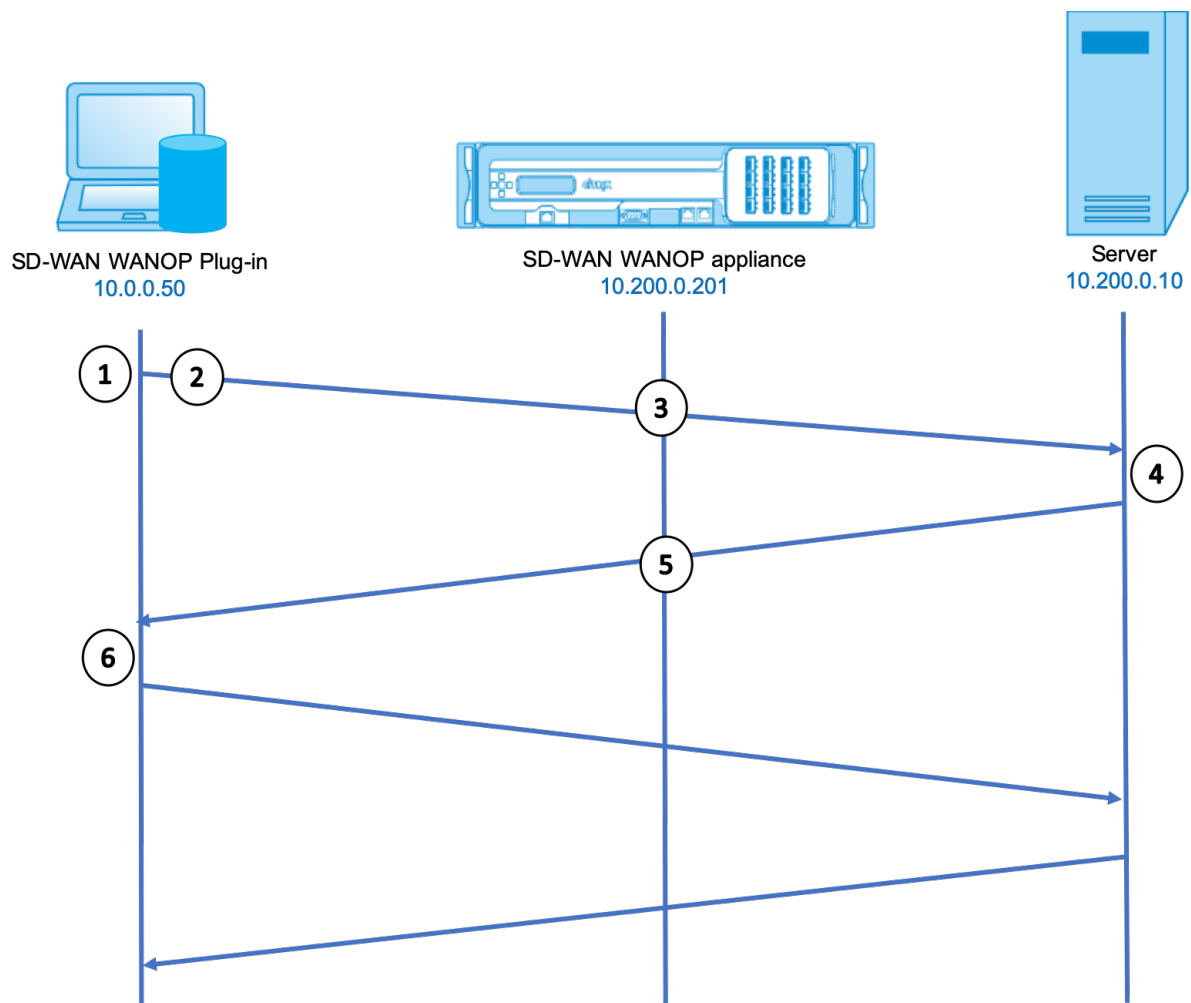
Der transparente Modus ähnelt der Beschleunigung von Appliance-zu-Appliance, ist jedoch nicht identisch mit dieser. Die Unterschiede sind:

- **Nur Clientinitiierte Verbindungen:** Der transparente Modus akzeptiert nur Verbindungen, die vom Plug-In-ausgestatteten System initiiert werden. Wenn Sie ein Plug-In-ausgestattetes System als Server verwenden, werden Serververbindungen nicht beschleunigt. Die Appliance-to-Appliance-Beschleunigung hingegen funktioniert unabhängig davon, welche Seite der Client ist und welche der Server ist. (Active-Mode FTP wird als Sonderfall behandelt, da die Verbindung, die die vom Plug-In angeforderte Datenübertragung initiiert, vom Server geöffnet wird.)
- **Signalverbindung** —Der transparente Modus verwendet eine Signalverbindung zwischen Plug-In und Appliance für die Übertragung von Statusinformationen. Die Beschleunigung von Appliance-zu-Appliance erfordert keine Signalverbindung, außer für sichere Peer-Beziehungen, die standardmäßig deaktiviert sind. Wenn das Plug-In eine Signalverbindung nicht öffnen kann, versucht es nicht, Verbindungen über die Appliance zu beschleunigen.
- **Daisy-Chaining** —Für eine Appliance, die sich im Pfad zwischen einem Plug-In und der ausgewählten Ziel-Appliance befindet, müssen Sie im Menü **Konfiguration: Tuning** die Daisy-Chaining-Funktion aktivieren.

Der transparente Modus wird häufig mit VPNs verwendet. Das WANOP Client-Plug-In ist mit den meisten IPSec- und PPTP-VPNs sowie mit Citrix Access Gateway VPNs kompatibel.

Die folgende Abbildung zeigt den Paketfluss im transparenten Modus. Dieser Paketfluss ist fast identisch mit der Beschleunigung von Appliance-zu-Appliance, mit der Ausnahme, dass die Entscheidung, ob versucht wird, die Verbindung zu beschleunigen, auf Beschleunigungsregeln basiert, die über die Signalverbindung heruntergeladen werden.

Abbildung 2. Paketfluss im transparenten Modus



1. Die Anwendung des Benutzers öffnet eine TCP-Verbindung zum Server und sendet ein TCP SYN-Paket.

**SRC: 10.0.0.50, Dst: 10.200.0.10**

2. Das WANOP-Plug-In sucht die Zieladresse und sieht, dass es mit einem Subnetz übereinstimmt, das von der Appliance beschleunigt wird. Es fügt WANOP-Optionen an den TCP-Header des SYN-Pakets. Es werden keine Adressen geändert.

**SRC: 10.0.0.50, Dst: 10.200.0.10**

3. Die Appliance notiert die SYN-Optionen und erkennt, dass es sich um eine beschleunigbare Verbindung handelt. Es entfernt die Optionen aus dem Paket und ermöglicht es, an den Server zu übergeben. Es werden keine Adressen geändert.

**SRC: 10.0.0.50, Dst: 10.200.0.10**

4. Der Server akzeptiert die Verbindung und antwortet mit einem TCP SYN-ACK-Paket.

**SRC: 10.200.0.10, Dst: 10.0.0.50**

5. Die Appliance kennzeichnet das SYN-ACK-Paket mit einer TCP-Header-Option, die anzeigt, dass die Beschleunigung stattfindet.

**SRC: 10.200.0.10, Dst: 10.0.0.50**

6. Das WANOP Plug-in empfängt das SYN-ACK-Paket. Die Optionen in den Paketheadern zeigen an, dass die Verbindung beschleunigt wird. Das Plug-in entfernt die Optionen und übergibt das SYN-ACK-Paket an die Anwendung. Die Verbindung ist nun vollständig geöffnet und beschleunigt.

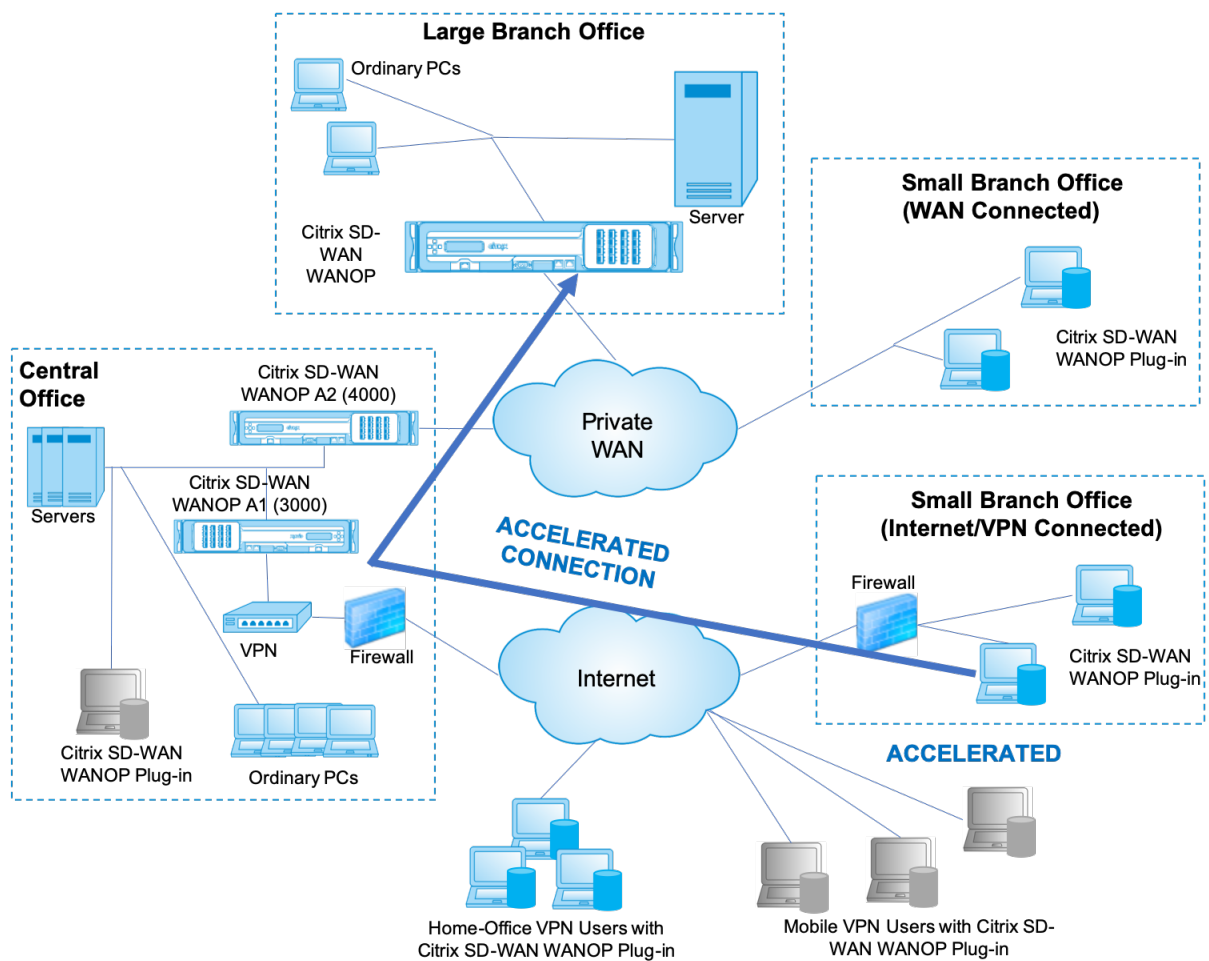
## Umleitungsmodus

Der Umleitungsmodus funktioniert auf folgende Weise anders als der transparente Modus:

- Die WANOP Client-Plug-In-Software leitet die Pakete um, indem sie explizit an die Appliance adressieren.
- Daher muss die Umleitungsmodus-Appliance nicht den gesamten WAN-Link-Datenverkehr abfangen. Da beschleunigte Verbindungen direkt an sie adressiert werden, können sie überall platziert werden, solange sie sowohl vom Plug-In als auch vom Server erreicht werden können.
- Die Appliance führt ihre Optimierungen durch und leitet dann die Ausgabepakete an den Server um, wobei die Quell-IP-Adresse in den Paketen durch eine eigene Adresse ersetzt wird. Aus Sicht des Servers stammt die Verbindung von der Appliance.
- Der Rückkehrverkehr vom Server wird an die Appliance adressiert, die Optimierungen in Rückwärtsrichtung durchführt und die Ausgabepakete an das Plug-In weiterleitet.
- Die Zielporthnummern werden nicht geändert, sodass Netzwerküberwachungsanwendungen den Datenverkehr weiterhin klassifizieren können.

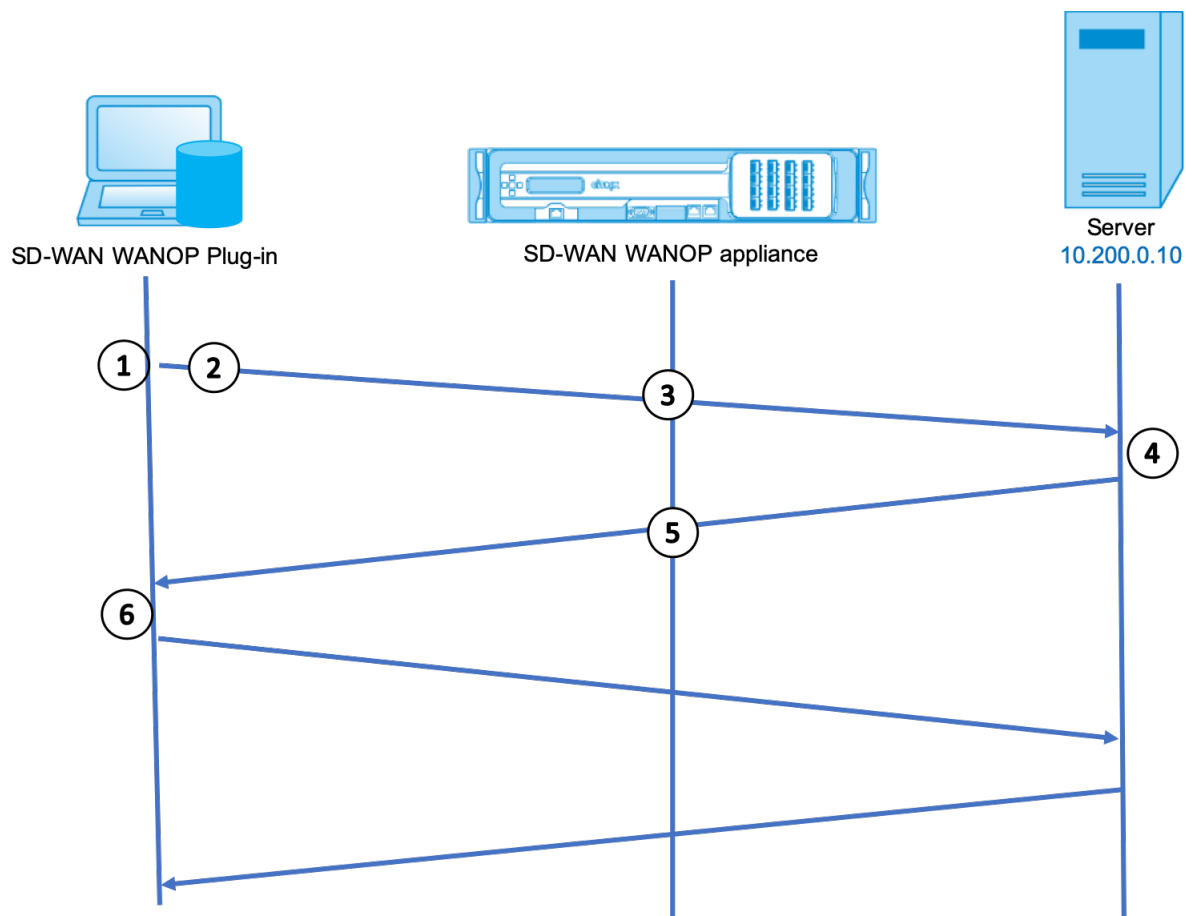
Die folgende Abbildung zeigt, wie der Redirector-Modus funktioniert.

Abbildung 1. Umleitungsmodus



Die folgende Abbildung zeigt den Paketfluss und die Adressenzuordnung im *Redirector-Modus*.

Abbildung 2. Paketfluss im Umleitungsmodus



1. Die Anwendung des Benutzers öffnet eine TCP-Verbindung zum Server und sendet ein TCP SYN-Paket.

**SRC: 10.0.0.50, Dst: 10.200.0.10**

2. Citrix SD-WAN WANOP Plug-In sucht die Zieladresse und entscheidet, die Verbindung mit der Appliance unter 10.200.0.201 umzuleiten.

**SRC: 10.0.0.50, dst: 10.200.0.201**

(10.200.0.10 wird in einem TCP-Optionsfeld beibehalten. Optionen 24-31 werden für verschiedene Parameter verwendet.)

3. Die Appliance akzeptiert die Verbindung und leitet das Paket an den Server weiter (unter Verwendung der Zieladresse aus dem TCP-Optionsfeld) und gibt sich selbst als Quelle an.

**SRC: 10.200.0.201, DST: 10.200.0.10**

4. Der Server akzeptiert die Verbindung und antwortet mit einem TCP SYN-ACK-Paket.

**SRC: 10.200.0.10, DST: 10.200.0.201**

5. Die Appliance schreibt die Adressen neu und leitet das Paket an das Plug-in weiter (Platzieren der Serveradresse in ein Optionsfeld).

**SRC: 10.200.0.201, Dst: 10.0.0.50**

6. Die Verbindung ist nun vollständig geöffnet. Der Client und der Server senden Pakete über die Appliance hin und her.

Während die Adressen im Redirector-Modus alvert werden, sind die Desitnationsportnummern nit (obwohl die kurzlebige Portnummer sein kann). Die Daten sind nicht gekapselt. Der Umleitungsmodus ist ein Proxy, kein Tunnel.

Es gibt keine 1:1 -Beziehung zwischen Paketen (obwohl am Ende die empfangenen Daten immer identisch sind mit den gesendeten Daten). Durch die Komprimierung können viele Eingabepakete in ein einzelnes Paket reduziert werden. CIFS-Accerlation führt spekulative Read-Ahead- und White-Behind Operationen durch. Auch, wenn Pakete zwischen appliace und dem Reperter-Plug-in gelöscht werden, wird die erneute Übertragung von der Appliance, noyt dem Server, mit erweiterten Wiederherstellungsalgorithmen behandelt.

## So wählt das Plug-In eine Appliance aus

Jedes Plug-In ist mit einer Liste der Appliances konfiguriert, die es kontaktieren kann, um eine beschleunigte Verbindung anzufordern.

Die Appliances verfügen jeweils über eine Liste von *Beschleunigungsregeln*, d. h. eine Liste von Zieladressen oder Ports, zu denen die Appliance beschleunigte Verbindungen herstellen kann. Das Plug-In lädt diese Regeln von den Appliances herunter und gleicht die Zieladresse und den Port jeder Verbindung mit dem Regelsatz der einzelnen Appliance ab. Wenn nur eine Appliance eine bestimmte Verbindung beschleunigen kann, ist die Auswahl einfach. Wenn mehr als eine Appliance die Verbindung beschleunigen kann, muss das Plug-In eine der Appliances auswählen.

Die Regeln für die Geräteauswahl lauten wie folgt:

- Wenn alle Appliances, die zur Beschleunigung der Verbindung anbieten, Umleiter-Modus-Appliances sind, wird die ganz links in der Appliance-Liste des Plug-Ins ausgewählt. (Wenn die Appliances als DNS-Adressen angegeben wurden und der DNS-Eintrag mehrere IP-Adressen aufweist, werden auch diese von links nach rechts gescannt.)
- Wenn einige Appliances, die zur Beschleunigung der Verbindung anbieten, den Redirector-Modus verwenden und einige den transparenten Modus verwenden, werden die Appliances im transparenten Modus ignoriert, und die Auswahl erfolgt über die Appliances im Umleitungsmodus.
- Wenn alle Appliances, die zur Beschleunigung der Verbindung anbieten, den transparenten Modus verwenden, wählt das Plug-In keine bestimmte Appliance. Es initiiert die Verbindung mit den SYN-Optionen des WANOP Client-Plug-Ins, und je nachdem, welche Kandidateneinheit dem zurückgebenden SYN-ACK-Paket entsprechende Optionen anfügt, wird verwendet.

Dadurch kann sich die Appliance, die tatsächlich dem Datenverkehr entspricht, mit dem Plug-In identifizieren. Das Plug-In muss jedoch über eine offene Signalverbindung mit der antwortenden Appliance verfügen, da sonst keine Beschleunigung stattfindet.

- Einige Konfigurationsinformationen gelten als global. Diese Konfigurationsinformationen stammen von der ganz links angezeigten Appliance in der Liste, für die eine Signalverbindung geöffnet werden kann.

## **Bereitstellen von Appliances für die Verwendung mit Plug-Ins**

April 19, 2021

Die Clientbeschleunigung erfordert eine spezielle Konfiguration auf der WANOP Client-Plug-in-Appliance. Weitere Überlegungen sind die Platzierung der Appliance. Plug-Ins werden normalerweise für VPN-Verbindungen bereitgestellt.

### **Verwenden Sie nach Möglichkeit eine dedizierte Appliance**

Der Versuch, dieselbe Appliance sowohl für die Plug-In-Beschleunigung als auch für die Verbindungsbeschleunigung zu verwenden, ist oft schwierig, da die beiden Anwendungen manchmal dazu führen, dass sich die Appliance an verschiedenen Stellen im Rechenzentrum befindet, und die beiden Anwendungen können unterschiedliche Regeln der Service-Klasse aufrufen.

Darüber hinaus kann eine einzelne Appliance als Endpunkt für die Plug-In-Beschleunigung oder als Endpunkt für die Standort-zu-Standort-Beschleunigung dienen, kann aber nicht beide Zwecke gleichzeitig für dieselbe Verbindung dienen. Wenn Sie eine Appliance sowohl für die Plug-In-Beschleunigung für Ihr VPN als auch für die Standort-zu-Standort-Beschleunigung auf ein Remote-Rechenzentrum verwenden, erhalten Plug-In-Benutzer daher keine Standort-zu-Standort-Beschleunigung. Die Schwere dieses Problems hängt davon ab, wie viele der von Plug-In-Benutzern verwendeten Daten von Remotesites stammen.

Da die Ressourcen einer dedizierten Appliance nicht zwischen Plug-In- und Standort-zu-Site-Anforderungen aufgeteilt sind, bieten sie jedem Plug-In-Benutzer mehr Ressourcen und damit eine höhere Leistung.

### **Inline-Modus verwenden, wenn möglich**

Eine Appliance sollte am selben Standort wie die von ihr unterstützte VPN-Einheit bereitgestellt werden. Typischerweise sind die beiden Einheiten in Einklang miteinander. Eine Inline-Bereitstellung bi-



et die einfachste Konfiguration, die meisten Funktionen und die höchste Leistung. Für beste Ergebnisse sollte die Appliance direkt mit der VPN-Einheit in Einklang stehen.

Appliances können jedoch einen beliebigen Bereitstellungsmodus verwenden, ausgenommen den Gruppenmodus oder den Hochverfügbarkeitsmodus. Diese Modi eignen sich sowohl für Appliance-zu-Appliance-Beschleunigung als auch für Client-zu-Appliance-Beschleunigung. Sie können allein (*transparenter Modus*) oder in Kombination mit dem Redirector-Modus verwendet werden.

## **Platzieren Sie die Appliances in einem sicheren Teil Ihres Netzwerks**

Eine Appliance hängt genauso von Ihrer vorhandenen Sicherheitsinfrastruktur ab wie Ihre Server. Es sollte auf der gleichen Seite der Firewall (und VPN-Einheit, falls verwendet) wie die Server platziert werden.

## **NAT-Probleme vermeiden**

Network Address Translation (NAT) auf der Plug-In-Seite wird transparent behandelt und ist kein Problem. Auf der Appliance-Seite kann NAT lästig sein. Wenden Sie die folgenden Richtlinien an, um eine reibungslose Bereitstellung sicherzustellen:

- Stellen Sie die Appliance in denselben Adressraum wie die Server ein, sodass alle Adressänderungen, die zum Erreichen der Server verwendet werden, auch auf die Appliance angewendet werden.
- Greifen Sie niemals auf die Appliance zu, indem Sie eine Adresse verwenden, die die Appliance nicht mit sich selbst verknüpft.
- Die Appliance muss auf die Server zugreifen können, indem sie dieselben IP-Adressen verwenden, unter denen Plug-In-Benutzer auf dieselben Server zugreifen.
- Kurz gesagt, wenden Sie NAT nicht auf die Adressen von Servern oder Appliances an.

## **Softboost Modus auswählen**

Wählen Sie auf der Seite Einstellungen konfigurieren: Bandbreitenverwaltung die Option Softboost. Softboost ist die einzige Art der Beschleunigung, die mit dem WANOP Client Plug-In Plug-In unterstützt wird.

## **Definieren von Plug-In-Beschleunigungsregeln**

Die Appliance verwaltet eine Liste von Beschleunigungsregeln, die den Clients mitteilen, welcher Datenverkehr beschleunigt werden soll. Jede Regel gibt eine Adresse oder ein Subnetz sowie einen

Portbereich an, den die Appliance beschleunigen kann.

**Was beschleunigt werden soll:** Die Wahl des Datenverkehrs, der beschleunigt werden soll, hängt von der Verwendung der Appliance ab:

- **VPN-Beschleuniger** - Wenn die Appliance als VPN-Beschleuniger verwendet wird und der gesamte VPN-Datenverkehr durch die Appliance fließt, sollte der gesamte TCP-Datenverkehr unabhängig vom Ziel beschleunigt werden.
- **Umleitungsmodus** - Im Gegensatz zum transparenten Modus ist eine Appliance im Redirector-Modus ein expliziter Proxy, der dazu führt, dass das Plug-In seinen Datenverkehr an die Redirector-Modus-Appliance weiterleitet, selbst wenn dies nicht wünschenswert ist. Beschleunigung kann kontraproduktiv sein, wenn der Client Datenverkehr an eine Appliance weiterleitet, die vom Server entfernt ist, insbesondere wenn diese Dreiecksroute eine langsame oder unzuverlässige Verbindung einführt. Daher empfiehlt Citrix, Beschleunigungsregeln so zu konfigurieren, dass eine bestimmte Appliance nur ihre eigene Site beschleunigt.
- **Sonstige Verwendung** - Wenn das Plug-In weder als VPN-Beschleuniger noch im Redirector-Modus verwendet wird, sollten die Beschleunigungsregeln Adressen enthalten, die remote zu den Benutzern und lokal in Rechenzentren sind.

**Definieren der Regeln** - Definieren Sie Beschleunigungsregeln auf der Registerkarte **Konfiguration: WANOP-Client-Plug-in: Beschleunigungsregeln**.

Regeln werden in der Reihenfolge ausgewertet, und die Aktion (Beschleunigen oder Ausschließen) wird von der ersten Übereinstimmungsregel übernommen. Damit eine Verbindung beschleunigt werden kann, muss sie mit einer Beschleunigungsregel übereinstimmen.

Die Standardaktion besteht darin, nicht zu beschleunigen.

1. Auf der Registerkarte Konfiguration: WANOP Plug-In: Beschleunigungsregeln:
  - Fügen Sie für jedes lokale LAN-Subnetz, das von der Appliance erreicht werden kann, eine Beschleunigungsregel hinzu. Das heißt, klicken Sie auf **Hinzufügen**, wählen Sie **Beschleunigen** aus, und geben Sie die Subnetz-IP-Adresse und -Maske ein.
  - Wiederholen Sie dies für jedes Subnetz, das lokal auf der Appliance ist.
2. Wenn Sie einen Teil des eingeschlossenen Bereichs ausschließen müssen, fügen Sie eine Ausschlussregel hinzu und verschieben Sie sie über die allgemeinere Regel. Beispielsweise sieht 10.217.1.99 wie eine lokale Adresse aus. Wenn es sich tatsächlich um den lokalen Endpunkt einer VPN-Einheit handelt, erstellen Sie eine Ausschlussregel für sie in einer Zeile oberhalb der Beschleunigungsregel für 10.217.1.0/24.
3. Wenn Sie Beschleunigung nur für einen einzelnen Port verwenden möchten (nicht empfohlen), z. B. Port 80 für HTTP, ersetzen Sie das Platzhalterzeichen im Feld Ports durch die spezifische

Portnummer. Sie können zusätzliche Ports unterstützen, indem Sie zusätzliche Regeln hinzufügen, eine pro Port.

4. Im Allgemeinen sollten Sie enge Regeln (in der Regel Ausnahmen) vor allgemeinen Regeln auflisten.
5. Klicken Sie auf **Anwenden**. Änderungen werden nicht gespeichert, wenn Sie von dieser Seite weg navigieren, bevor Sie sie anwenden.

## IP-Port-Nutzung

Verwenden Sie die folgenden Richtlinien für die Verwendung von IP-Ports:

- **Ports, die für die Kommunikation mit dem WANOP Client Plug-in verwendet werden**—Das Plug-In führt einen Dialog mit der Appliance über eine Signalverbindung, die standardmäßig auf Port 443 (HTTPS) ist, der über die meisten Firewalls erlaubt ist.
- **Ports, die für die Kommunikation mit Servern verwendet werden**—Die Kommunikation zwischen dem WANOP Client-Plug-in und der Appliance verwendet dieselben Ports, die der Client für die Kommunikation mit dem Server verwenden würde, wenn das Plug-in und die Appliance nicht vorhanden wären. Das heißt, wenn ein Client eine HTTP-Verbindung an Port 80 öffnet, stellt er eine Verbindung mit der Appliance an Port 80 her. Die Appliance wiederum kontaktiert den Server an Port 80.

Im Redirector-Modus wird nur der bekannte Port (d. h. der Zielport auf dem TCP SYN-Paket) beibehalten. Der flüchtige Port bleibt nicht erhalten. Im transparenten Modus bleiben beide Ports erhalten.

Die Appliance geht davon aus, dass sie mit dem Server an jedem vom Client angeforderten Port kommunizieren kann, und der Client geht davon aus, dass er mit der Appliance an jedem gewünschten Port kommunizieren kann. Dies funktioniert gut, wenn die Appliance denselben Firewallregeln wie die Server unterliegt. Wenn dies der Fall ist, gelingt jede Verbindung, die in einer direkten Verbindung erfolgreich wäre, in einer beschleunigten Verbindung.

## Verwendung von TCP-Optionen und Firewalls

Die Parameter des WANOP Client-Plug-Ins werden in den TCP-Optionen gesendet. TCP-Optionen können in jedem Paket auftreten und sind garantiert in den SYN- und SYN-ACK-Paketen vorhanden, die die Verbindung herstellen.

Die Firewall darf TCP-Optionen im Bereich von 24-31 (Dezimalzahl) nicht blockieren, da sonst keine Beschleunigung möglich ist. Die meisten Firewalls blockieren diese Optionen nicht. Eine Cisco PIX- oder ASA-Firewall mit Version 7.x-Firmware kann dies jedoch standardmäßig tun, und daher müssen Sie die Konfiguration anpassen.

## Anpassen der MSI-Datei des Plug-Ins

April 19, 2021

Sie können Parameter in der WANOP-Client-Plug-in-Verteilungsdatei ändern, die im standardmäßigen Microsoft Installer (MSI) Format vorliegt. Die Anpassung erfordert die Verwendung eines MSI-Editors.

### Hinweis

Die geänderten Parameter in Ihrem bearbeiteten MSI-Datei gilt nur für neue Installationen. Wenn vorhandene Plug-In-Benutzer auf eine neue Version aktualisieren, werden ihre vorhandenen Einstellungen beibehalten. Daher sollten Sie nach dem Ändern der Parameter Ihren Benutzern empfehlen, die alte Version zu deinstallieren, bevor Sie die neue installieren.

### Best Practices:

Erstellen Sie einen DNS-Eintrag, der in die nächste Plug-in-fähige Appliance aufgelöst wird. Definieren Sie beispielsweise Repeater.MyCompany.com und lassen Sie es auf Ihre Appliance auflösen, wenn Sie nur über eine Appliance verfügen. Oder, wenn Sie beispielsweise fünf Appliances haben, haben Repeater.MyCompany..com Auflösung zu einer Ihrer fünf Appliances, wobei die Appliance aufgrund der Nähe zum Client oder zur VPN-Einheit ausgewählt wurde. Beispielsweise sollte ein Client, der eine Adresse verwendet, die mit einem bestimmten VPN verknüpft ist, Repeater.MyCompany.com mit der IP-Adresse der WANOP Client Plug-In-Appliance aufgelöst werden, die mit diesem VPN verbunden ist. Bauen Sie diese Adresse in Ihre Plug-In-Binärdatei mit einem MSI-Editor wie Orca ein. Wenn Sie Appliances hinzufügen, verschieben oder entfernen, wird durch Ändern dieser einzelnen DNS-Definition auf dem DNS-Server automatisch die Appliance-Liste der Plug-Ins aktualisiert.

Der DNS-Eintrag kann auch auf mehrere Appliances aufgelöst werden. Dies ist jedoch nicht wünschenswert, wenn alle Appliances identisch konfiguriert sind, da das Plug-In einige Merkmale der Appliance ganz links in der Liste übernimmt und sie global anwendet (einschließlich SSL-Komprimierungsmerkmalen). Dies kann zu unerwünschten und verwirrenden Ergebnissen führen, insbesondere wenn der DNS-Server die Reihenfolge der IP-Adressen für jede Anforderung rotiert.

### Installieren Sie den Orca MSI-Editor:

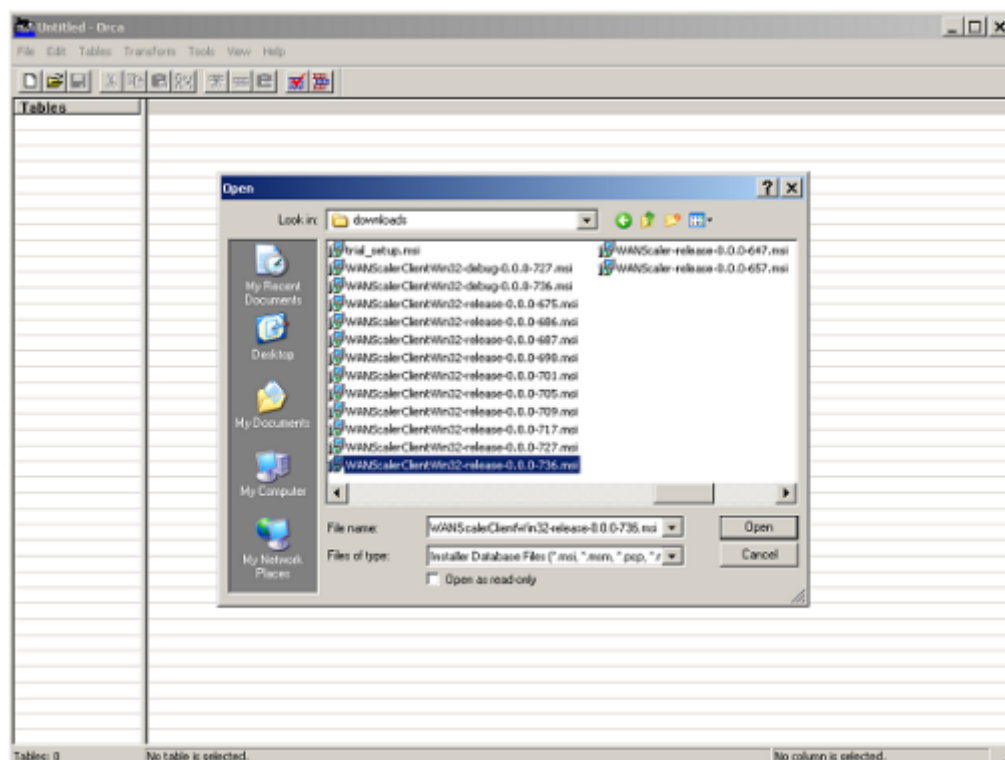
Es gibt viele MSI-Editoren, darunter Orca, das Teil des kostenlosen Plattform-SDK von Microsoft ist und von Microsoft heruntergeladen werden kann.

### So installieren Sie den Orca MSI-Editor:

1. Laden Sie die PSDK-x86.exe Version des SDK herunter und führen Sie es aus. Folgen Sie den Installationsanweisungen.

2. Sobald das SDK installiert ist, muss der Orca-Editor installiert werden. Er ist unter Microsoft Platform SDK\Bin\Orca.Msi. Starten Sie Orca.msi, um den eigentlichen Orca-Editor (orca.exe) zu installieren.
3. **Ausführen von Orca**—Microsoft stellt seine Orca-Dokumentation online bereit. In den folgenden Informationen wird beschrieben, wie Sie die wichtigsten WANOP Client Plug-in-Parameter bearbeiten.
4. Starten Sie Orca mit **Start > Alle Programme > Orca**. Wenn ein leeres Orca-Fenster angezeigt wird, öffnen Sie die MSI-Datei des WANOP Client Plug-in Plug-in mit **Datei > Öffnen**.

**Abbildung 1. Verwenden von Orca**



5. Klicken Sie im Menü **Tabellen** auf **Eigenschaft**. Eine Liste aller bearbeitbaren Eigenschaften der MSI-Datei wird angezeigt. Bearbeiten Sie die in der folgenden Tabelle gezeigten Parameter. Um einen Parameter zu bearbeiten, doppelklicken Sie auf seinen Wert, geben Sie den neuen Wert ein, und drücken Sie die **EINGABETASTE**.

Weitere Informationen finden Sie in der [Tabelle](#)

- a) Klicken Sie im Menü **Tabellen** auf **Eigenschaft**. Eine Liste aller bearbeitbaren Eigenschaften der MSI-Datei wird angezeigt. Bearbeiten Sie die in der folgenden Tabelle gezeigten Parameter. Um einen Parameter zu bearbeiten, doppelklicken Sie auf seinen Wert, geben Sie den neuen Wert ein und drücken Sie die Eingabetaste.

Weitere Informationen finden Sie in der [Tabelle](#)

### Abbildung 2: Bearbeiten von Parametern in Orca:

WANScalerClientWin32-release-0.0.0-736.msi - Orca

File Edit Tables Transform Tools View Help

Tables

- ActionText
- AdminExecuteSequence
- AdminUISequence
- AdminExecuteSequence
- AppSearch
- Binary
- Checkbox
- Component
- Control
- ControlCondition
- ControlEvent
- CreateFolder
- CustomAction
- Dialog
- Directory
- Error
- EventMapping
- Feature
- FeatureComponents
- File
- Icon
- InstallExecuteSequence
- InstallUISequence
- LaunchCondition
- LaunchBox
- Media
- ModuleComponents
- ModuleDependency
- ModuleSignature
- MultiHash
- Property**
- RadioButton
- RegLocator
- Registry
- RemoveFile
- RemoveRegistry
- SelfReg
- ServiceControl
- ServiceInstall
- Shortcut

Property

Property	Value
Manufacturer	Cibix Systems, Inc.
ProductCode	{00E1F262-8EEA-47D1-9901-81D826A97E(CD)}
ProductLanguage	1033
ProductName	Cibix WANScaler Client 0.0.0.736
ProductVersion	0.0.0.736
UpgradeCode	{0DAA63E2-0480-11DA-9903-001DC6E19530}
BUILD_FLAVOR	Release
ALLUSERS	1
ARPPRODUCTNAME	WANScaler Client from Cibix Systems, Inc.
ARPPRODUCTICON	OrbitIcon
ORCAHOST	69.59.175.13
ORCAPORT	443
DISCHARGE	250
DISCHARGE	10000
PRIMARYFOLDER	INSTALLDIR
WIXUI_INSTALLDIR	OrbitData
DefaultUIFont	WixUI_Font_Normal
WixUI_Mode	InstallDir
ARPHOHCOPY	1
WixUI_WelcomeDlg_Next	LicenseAgreementDlg
WixUI_LicenseAgreementDlg_Back	WelcomeDlg
WixUI_LicenseAgreementDlg_Next	InstallDirDlg
WixUI_InstallDirDlg_Back	LicenseAgreementDlg
WixUI_InstallDirDlg_Next	VerifyReadDlg
WixUI_InstallDirDlg_Browse	BrowseDlg
WixUI_VerifyReadDlg_BadRepair	MaintenanceTypeDlg
WixUI_VerifyReadDlg_BadRemove	MaintenanceTypeDlg
WixUI_VerifyReadDlg_BadInstallDir	InstallDirDlg
WixUI_MaintenanceWelcomeDlg_Next	MaintenanceTypeDlg
WixUI_MaintenanceTypeDlg_Repair	VerifyReadDlg
WixUI_MaintenanceTypeDlg_Remove	VerifyReadDlg
WixUI_MaintenanceTypeDlg_Back	MaintenanceWelcomeDlg
ErrorDialog	ErrorDlg
WixUIRPOption	UserRM
SecureCustomProperties	MWERFPRODUCTFOUND;PREVIOUSINSTALLER;PREVIOUSVERSIONINGINSTALL...
DG_DNE_P1_ORDER_REG_VER.70087FC1_0408_4518_9402_44039...	0
DG_BuildNumber.dnorder.70087FC1_0408_4518_9402_440390E...	15349
DG_PkgIdRev.dnorder.ssm.70087FC1_0408_4518_9402_440390...	1
DG_Product_Version.dnorder.70087FC1_0408_4518_9402_44039...	2.22.0.0
APPS TEST	1

Tables: 45 Property: 44 rows Value: Localizable[0]

6. Wenn Sie fertig sind, verwenden Sie den Befehl **Datei: Speichern unter**, um Ihre bearbeitete Datei unter einem neuen Dateinamen zu speichern, z. B. test.msi.

Ihre Plug-In-Software wurde nun angepasst.

## Hinweis

Einige Benutzer haben einen Fehler in orca gesehen, der dazu führt, dass Dateien auf 1 MB abgeschnitten werden. Überprüfen Sie die Größe der gespeicherten Datei. Wenn sie abgeschnitten wurde, erstellen Sie eine Kopie der Originaldatei und überschreiben Sie das Original mit dem Befehl Speichern.

Nachdem Sie die Appliance-Liste mit Orca angepasst und die angepasste MSI-Datei an Ihre Benutzer verteilt haben, muss der Benutzer bei der Installation der Software keine Konfigurationsinformationen eingeben.

## Bereitstellen von Plug-Ins unter Windows

April 19, 2021

Das WANOP Client-Plug-In ist eine ausführbare Microsoft-Installationsdatei (MSI), die Sie herunterladen und installieren, wie bei jedem anderen webverteilten Programm. Rufen Sie diese Datei im MyCitrix-Abschnitt der Citrix.com -Site ab.

#### **Hinweis**

Die Benutzeroberfläche des WANOP Client-Plug-ins bezeichnet sich selbst als Citrix Acceleration Plug-in Manager.

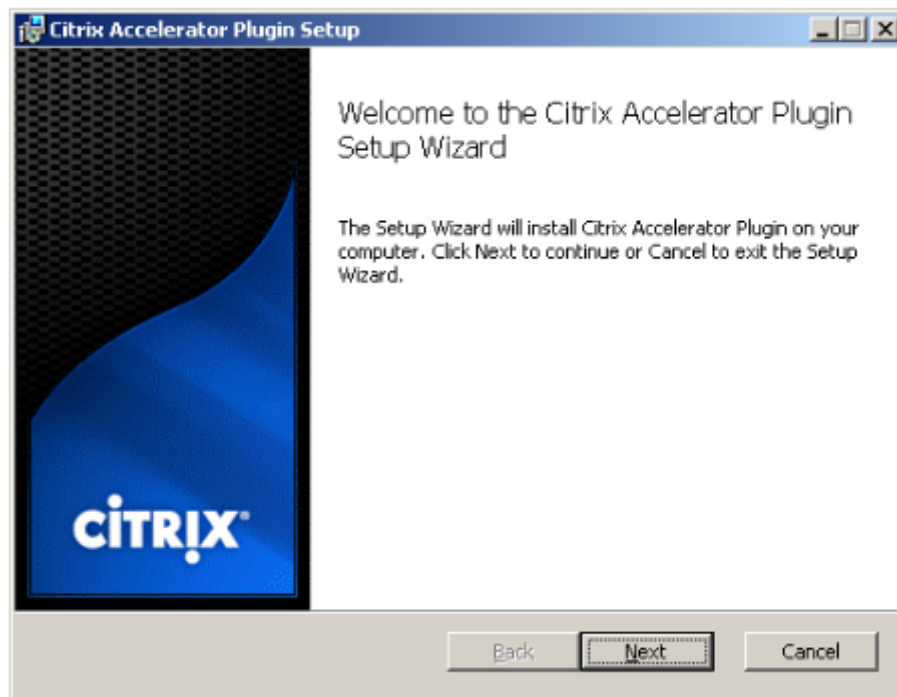
Die einzige Benutzerkonfiguration, die vom Plug-in benötigt wird, ist die Liste der Appliance-Adressen. Diese Liste kann aus einer kommagetrennten Liste von IP- oder DNS-Adressen bestehen. Die beiden Formen können gemischt werden. Sie können die Verteilungsdatei so anpassen, dass die Liste standardmäßig auf Ihre Appliance verweist. Nach der Installation ist der Betrieb transparent. Der Datenverkehr zu beschleunigten Subnetzen wird über eine entsprechende Appliance gesendet, und der gesamte andere Datenverkehr wird direkt an den Server gesendet. Die Benutzeranwendung ist sich nicht bewusst, dass dies geschieht.

## **Installation**

So installieren Sie den WANOP Client Plug-in Plug-in Accelerator auf Windows-Systemen:

1. Die Datei Repeater\*.msi ist eine Installationsdatei. Schließen Sie alle Anwendungen und alle Fenster, die möglicherweise geöffnet sind, und starten Sie das Installationsprogramm auf die übliche Weise (doppelklicken Sie in einem Dateifenster auf, oder verwenden Sie den Befehl run).

#### **Abbildung 1. Bildschirm für die Erstinstallation:**



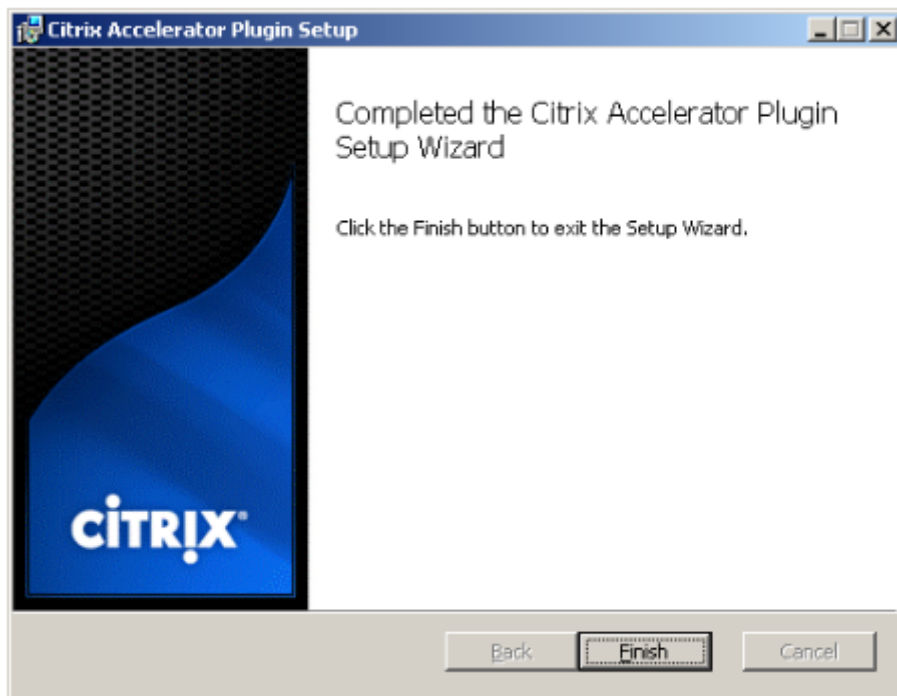
Die folgenden Schritte sind für eine interaktive Installation. Eine unbeaufsichtigte Installation kann mit dem Befehl durchgeführt werden:

*msiexec /i client\_msi\_file /qn*

2. Das Installationsprogramm fragt nach dem Speicherort, an dem die Software installiert werden soll. Das angegebene Verzeichnis wird sowohl für die Clientsoftware als auch für den datenträgerbasierten Komprimierungsverlauf verwendet. Zusammen benötigen sie mindestens 500 MB Speicherplatz.
3. Wenn das Installationsprogramm abgeschlossen ist, werden Sie möglicherweise aufgefordert, das System neu zu starten. Nach einem Neustart startet das WANOP Client Plug-In Plug-In automatisch.

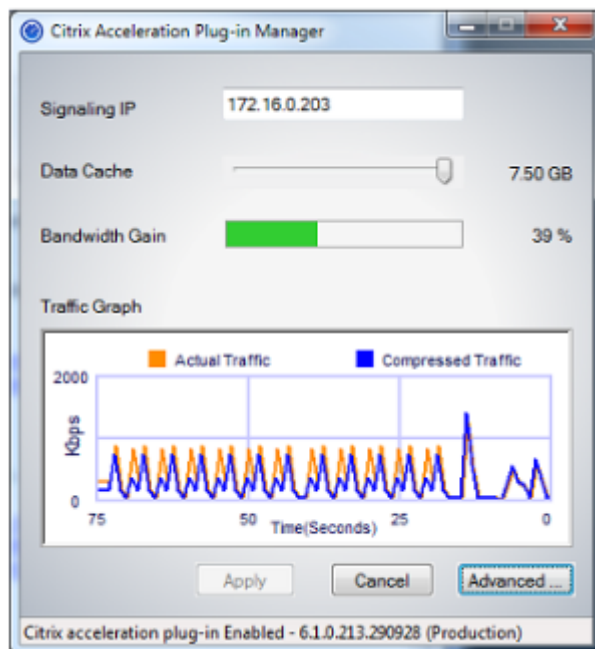
**Abbildung 2. Endgültiger Installationsbildschirm:**





4. Klicken Sie mit der rechten Maustaste auf das Accelerator-Symbol in der Taskleiste, und wählen Sie **Beschleunigung verwalten** aus, um den Citrix Plug-in Accelerator Manager zu starten.

**Abbildung 3. Citrix Accelerator-Plug-in-Manager, Initialanzeige (Basic):**



5. Wenn die MSI-Datei nicht für Ihre Benutzer angepasst wurde, geben Sie die Signaladresse und den Speicherplatz an, der für die Komprimierung verwendet werden soll:
- Geben Sie im Feld Appliances: Signaladressen die signalierende IP-Adresse Ihrer Appli-

ance ein. Wenn Sie mehr als eine Plug-In-fähige Appliance haben, führen Sie sie alle durch Kommas getrennt auf. Entweder IP- oder DNS-Adressen sind akzeptabel.

- Wählen Sie mithilfe des Schiebereglers Datencache den Speicherplatz aus, der für die Komprimierung verwendet werden soll. Mehr ist besser. 7,5 GB sind nicht zu viel, wenn Sie so viel Speicherplatz zur Verfügung haben.
- Drücken Sie Übernehmen.

Der WANOP Client Plug-In Accelerator läuft jetzt. Alle zukünftigen Verbindungen zu beschleunigten Subnetzen werden beschleunigt

Auf der Registerkarte Erweiterte Regeln des Plug-Ins sollte in der Liste Beschleunigungsregeln jede Appliance als Verbunden und die beschleunigten Subnetze jeder Appliance als Beschleunigt angezeigt werden. Wenn nicht, aktivieren Sie das IP-Feld Signaladressen und Ihre Netzwerkkonnektivität im Allgemeinen.

## Problembehandlung bei Plug-Ins

Die Plug-In-Installation verläuft in der Regel reibungslos. Wenn nicht, überprüfen Sie die folgenden Probleme:

### Häufige Probleme:

- Wenn Sie das System nicht neu starten, wird das WANOP Client-Plug-In nicht ordnungsgemäß ausgeführt.
- Ein stark fragmentierter Datenträger kann zu einer schlechten Komprimierungsleistung führen.
- Ein Beschleunigungsfehler (keine beschleunigten Verbindungen auf der Registerkarte **Diagnose**) weist normalerweise darauf hin, dass die Kommunikation mit der Appliance verhindert wird. Überprüfen Sie die Liste **Konfiguration: Beschleunigungsregeln** im Plug-In, um sicherzustellen, dass die Appliance erfolgreich kontaktiert wird und dass die Zieladresse in einer der Beschleunigungsregeln enthalten ist. Typische Ursachen für Verbindungsfehler sind:
  - Die Appliance wird nicht ausgeführt, oder die Beschleunigung wurde deaktiviert.
  - Eine Firewall entfernt die TCP-Optionen des WANOP Client-Plug-Ins irgendwann zwischen dem Plug-In und der Appliance.
  - Das Plug-In verwendet ein nicht unterstütztes VPN.

## Deterministischer Netzwerk-Enhancer Sperrfehler

In seltenen Fällen wird nach der Installation des Plug-Ins und dem Neustart des Computers die folgende Fehlermeldung zweimal angezeigt:

Deterministic Network Enhancer Installation erfordert zunächst einen Neustart, um gesperrte Ressourcen freizumachen. Führen Sie diese Installation erneut aus, nachdem Sie den Computer neu gestartet haben.

Sie umgehen das Problem wie folgt:

1. Gehen Sie zu **Software hinzufügen/entfernen** und entfernen Sie das WANOP Client-Plug-in, falls vorhanden.
2. Gehen Sie zu **Systemsteuerung > Netzwerkadapter > LAN-Verbindung > Eigenschaften**, suchen Sie den Eintrag für Deterministic Network Enhancer, deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **OK**. (Ihr Netzwerkadapter wird möglicherweise unter einem anderen Namen als LAN-Verbindung aufgerufen.)
3. Öffnen Sie ein Befehlsfenster und gehen Sie zu c:windowsinf (oder dem entsprechenden Verzeichnis, wenn Sie Windows an einem nicht standardmäßigen Speicherort installiert haben).
4. Geben Sie den folgenden Befehl ein:  
finden Sie dne2000.cat oem\*.inf
5. Suchen Sie die Datei oem\*.inf mit der höchsten Zahl, die eine übereinstimmende Zeile zurückgegeben hat (die passende Zeile ist CatalogFile= dne2000.cat), und bearbeiten Sie sie. Beispiel:  
Notizblock oem13.inf
6. Löschen Sie alles außer den drei Zeilen oben, die mit Semikolons beginnen, und speichern Sie die Datei. Dadurch werden alle unangemessenen oder veralteten Einstellungen gelöscht und bei der nächsten Installation werden Standardwerte verwendet.
7. Wiederholen Sie die Installation.

## Andere Installationsprobleme

Jedes Problem bei der Installation des WANOP Client-Plug-Ins ist in der Regel das Ergebnis einer bestehenden Netzwerk-, Firewall- oder Antivirensoftware, die die Installation beeinträchtigt. Normalerweise gibt es nach Abschluss der Installation keine weiteren Probleme.

Wenn die Installation fehlschlägt, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Plug-In-Installationsdatei auf Ihr lokales System kopiert wurde.
2. Trennen Sie alle aktiven VPN/Remote-Netzwerkclients.
3. Deaktivieren Sie alle Firewall- und Antivirus-Software vorübergehend.
4. Wenn etwas davon schwierig ist, tun Sie, was Sie können.
5. Installieren Sie das WANOP Client-Plug-In neu.
6. Wenn dies nicht funktioniert, starten Sie das System neu und versuchen Sie es erneut.

## Citrix SD-WAN WANOP-Plug-in-GUI

April 19, 2021

Die Benutzeroberfläche des WANOP Client-Plug-ins wird angezeigt, wenn Sie mit der rechten Maustaste auf das Symbol des **Citrix Accelerator-Plug-ins** klicken und die Option **Beschleunigung verwalten** auswählen. Zuerst wird die Basic-Anzeige der GUI angezeigt. Es gibt auch ein Advanced Display, das auf Wunsch verwendet werden kann.

### Basisanzeige

Auf der Seite Basic können Sie zwei Parameter festlegen:

- Das Feld Signaladressen gibt die IP-Adresse jeder Appliance an, mit der das Plug-In eine Verbindung herstellen kann. Citrix empfiehlt, nur eine Appliance aufzulisten, Sie können jedoch eine durch Kommas getrennte Liste erstellen. Dies ist eine geordnete Liste, wobei die ganz links Appliances Vorrang vor den anderen haben. Die Beschleunigung wird mit der ganz links stehenden Appliance versucht, für die eine Signalverbindung hergestellt werden kann. Sie können sowohl DNS-Adressen als auch IP-Adressen verwenden.

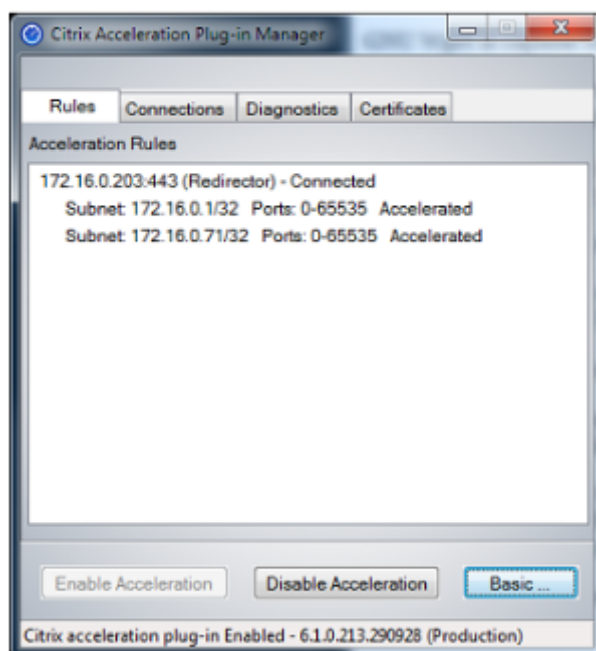
Beispiele: 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

- Der Schieberegler Datencache passt den Speicherplatz an, der dem datenträgerbasierten Komprimierungsverlauf des Plug-Ins zugewiesen ist. Mehr ist besser.

Darüber hinaus gibt es eine Schaltfläche, um zur erweiterten Anzeige zu wechseln.

### Erweiterte Anzeige

Die Seite Erweitert enthält vier Registerkarten: Regeln, Verbindungen, Diagnose und Zertifikate.



Am unteren Rand der Anzeige befinden sich Schaltflächen, um die Beschleunigung zu aktivieren, die Beschleunigung zu deaktivieren und zur Seite Basic zurückzukehren.

## Registerkarte Regeln

Auf der Registerkarte Regeln wird eine abgekürzte Liste der von den Appliances heruntergeladenen Beschleunigungsregeln angezeigt. Jedes Listenelement zeigt die Signaladresse und den Port der Appliance, den Beschleunigungsmodus (Redirector oder transparent) und den Verbindungsstatus, gefolgt von einer Zusammenfassung der Regeln der Appliance.

## Registerkarte Verbindungen

Die Registerkarte **Verbindungen** listet die Anzahl der offenen Verbindungen verschiedener Typen auf:

- **Beschleunigte Verbindungen**—Die Anzahl der offenen Verbindungen zwischen dem WANOP Client Plug-in und Appliances. Diese Nummer enthält eine Signalverbindung pro Appliance, enthält jedoch keine beschleunigten CIFS-Verbindungen. Wenn Sie auf Mehr klicken, wird ein Fenster mit einer kurzen Zusammenfassung jeder Verbindung geöffnet. (Alle Schaltflächen Mehr ermöglichen es Ihnen, die Informationen im Fenster in die Zwischenablage zu kopieren, falls Sie sie für den Support freigeben möchten.)
- **Beschleunigte CIFS-Verbindungen**—Die Anzahl der offenen, beschleunigten Verbindungen mit CIFS-Servern (Windows File System). Dies entspricht normalerweise der Anzahl der bereitgestellten Netzwerkdateisysteme. Wenn Sie auf Mehr klicken, werden dieselben Informationen

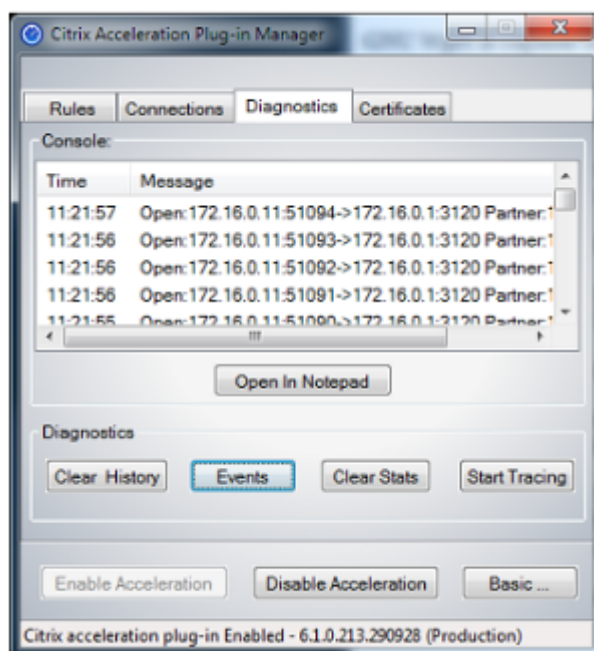
angezeigt wie bei beschleunigten Verbindungen sowie ein Statusfeld, das Aktiv meldet, wenn die CIFS-Verbindung mit den speziellen CIFS-Optimierungen des WANOP Client-Plug-Ins ausgeführt wird.

- **Beschleunigte MAPI-Verbindungen**—Die Anzahl der offenen, beschleunigten Outlook/Exchange-Verbindungen.
- **Beschleunigte ICA-Verbindungen**:Die Anzahl der geöffneten, beschleunigten Citrix Virtual Apps and Desktops Verbindungen mit den ICA- oder CGP-Protokollen.
- **Nicht beschleunigte Verbindungen**—Öffnet Verbindungen, die nicht beschleunigt werden. Sie können auf Mehr klicken, um eine kurze Beschreibung anzuzeigen, warum die Verbindung nicht beschleunigt wurde. Normalerweise ist der Grund dafür, dass keine Appliance die Zieladresse beschleunigt, die als Dienstrichtlinienregel gemeldet wird.
- **Verbindungen öffnen/schließen**—Verbindungen, die nicht vollständig geöffnet sind, aber gerade geöffnet oder geschlossen werden (TCP-Verbindungen halb offen oder halb geschlossen). Die Schaltfläche Mehr zeigt einige zusätzliche Informationen zu diesen Verbindungen an.

## Registerkarte Diagnose

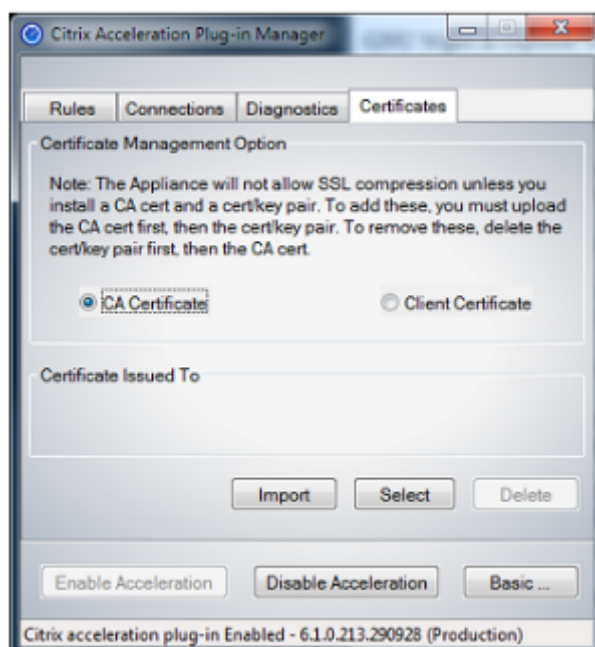
Auf der Seite Diagnose werden die Anzahl der Verbindungen in verschiedenen Kategorien sowie weitere nützliche Informationen angezeigt.

- **Ablaufverfolgung/Ablaufverfolgung starten**—Wenn Sie ein Problem melden, werden Sie möglicherweise von Ihrem Citrix Vertreter aufgefordert, eine Verbindungsverfolgung durchzuführen, um Probleme zu ermitteln. Diese Schaltfläche startet und stoppt die Ablaufverfolgung. Wenn Sie die Ablaufverfolgung beenden, werden die Ablaufverfolgungsdateien in einem Pop-upfenster angezeigt. Senden Sie sie auf die von ihm empfohlenen Mittel an Ihren Citrix Vertreter.
- **Verlauf löschen**—Dieses Feature sollte nicht verwendet werden.
- **Statistiken löschen**—Durch Drücken dieser Schaltfläche wird die Statistik auf der Registerkarte Leistung gelöscht.
- **Konsole**: Ein scrollbares Fenster mit aktuellen Statusmeldungen, meist Meldungen zum Öffnen und Schließen von Verbindungen, aber auch Fehler- und sonstige Statusmeldungen.



## Registerkarte Zertifikate

Auf der Registerkarte Zertifikate können Sie Sicherheitsanmeldeinformationen für das optionale Secure Peering-Feature installieren. Mit diesen Sicherheitsanmeldeinformationen kann die Appliance überprüfen, ob es sich bei dem Plug-In um einen vertrauenswürdigen Client handelt oder nicht.



So laden Sie das CA-Zertifikat und das Zertifikatschlüsselpaar hoch:

1. Wählen Sie **CA-Zertifikatverwaltung** aus.
2. Klicken Sie auf **Importieren**.
3. Laden Sie ein Zertifizierungsstellenzertifikat hoch. Die Zertifikatdatei muss einen der unterstützten Dateitypen (.pem, .crt., .cer oder .spc) verwenden. Möglicherweise wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, den Zertifikatspeicher auszuwählen, den Sie verwenden möchten, und eine Liste mit Schlüsselwörtern anzuzeigen. Wählen Sie das erste Schlüsselwort in der Liste aus.
4. Wählen Sie **Clientzertifikatverwaltung** aus.
5. Klicken Sie auf **Importieren**.
6. Wählen Sie das Format des Zertifikatschlüsselpaars (PKCS12 oder PEM/DER).
7. Klicken Sie auf **Absenden**.

#### Hinweis

Bei PEM/DER gibt es separate Upload-Boxen für Zertifikat und Schlüssel. Wenn Ihr Zertifikatschlüsselpaar in einer einzigen Datei kombiniert wird, geben Sie die Datei zweimal an, einmal für jedes Feld.

## Aktualisieren des Citrix SD-WAN WANOP-Plug-ins

April 19, 2021

Um eine neuere Version des WANOP Client-Plug-ins zu installieren, befolgen Sie das gleiche Verfahren, das Sie bei der ersten Installation des Plug-Ins verwendet haben.

### Deinstallieren des WANOP-Client-Plug-ins

Verwenden Sie zum Deinstallieren des WANOP Client Plug-Ins das Windows-Hilfsprogramm **“Programme hinzufügen/entfernen”**. Das WANOP Client-Plug-in wird in der Liste der aktuell installierten Programme als **Citrix Acceleration Plug-in** aufgeführt. Wählen Sie es aus und klicken Sie auf **Entfernen**.

Starten Sie das System neu, um die Deinstallation des Clients abzuschließen.



## Citrix Virtual Apps and Desktops Beschleunigung

April 19, 2021

### Hinweis

In dieser Diskussion bezieht sich *Virtual Apps* auf die ICA- und CGP-Protokollströme. Daher gilt das Thema Virtual Apps auch für Virtual Desktops.

Virtual Apps/Virtual Desktops (ICA/CGP)-Beschleunigung umfasst drei Komponenten:

- **Komprimierung:** Das Gerät wechselt mit Virtual Apps-Clients und Servern zum Komprimieren von Virtual Apps-Datenstreams für interaktive Daten (Tastatur/Maus/Anzeige/Audio) und Batchdaten (Drucken und Dateiübertragungen). Diese Interaktion erfolgt transparent und erfordert keine Konfiguration der Appliance. Auf älteren Virtual Apps-Servern (Release 4.x) ist einiges an Konfiguration erforderlich (siehe unten).
- **Multistream ICA**—Neben der Komprimierung unterstützen Citrix SD-WAN WANOP-Appliances das neue Multistream-ICA-Protokoll, in dem bis zu vier Verbindungen für die verschiedenen ICA-Prioritäten verwendet werden, anstatt alle Prioritäten gegenüber derselben Verbindung zu multiplexen. Dieser Ansatz verleiht interaktiven Aufgaben eine höhere Reaktionsfähigkeit, insbesondere in Kombination mit der Traffic-Gestaltung der Appliance.
- **Traffic Shaping**—Der Citrix SD-WAN WANOP Traffic Shaper verwendet die Prioritätsbits in den Virtual Apps-Datenprotokollen, um die Priorität der Verbindung in Echtzeit zu modulieren und den Bandbreitenanteil jeder Verbindung mit der derzeit übertragenen Verbindung abzugleichen.

### Hinweis

Multistream-ICA ist standardmäßig deaktiviert. Sie kann auf der Seite Features aktiviert werden. Multistream-ICA und AutoQoS erfordern die Aktivierung der Sitzungszuverlässigkeit.

Zum Optimieren von ICA-Verbindungen für Citrix Virtual Apps and Desktops Version 7.0 und höher unterstützt Citrix SD-WAN WANOP-Gerät Citrix Receiver für Chrome Release 1.4 und höher und Citrix Receiver für HTML5 Version 1.4 und höher.

**HDX-Transportprotokoll von UDP/EDT zu TCP**—Unter bestimmten Netzwerkbedingungen kann UDP/EDT nicht als optimiertes Protokoll zur Bereitstellung von HDX-Datenverkehr verwendet werden. Sie können das Protokoll in TCP ändern, damit WANOP Folgendes bereitstellen kann:

- Vorteile für Compression/DDup
- Sichtbarkeit (lokale Berichte und HDX Insight)

WANOP kann EDT-Verkehr blockieren und die Sitzung auf TCP erzwingen. Während der Sitzungsinitiiierung startet Citrix Receiver die Sitzung sowohl auf TCP als auch auf EDT. Wenn EDT-Sitzung nicht eingerichtet ist, wird die TCP-Sitzung verwendet. WANOP GUI bietet eine Option, um die Sitzung auf TCP-Protokoll auf der Featuesseite zu erzwingen.

## Konfigurieren von Virtual Apps-Beschleunigung

April 19, 2021

Die Virtual Apps-Beschleunigung gilt für die Protokolle ICA und CGP in Virtual Apps. Die Citrix SD-WAN WANOP-Appliances, Virtual Apps-Server und Virtual Apps-Clients sorgen für eine kooperative Beschleunigung der Virtual Apps-Verbindungen und bieten eine erhebliche Beschleunigung im Vergleich zu virtuellen Apps allein. Diese Zusammenarbeit erfordert aktuelle Versionen aller drei Komponenten.

Die Virtual Apps-Komprimierung wechselt dynamisch zwischen speicherbasierter Komprimierung für interaktive Kanäle (z. B. Maus, Tastatur und Bildschirmdaten) und datenträgerbasierter Komprimierung für Massenaufgaben (z. B. Dateiübertragungen und Druckaufträge). Komprimierungsverhältnisse steigen, wenn der Komprimierungsverlauf ausgefüllt wird, und erhöhen die Datenmenge, die mit neuen Daten verglichen werden kann. Die Virtual Apps-Komprimierung bietet doppelt so viel Datenreduktion wie unbeaufsichtigte Virtual Apps, die bei repetitiven Massenübertragungen (z. B. Drucken oder Aufeinanderfolgende Versionen desselben Dokuments) oft mehr als 50:1 dauert.

Die Virtual Apps-Komprimierung erreicht eine hohe Verbindungsauslastung ohne Überlastung, da sich Die Benutzer nicht gegenseitig stören.

### Aktivieren der Virtual Apps-Beschleunigung

1. Überprüfen Sie die ICA-Service-Class-Richtlinie. Auf der Seite Konfiguration: Dienstklassen sollte die ICA-Serviceklasse in der Spalte Beschleunigung den Datenträger und die ICA-Prioritäten in der Spalte Traffic Shaping anzeigen. Wenn nicht, bearbeiten Sie die Service-Klassendefinition.
2. Aktualisieren Sie Server und Clients für Virtual Apps 4.x. (In Virtual Apps 5.0 oder höher nicht erforderlich). Verwenden Sie Presentation Server 4.5 mit Hotfix Rollup Pack PSE450W2K3R03 (Beta) oder höher. Dieses Release enthält die folgende Server- und Clientsoftware, die beide für die Virtual Apps-Komprimierung installiert werden müssen:
  - a) Serverpaket PSE450R03W2K3WS.msp oder höher.
  - b) Client-Version 11.0.0.5357 oder höher.
3. Aktualisieren Sie Virtual Desktops-Server und -Clients auf die Version 4.0 oder höher.

- Überprüfen Sie die Registrierungseinstellungen des Virtual Apps-Servers. (In Virtual Apps 5.0 oder höher nicht erforderlich.) Überprüfen Sie auf den Virtual Apps-Servern die folgenden Einstellungen und korrigieren oder erstellen Sie sie nach Bedarf:

```
pre codeblock HKLM\System\CurrentControlSet\Control\Citrix\
WanScaler\EnableForSecureIca = 1 HKLM\System\CurrentControlSet
\Control\Citrix\WanScaler\EnableWanScalerOptimization = 1 HKLM\
System\CurrentControlSet\Control\Citrix\WanScaler\UchBehavior = 2
<!--NeedCopy-->
```

Dies sind alle DWORD-Werte.

- Öffnen und verwenden Sie Virtual Apps-Verbindungen zwischen aktualisierten Virtual Apps-Clients und Servern, die das aktualisierte Citrix SD-WAN WANOP durchlaufen. Standardmäßig verwenden diese Sitzungen CGP. Deaktivieren Sie für ICA auf dem Client unter Citrix Program Neighborhood das Kontrollkästchen Custom ICA-Verbindungen. Klicken Sie dann mit der rechten Maustaste auf ein Verbindungssymbol, navigieren Sie zu **Eigenschaften > Optionen**, und klicken Sie auf **Sitzungszuverlässigkeit aktivieren**. Multistream-ICA und AutoQoS erfordern die Aktivierung der Sitzungszuverlässigkeit.
- Überprüfen Sie die Beschleunigung.

Nachdem Sie Virtual Apps-Sitzungen über die beschleunigte Verbindung gestartet haben, sollten beschleunigte ICA-Verbindungen auf der Seite “Überwachen: Verbindungen” des Geräts angezeigt werden. Ein Komprimierungsverhältnis größer als 1:1 gibt an, dass die Komprimierung stattfindet.

## Optimieren von Citrix Receiver für HTML5

December 14, 2022

Anwendung, die dynamische Inhalte bereitstellen muss, arbeiten auf HTML5 WebSockets. Citrix Receiver für Chrome und Citrix Receiver für HTML5 sind solche Anwendungen, die HTML5 WebSockets unterstützen. Diese Anwendungen haben den Zugriff auf virtuelle Desktops vereinfacht, da sie in die aktuellen Webbrowser integriert werden können, die HTML5-WebSockets unterstützen.

### Hinweis

Sie müssen keine Änderungen an der Appliance-Konfiguration vornehmen, um diese Funktion verwenden zu können.

## Wie eine Citrix SD-WAN WANOP-Appliance Citrix Receiver für HTML5 optimiert

In einer typischen Zweigstelle und einem Datacenter werden freigegebene Ressourcen wie der Virtual Desktop Agent (VDA) auf einem Citrix Hypervisor Server im Datacenter installiert. Clients aus den Zweigstellen greifen mithilfe von Citrix Receiver auf diese freigegebenen Ressourcen über das Netzwerk zu.

In einer typischen Zweigstelle und einem Datacenter werden freigegebene Ressourcen wie der Virtual Desktop Agent (VDA) auf einem Citrix Hypervisor Server im Datacenter installiert. Clients aus den Zweigstellen greifen mithilfe von Citrix Receiver auf diese freigegebenen Ressourcen über das Netzwerk zu.

Als HTML-kompatibel verwendet VDA einen WebSocket-Listener, der auf Port 8008 ausgeführt wird. Beim Zugriff auf eine Anwendung initiiert der Client eine TCP-Verbindung an Port 8008 und sendet damit eine HTTP-Anforderung an den Server, um die Verbindung zu aktualisieren und das WebSocket-Protokoll zu verwenden. Nachdem der Client die WebSocket-Verbindung mit VDA ausgehandelt hat, beginnen Independent Computing Architecture (ICA) Verhandlungen, und der Client und der Server verwenden ICA über HTML5, um Daten auszutauschen. Weitere Informationen zur Abfolge von Nachrichten, die zwischen Client und Server ausgetauscht werden, finden Sie unter Nachrichten, die zwischen dem Client und dem Server ausgetauscht werden.

Nachdem Verbindungen zwischen den Clients und dem Server hergestellt wurden, beginnt die Citrix SD-WAN WANOP-Appliance mit der Optimierung der Verbindungen, indem der Datenverkehr über das Netzwerk beschleunigt und Webseiten und andere Anwendungen mit Citrix Receiver für HTML5 beschleunigt werden. Die Funktionalität der Optimierung der Citrix Receiver für HTML5-Verbindungen ähnelt der HTTP-Beschleunigung.

### Hinweis

- Weitere Informationen zu HTML5 finden Sie unter [Funktionsweise von HTML5](#).
- Weitere Informationen zu Citrix Receiver für HTML5 finden Sie unter <http://support.citrix.com/proddocs/topic/html5.html>.
- Weitere Hinweise zu den Systemanforderungen von Receiver für HTML5 finden Sie unter <http://support.citrix.com/proddocs/topic/receiver-html5-14/receiver-html5-sys-req.html>.

## Konfigurieren einer Citrix SD-WAN WANOP-Appliance zur Optimierung von Citrix Receiver für HTML5

Die Optimierung von Citrix Receiver für HTML5-Verbindungen ist eine Null-Konfigurationsfunktion. Sie müssen keine Konfigurationsänderungen an der Appliance vornehmen. Beim Upgrade der Citrix SD-WAN WANOP-Software auf CB 7.3.1 oder höher wird die Alt-HTTP-Anwendungsklassifizierung auf dem Gerät erstellt und diese Anwendungsklassifizierung Port 8008 zugeordnet. Dies ist der Stan-

dardwert für Virtual Desktops. Sobald Sie die Software aktualisieren, ist die Appliance bereit, native Chrome-Verbindungen zu optimieren, die Citrix Receiver für HTML5 verwenden.

Wenn Sie SSL-Verschlüsselung für Verbindungen über Citrix Receiver für HTML5 verwenden, verwenden Verbindungen ICA über SSL. Um die ICA over SSL-Beschleunigung mit Citrix Receiver für HTML5 zu aktivieren, müssen Sie die standardmäßige SSL-Beschleunigung konfigurieren, die die entsprechende Ziel-IP-Adresse in der Dienstklasse und der SSL-Profilzuordnung enthält. Wenn Sie planen, die Appliance im ICA-Proxymodus bereitzustellen, müssen Sie die StoreFront-VIP-Adresse StoreFront-Zertifikaten zuordnen. Wenn Sie die Appliance in einem End-to-End-SSL-Verschlüsselungsbereitstellungsmodus bereitstellen möchten, müssen Sie die VDA-IP-Adresse den VDA-Zertifikaten zuordnen.

### Warnung

Stellen Sie sicher, dass Sie die Portnummer der alt-http-Anwendung nicht in eine andere Portnummer ändern. Wenn Sie diesen Anwendungsklassifizierer löschen oder Änderungen vornehmen müssen, müssen Sie den Port 8008 dem HTTP-Anwendungsklassifizierer hinzufügen.

## Überprüfen von Citrix Receiver für HTML5-Verbindungen

Um zu überprüfen, ob die Appliance Citrix Receiver für HTML5-Verbindungen optimiert, können Sie überprüfen, ob Verbindungen auf den Überwachungsseiten Citrix (ICA/CGP) und ICA Advanced aufgeführt sind. Das Vorhandensein von HTML5-Verbindungen auf den Überwachungsseiten ist ein Hinweis darauf, dass die Appliance Citrix Receiver für HTML5-Verbindungen optimiert.

### So überprüfen Sie die Citrix Receiver für HTML5-Verbindung auf einer Citrix SD-WAN WANOP-Appliance:

1. Navigieren Sie zur Seite **Überwachung > Optimierung > Citrix (ICA/CGP)**.
2. Überprüfen Sie auf der Registerkarte **ICA-Verbindungen**, ob die HTML5-Verbindungen aufgelistet sind. Eine HTML5-Verbindung wird mit HTML als Präfix in der Spalte Client-Computernamen angezeigt, wie im folgenden Screenshot gezeigt:

Published Application or Desktop	Client Computer Name	Client IP Address	Server IP Address	Protocol	Duration	Transferred Bytes	Acceleration Status	Encryption
Word 2013_1	HTML-2922-1550	14.141.5.5	10.102.255.210	ICA over SSL	11h 45m 17s	1.19 MB	●	Basic (XOR)
SC Ar26 Win 2008 R2 RDS	HTML-1184-5111	14.141.5.5	10.102.255.210	ICA over SSL	4m 7s	196.88 KB	●	Basic (XOR)

3. Navigieren Sie zur Seite **Überwachung > Optimierung > ICA Erweitert**.

4. Scrollen Sie auf der Registerkarte **Conn Info** nach unten zum Abschnitt ICA-Client- und Server-Informationen. Einträge für HTML5-Verbindungen enthalten Citrix HTML5-Client in der Spalte Product ID, wie im folgenden Screenshot gezeigt:

Dashboard

Monitoring

Configuration

Notifications (0)

Optimization

Citrix (ICA/CGP)

Connections

Compression

Filesystem (CIFS/SMB)

LAN vs WAN

Links Usage

Outlook (MAPI)

Service Classes

Top Applications

Traffic Shaping

Usage Graph

ICA Advanced

Appliance Performance

Partners & Plug-ins

Monitoring > Optimization > ICA Advanced

Show Acceleration Status and Diagnostics: ALL Connections [Toggle](#)

Acceleration Status and Diagnostics

Conn ID	Connection Status	Session Status	Diagnostics	Remedy
116	<div></div>	<div></div>	OK	None
113	<div></div>	<div></div>	OK	None

Connection Attributes

Conn ID	Protocol	Stream	ICA Priority	Encryption	CB Pair Compression	CB Conn Compression Algorithm	CB Side	Client CB Compression	Server CB Compression	Acceleration Partner Type
116	ICA over SSL	Single	mixed	Basic (XOR)	on	DBC	Server	Disk	Disk	Appliance
113	ICA over SSL	Single	mixed	Basic (XOR)	on	DBC	Server	Disk	Disk	Appliance

ICA Client and Server Information

Client Info							Server Info				
Conn ID	Stream	Initial Program	Name	Version	Product ID	Directory	Launcher	Farm Name	Name	User Name	Domain
116	Single	SC Ar26 Win 2008 R2 RDS	HTML-1184-5111	1.4.0.5018	Citrix HTML5 client	none	ReceiverWeb		SC-RDS-AR26-02	sanjays	citrite
113	Single	Word 2013_1	HTML-2922-1550	1.5	Citrix HTML5 client	none	ReceiverWeb		CH-RDS-AR26-05	thavamanir	citrite

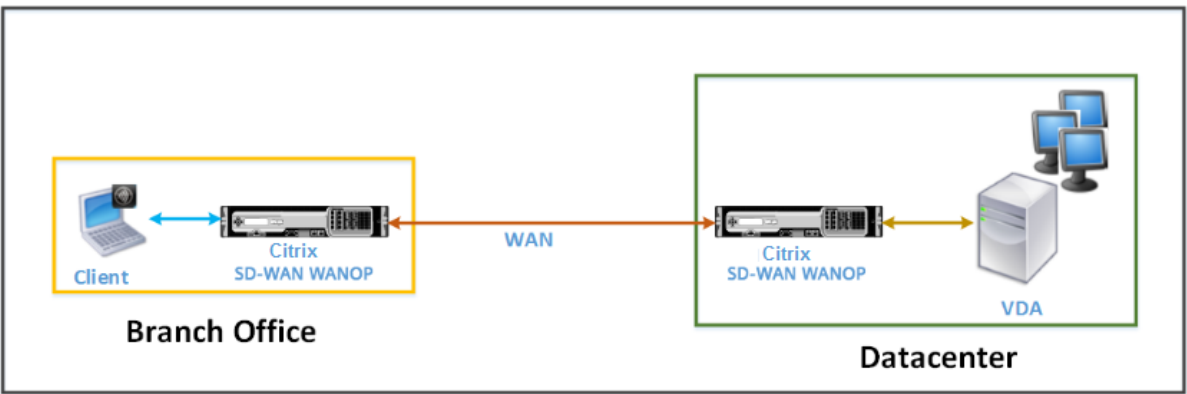
ICA Session Information

## Bereitstellungsmodi

April 19, 2021

In einer typischen Citrix SD-WAN WANOP-Bereitstellung werden die Citrix SD-WAN WANOP-Appliances zwischen Zweigstellen und Rechenzentren gepaart. Sie installieren gemeinsam genutzte Ressourcen, z. B. VDA, im Rechenzentrum. Clients aus verschiedenen Zweigstellen greifen mithilfe von Citrix Receiver auf Datencenterrressourcen zu, wie in der folgenden Abbildung dargestellt.

Eine typische Citrix SD-WAN WANOP-Bereitstellungstopologie

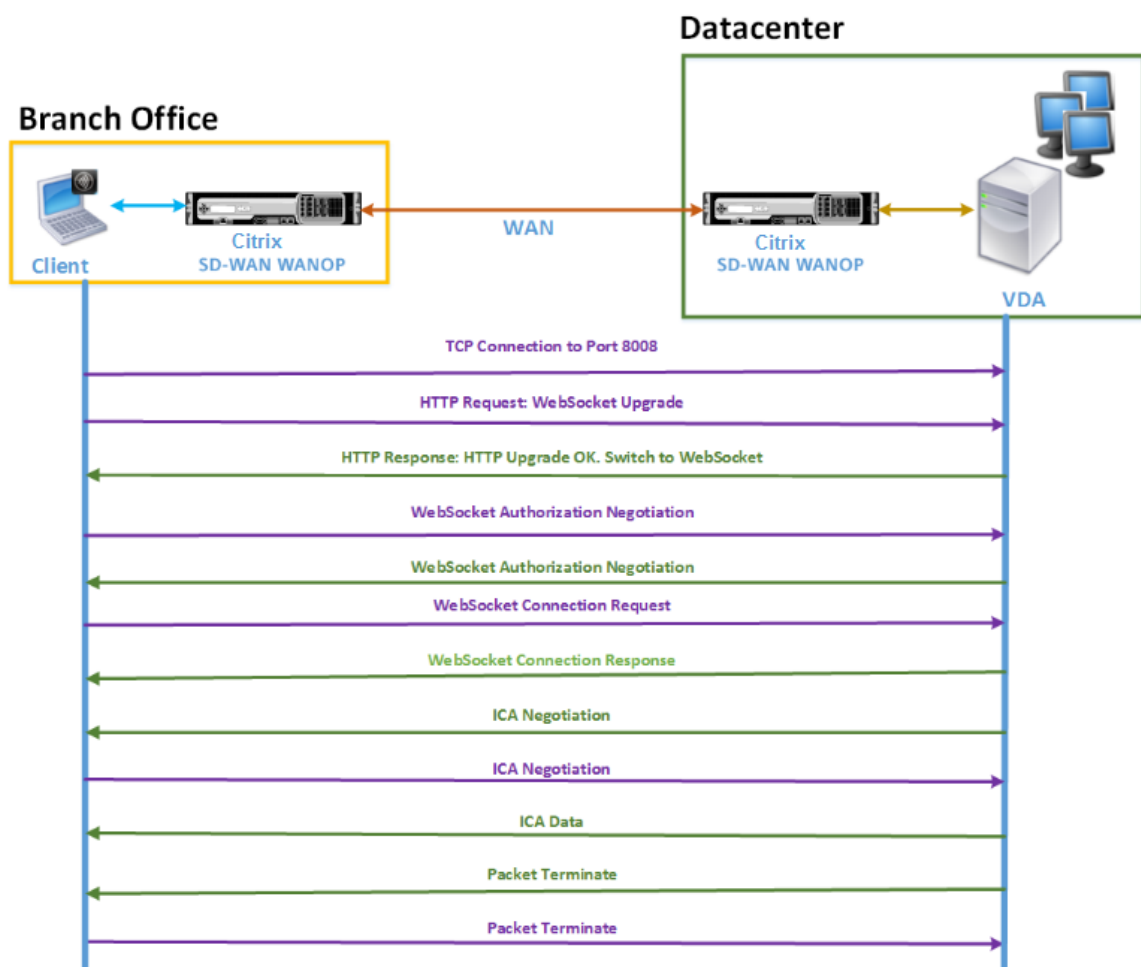


Clients installieren ein Citrix Receiver-Softwareprodukt, z. B. Citrix Receiver für HTML5, auf ihren lokalen Computern und verwenden es, um auf Ressourcen im Rechenzentrum zuzugreifen.

Verbindungen über das Paar Citrix SD-WAN WANOP Appliances werden optimiert.

## Verstehen von Nachrichten, die zwischen dem Client und dem Server ausgetauscht werden

Wie bei jeder Art von Netzwerkverbindung tauscht ein Client, der Citrix Receiver für HTML5 verwendet, verschiedene Nachrichten mit dem Server aus. Die folgende Abbildung zeigt einen typischen Nachrichtenfluss zwischen Client und Server, wenn eine Verbindung zwischen ihnen hergestellt wird.



Wie in der obigen Abbildung gezeigt, wird die folgende Meldungsfolge zwischen dem Client und dem Server ausgetauscht, wenn ein Client aus einer Zweigstelle auf Serverressourcen für Rechenzentren zugreifen möchte:

1. Client verwendet Citrix Receiver für HTML5, um eine TCP-Verbindungsanforderung an VDA an Port 8008 zu senden.
2. Nach dem Herstellen der TCP-Verbindung sendet der Client eine WebSocket-Upgradeanforderung

an VDA.

3. VDA reagiert auf die Upgradeanforderung und wechselt zum WebSocket-Protokoll.
4. Client und VDA verhandeln die WebSocket-Autorisierung.
5. Client sendet eine WebSocket-Verbindungsanforderung an VDA.
6. VDA antwortet auf die WebSocket-Verbindungsanforderung.
7. VDA initiiert ICA-Verhandlung mit dem Client.
8. Nach der ICA-Verhandlung beginnt der VDA die Übertragung von ICA-Daten.
9. VDA sendet Paketbeendungsanmeldung.
10. Client antwortet mit der Paketbeendungsanmeldung.

#### **Hinweis**

Das obige Beispiel listet die Beispielmeldungen auf, die über WebSocket gegen ICA ausgetauscht wurden. Wenn Sie ICA over Common Gateway Protocol (CGP) verwenden, verhandeln Client und Server CGP anstelle von WebSocket. Bei ICA über TCP verhandeln Client und Server jedoch ICA.

Abhängig von den Komponenten, die Sie im Netzwerk bereitgestellt haben, wird die Verbindung an verschiedenen Stellen beendet. Die obige Abbildung stellt eine Topologie dar, für die keine zusätzlichen Komponenten im Netzwerk bereitgestellt werden. Daher kommuniziert der Client direkt mit VDA an Port 8008. Wenn Sie jedoch ein Gateway wie Citrix Gateway im Rechenzentrum installiert haben, wird die Verbindung mit dem Gateway hergestellt und der VDA proxiiert. Bis das Gateway die WebSocket-Autorisierung aushandelt, gibt es keine Kommunikation mit VDA. Nachdem das Gateway die WebSocket-Autorisierung ausgehandelt hat, wird eine Verbindung mit VDA geöffnet. Danach fungiert das Gateway als Zwischenhändler und übergibt Nachrichten vom Client an den VDA und umgekehrt.

Wenn ein VPN-Tunnel zwischen einem auf dem Client installierten Citrix Gateway-Plugin und Citrix Gateway im Rechenzentrum erstellt wird, leitet das Gateway alle Clientmeldungen unmittelbar nach dem Aufbau einer TCP-Verbindung transparent an VDA weiter und umgekehrt.

#### **Hinweis**

Um eine Verbindung zu optimieren, die End-to-End-SSL-Verschlüsselung erfordert, wird eine TCP-Verbindung an Port 443 auf VDA hergestellt.

## **Unterstützte Bereitstellungsmodi**

Bei der Konfiguration einer Citrix SD-WAN WANOP-Appliance zur Optimierung von Citrix Receiver für HTML5 können Sie je nach Netzwerkanforderungen einen der folgenden Bereitstellungsmodi in Betra-



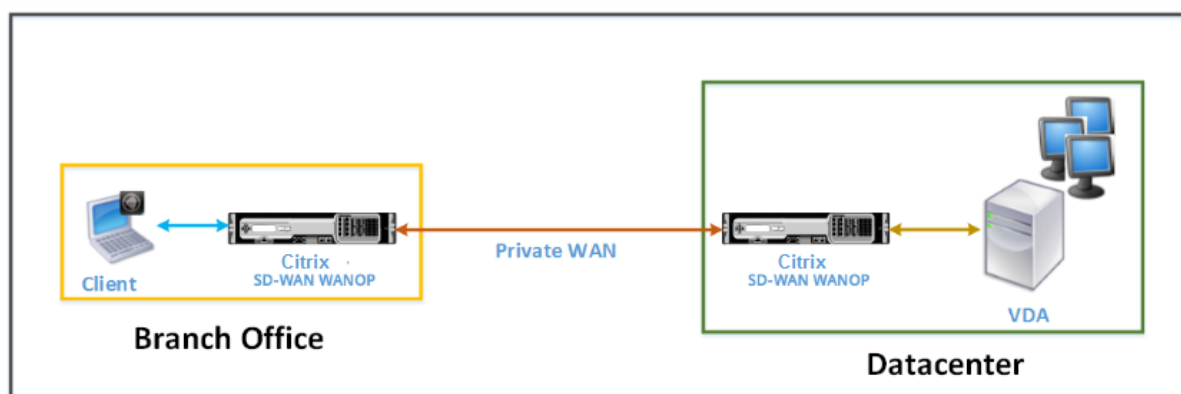
cht ziehen. Zur Optimierung von Citrix Receiver für HTML5-Verbindungen unterstützen Citrix SD-WAN WANOP-Appliances die folgenden Bereitstellungsmodi:

- Direkter Zugang
- Direkter Zugriff mit End-to-End-SSL-Verschlüsselung
- ICA-Proxy-Modus
- ICA-Proxy-Modus mit End-to-End-SSL-Verschlüsselung
- VPN-Modus (Full Virtual Private Network)
- VPN-Modus (Full Virtual Private Network) mit End-to-End-SSL-Verschlüsselung

### Direkter Zugang:

Die folgende Abbildung zeigt die Bereitstellungstopologie von Citrix Receiver für HTML5, die auf dem Client im Direktzugriffsmodus installiert ist.

Citrix SD-WAN WANOP Appliances im Direktzugriffsmodus bereitgestellt



Im Direktzugriffsmodus wird ein Paar Citrix SD-WAN WANOP-Appliances in einer Zweigstelle und im Rechenzentrum im Inlinemodus installiert. Ein Client greift über das private WAN über Citrix Receiver für HTML5 auf VDA-Ressourcen zu. Verbindungen vom Client zu den VDA-Ressourcen werden durch Verschlüsselung auf ICA-Ebene gesichert. Nachrichten, die zwischen dem Client und dem VDA ausgetauscht werden, werden unter Grundlegendes zu Nachrichten, die zwischen dem Client und dem Server ausgetauscht werden, erläutert.

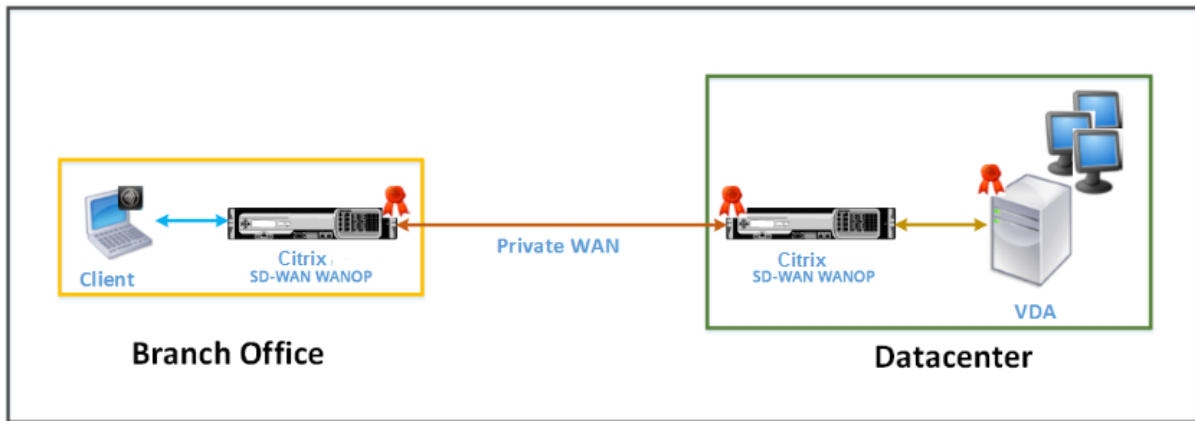
Die zwischen dem Client und dem VDA-Rechenzentrum installierten Citrix SD-WAN WANOP-Appliances optimieren die zwischen ihnen hergestellten Citrix Receiver für HTML5-Verbindungen.

Eine Bereitstellung mit direktem Zugriff eignet sich für ein Unternehmensintranet, auf dem Clients ohne Citrix Gateway oder eine andere Firewall eine Verbindung herstellen. Sie stellen ein Setup mit Direktzugriff bereit, wenn Citrix SD-WAN WANOP-Appliances im Inlinemodus bereitgestellt werden und ein Client aus einem privaten WAN eine Verbindung mit den VDA-Ressourcen herstellt.

### Direkter Zugriff mit End-to-End-SSL-Verschlüsselung:

Die folgende Abbildung zeigt die Bereitstellungstopologie von Citrix Receiver für HTML5, die auf dem Client im Direktzugriffsmodus installiert ist, der mit End-to-End-SSL-Verschlüsselung gesichert ist.

Citrix SD-WAN WANOP-Appliances im Direktzugriffsmodus bereitgestellt, gesichert mit End-to-End-SSL-Verschlüsselung



Der direkte Zugriff mit End-to-End-SSL-Verschlüsselungsmodus ähnelt dem Direct Access-Modus, mit dem Unterschied, dass die Verbindung zwischen den Client- und VDA-Ressourcen durch SSL-Verschlüsselung gesichert ist und Port 443 anstelle von Port 8008 für die Verbindung verwendet.

Bei dieser Bereitstellung wird die Kommunikation zwischen einem Paar Citrix SD-WAN WANOP-Appliances durch die Herstellung der beiden Appliance-gesicherten Partner gesichert. Diese Bereitstellung eignet sich für ein Unternehmensnetzwerk, in dem Verbindungen zwischen Client- und VDA-Ressourcen durch SSL-Verschlüsselung gesichert sind.

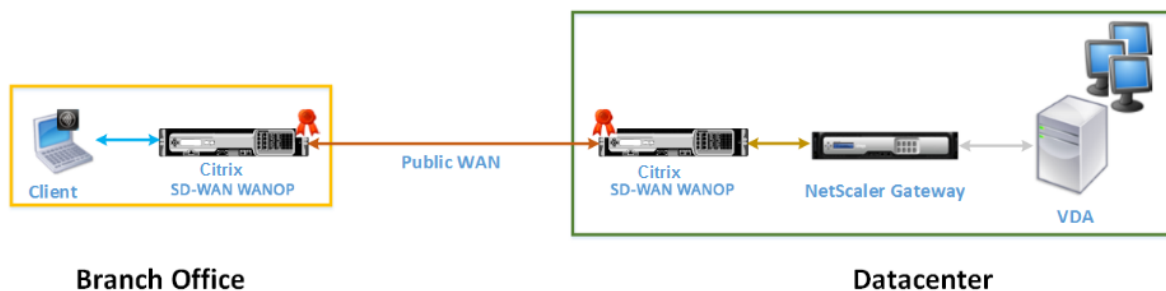
#### Hinweis

Sie müssen entsprechende Zertifikate auf den Appliances konfigurieren, um sichere Partner zu erstellen. Weitere Hinweise zum sicheren Partnering finden Sie unter [Sicheres Peering](#).

#### ICA-Proxy-Modus:

Die folgende Abbildung zeigt die Bereitstellungstopologie von Citrix Receiver für HTML5, die auf dem Client im ICA-Proxymodus installiert ist.

Citrix SD-WAN WANOP-Appliances im ICA-Proxy-Modus bereitgestellt



Im ICA-Proxy-Modus wird ein Paar Citrix SD-WAN WANOP-Appliances in der gesamten Zweigstelle und ein Rechenzentrum im Inlinemodus installiert. Darüber hinaus installieren Sie Citrix Gateway, das VDA proxyiert, im Rechenzentrum. Ein Client greift über das öffentliche WAN über Citrix Receiver für HTML5 auf VDA-Ressourcen zu. Da das Gateway den VDA proxyiert, werden zwei Verbindungen hergestellt: eine SSL-Verbindung zwischen dem Client und Citrix Gateway und eine ICA-gesicherte Verbindung zwischen Citrix Gateway und VDA. Das Citrix Gateway baut im Auftrag des Clients eine Verbindung mit VDA-Ressourcen auf. Verbindungen vom Gateway zu den VDA-Ressourcen werden durch Verschlüsselung auf ICA-Ebene gesichert.

Nachrichten, die zwischen dem Client und dem VDA ausgetauscht werden, werden unter Grundlegendes zu Nachrichten, die zwischen dem Client und dem Server ausgetauscht werden, erläutert. In diesem Fall wird die Verbindung jedoch bei Citrix Gateway beendet. Das Gateway dient also Proxy für den VDA und öffnet eine Verbindung zu VDA erst, nachdem das Gateway die WebSocket-Autorisierung ausgehandelt hat. Das Gateway übergibt Nachrichten dann transparent vom Client an den VDA und umgekehrt.

Wenn Sie erwarten, dass Benutzer über ein öffentliches WAN auf VDA-Ressourcen zugreifen, können Sie den eingerichteten ICA-Proxy-Modus bereitstellen.

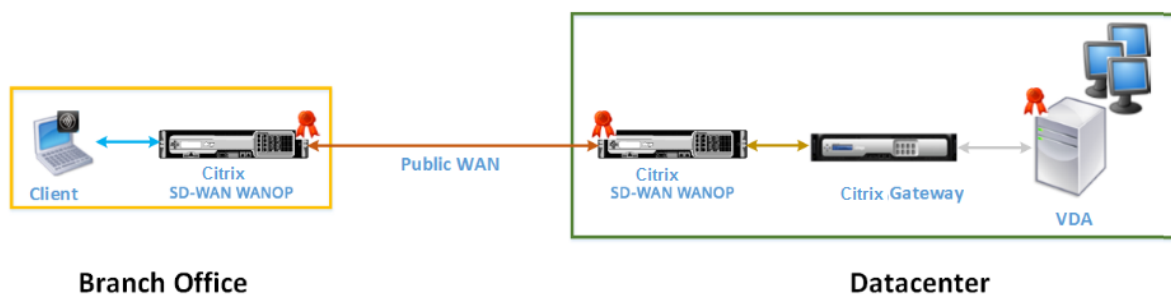
#### Hinweis

Sie müssen entsprechende Zertifikate auf den Appliances konfigurieren, um sichere Partner zu erstellen. Weitere Hinweise zum sicheren Partnering finden Sie unter [Sicheres Peering](#).

#### ICA-Proxy-Modus mit End-to-End-SSL-Verschlüsselung:

Die folgende Abbildung zeigt die Bereitstellungstopologie von Citrix Receiver für HTML5, die auf dem Client im ICA-Proxymodus installiert ist, der mit End-to-End-SSL-Verschlüsselung gesichert ist.

Citrix SD-WAN WANOP-Appliances im ICA-Proxy-Modus bereitgestellt, gesichert mit End-to-End-SSL-Verschlüsselung



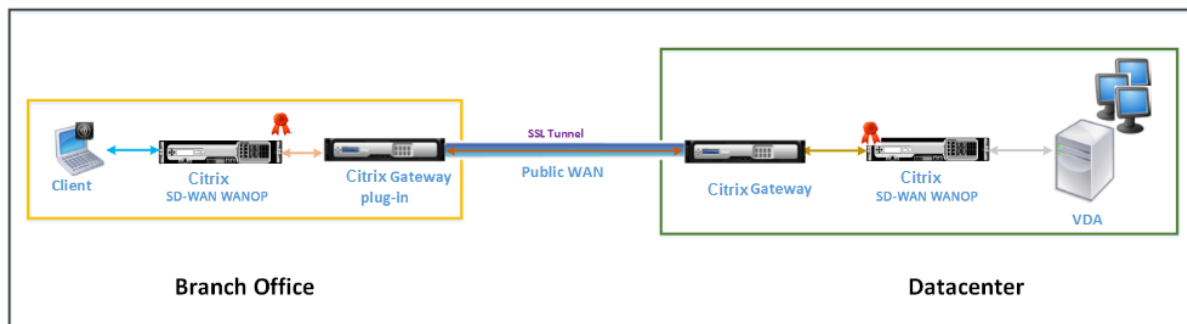
Der ICA-Proxy-Modus mit End-to-End-SSL-Verschlüsselungsmodus ähnelt dem normalen ICA-Proxy-Modus, mit dem Unterschied, dass die Verbindung zwischen dem Citrix Gateway und dem VDA durch SSL-Verschlüsselung gesichert ist, anstatt eine ICA-gesicherte Verbindung zu verwenden. In diesem Szenario müssen Sie entsprechende Zertifikate auf der Citrix SD-WAN WANOP Appliance und VDA installieren. Die Verbindung zwischen dem Citrix Gateway und dem VDA verwendet Port 443 anstelle von Port 8008, wie im Fall des normalen ICA-Proxy-Modus.

Diese Bereitstellung eignet sich für ein Netzwerk, in dem Sie die End-to-End-Kommunikation zwischen Clients und VDA sichern müssen, einschließlich der Verbindung zwischen Citrix Gateway und VDA.

#### **Volle VPN-Modus (Virtual Private Network):**

Die folgende Abbildung zeigt die Bereitstellungstopologie von Citrix Receiver für HTML5, die auf dem Client im vollständigen VPN-Modus (Virtual Private Network) installiert ist.

Citrix SD-WAN WANOP-Appliances im VPN-Modus bereitgestellt



Im vollständigen VPN-Modus wird ein Paar Citrix SD-WAN WANOP-Appliances in einer Zweigstelle und im Rechenzentrum im Inlinemodus installiert. Zusätzlich zu Citrix Receiver für HTML5 installieren Sie das Citrix Gateway-Plugin auf dem Client und Citrix Gateway, das ein externes Netzwerk im Rechenzentrum anbietet. Das Citrix Gateway-Plugin auf dem Client und Citrix Gateway im Rechenzentrum erstellen einen SSL-Tunnel oder ein VPN über das Netzwerk, wenn sie eine Verbindung herstellen. Infolgedessen hat der Client einen direkten sicheren Zugriff auf die VDA-Ressourcen mit transparenter Verbindung über die Citrix SD-WAN WANOP-Appliance. Wenn die Clientverbindung bei Citrix Gateway beendet wird, öffnet das Gateway eine transparente Verbindung zu Port 8008 auf dem VDA.

Nachrichten, die zwischen dem Client und dem VDA ausgetauscht werden, werden im Abschnitt Grundlegendes zu den zwischen dem Client und dem Server ausgetauschten Nachrichten erläutert. In diesem Fall wird die Verbindung jedoch bei Citrix Gateway beendet. Das Gateway dient als Proxy für den VDA und öffnet eine transparente Verbindung zu VDA an Port 8008 und übergibt transparent alle Nachrichten vom Client an den VDA und umgekehrt.

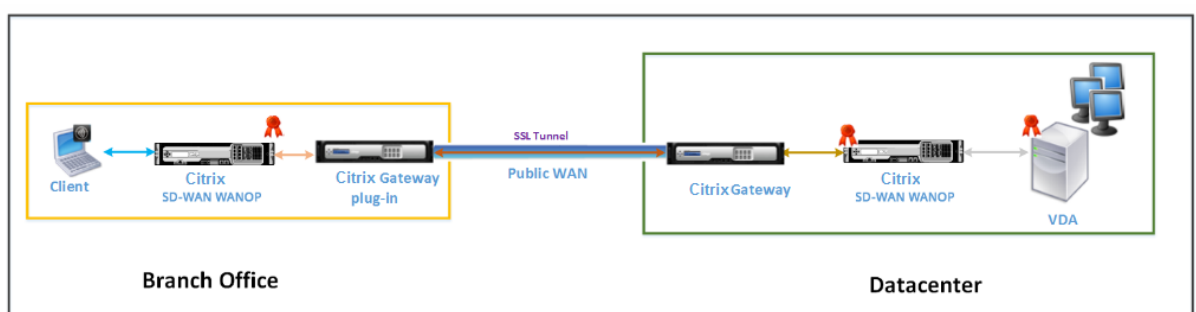
Das Citrix SD-WAN WANOP-Plug-In ermöglicht dem Client den Zugriff auf Ressourcen unabhängig vom Standort des Clients. Wenn Sie erwarten, dass Clients Zugriff auf die VDA-Ressourcen von anderen Standorten als ihren Desktops benötigen, können Sie das Setup im VPN-Modus (Full Virtual Private Network) bereitstellen.

Diese Bereitstellung eignet sich für Organisationen, die erwarten, dass ihre Mitarbeiter auf Reisen auf Ressourcen zugreifen.

### **Vollständiger VPN-Modus (Virtual Private Network) mit End-to-End-SSL-Verschlüsselung:**

Die folgende Abbildung zeigt die Bereitstellungstopologie von Citrix Receiver für HTML5, die auf dem Client im vollständigen VPN-Modus installiert ist, der mit End-to-End-SSL-Verschlüsselung gesichert ist.

Citrix SD-WAN WANOP-Appliances im VPN-Modus bereitgestellt, gesichert mit End-to-End-SSL-Verschlüsselung



Der vollständige Virtual Private Network (VPN) -Modus mit End-to-End-SSL-Verschlüsselung ähnelt dem normalen Voll-VPN-Modus, mit dem Unterschied, dass die Kommunikation zwischen Citrix Gateway und VDA durch SSL-Verschlüsselung gesichert ist und Port 443 anstelle von Port 8008 verwendet.

Diese Bereitstellung eignet sich für Organisationen, die eine End-to-End-SSL-Verschlüsselung für Ressourcen benötigen, auf die die Mitarbeiter zugreifen, die unterwegs sind.

## **Adaptive Interoperabilität des Verkehrs**

April 19, 2021

Adaptiver Transport ist eine Datenübertragungsmethode für Citrix Virtual Apps and Desktops. Sie ist schneller, passt sich an, verbessert die Anwendungsinteraktivität und ist bei schwierigen Langstrecken-WAN- und Internetverbindungen interaktiver. Adaptiver Transport bietet eine hohe Serverskalierbarkeit und eine effiziente Bandbreitennutzung. Bei Verwendung des adaptiven Transports reagieren virtuelle ICA-Kanäle automatisch auf veränderliche Netzwerkbedingungen. Sie wechseln automatisch zwischen dem Citrix Protokoll Enlightened Data Transport (EDT) und TCP, um die beste Leistung zu erzielen. Standardmäßig ist der adaptive Transport aktiviert, und EDT wird nach Möglichkeit mit Fallback auf TCP verwendet.

Citrix SD-WAN WANOP bietet sitzungsübergreifende tokenisierte Komprimierung (Datenduplizierung), einschließlich URL-basierter Video-Caching. Sie reduziert die Bandbreite, wenn zwei oder mehr Personen am Standort des Büros das gleiche vom Client abgerufen Video ansehen oder signifikante Teile derselben Datei oder Dokument übertragen oder drucken. Die Prozesse zur ICA-Datenreduktion und Druckauftragskomprimierung auf dem Zweigstellengerät entlasten zudem die VDA-Server-CPU und sorgen für eine bessere Skalierbarkeit von Citrix Virtual Apps and Desktops-Servern.

Wenn TCP als Datentransportprotokoll verwendet wird, unterstützt Citrix SD-WAN WANOP die oben beschriebene Optimierung. Wenn Sie Citrix SD-WAN WANOP bei Netzwerkverbindungen verwenden, wählen Sie TCP und deaktivieren Sie EDT. Durch die Verwendung der TCP-Flusssteuerung und der Überlastungssteuerung stellt Citrix SD-WAN WANOP die äquivalente Interaktivität mit EDT bei hoher Latenz und moderater Paketverluste sicher.

Informationen zur Konfiguration des adaptiven Transports auf Citrix Virtual Apps and Desktops finden Sie unter [Adaptiver Transport](#).

## Citrix Hypervisor 6.5-Upgrade

April 19, 2021

### Wichtig

**Für ein Upgrade auf Citrix Hypervisor Version 6.5 müssen die Appliances die Citrix SD-WAN WANOP-Softwareversion 9.0.x oder höher ausführen.**

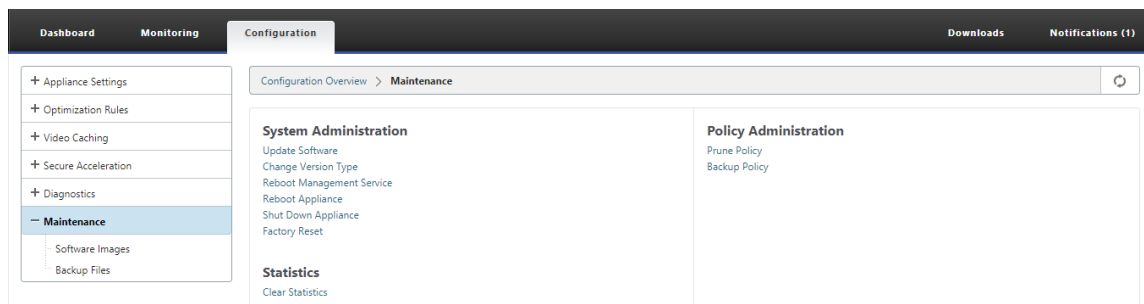
### Hinweis

Versuchen Sie nicht, ein Upgrade durchzuführen, wenn die Appliance mit einer niedrigeren Softwareversion als Version 9.0.x ausgeführt wird, um Upgrade-Probleme zu vermeiden.

## Ausführen eines Upgrades auf Citrix Hypervisor 6.5

Um ein Upgrade auf Citrix Hypervisor 6.5 auf SD-WAN WANOP-Appliances durchzuführen, stellen Sie sicher, dass die Appliance die Softwareversionsversion 9.0.x oder höher ausführt. Wenn auf den Appliances eine ältere Softwareversion ausgeführt wird, führen Sie zuerst ein Upgrade auf die neueste Softwareversion durch.

1. Gehen Sie in Citrix SD-WAN WANOP GUI zu **Konfiguration > Wartung > Update Software**. Laden Sie die *ns-sdw-wo.upg-Datei* <Build\_No> herunter, um die Appliance zu aktualisieren.

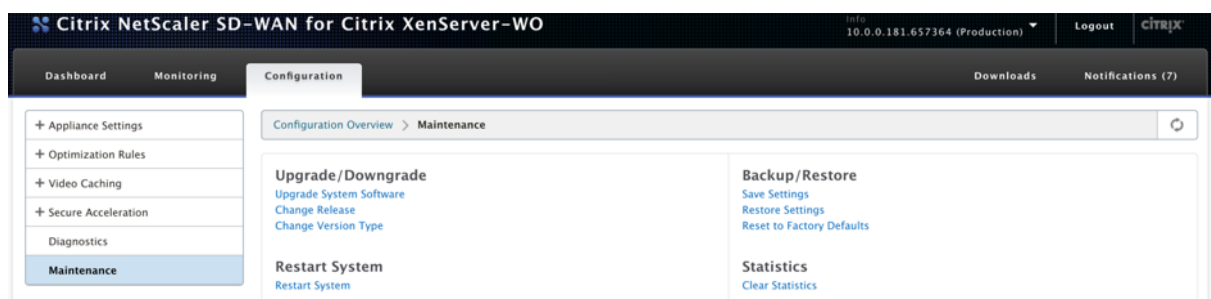


2. Nach dem Upgrade auf die neueste Softwareversion der WANOP-Software navigieren Sie in der GUI zu **Konfiguration > Wartung > Software aktualisieren**. Laden Sie die Datei *ns-sdw-xen65-pkg\_v1.5.upg hoch*.
3. Warten Sie etwa 20 Minuten, bis das Upgrade abgeschlossen ist. Die Appliance wird neu gestartet, nachdem das Upgrade erfolgreich abgeschlossen wurde.

## Wartung

April 19, 2021

Verwenden Sie die Seite **Wartung**, um Wartungsaktivitäten wie ein Upgrade von Systemsoftware, Backups und Wiederherstellen von Konfigurationen und Löschen von Statistiken durchzuführen.



## Upgrade/Downgrade

### Systemsoftware aktualisieren

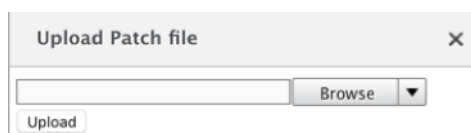
Für jedes Appliance-Modell gibt es ein anderes Citrix SD-WAN -Softwarepaket. Sie müssen das entsprechende SD-WAN WANOP-Softwarepaket für eine Appliance herunterladen, die Sie in ein Netzwerk aufnehmen möchten, und es auf Ihrem lokalen Laufwerk speichern.

Die Appliance-Software wird mithilfe von Patch-Dateien aktualisiert, die Sie von Citrix erhalten.

#### HINWEIS:

Wenn auf den Appliances eine ältere Softwareversion ausgeführt wird, müssen Sie zuerst auf die neueste Softwareversion aktualisieren.

Um die Systemsoftware zu aktualisieren, gehen Sie zu **Konfiguration > Wartung**. Wählen Sie unter **Upgrade/Downgrade** die **Option Systemsoftware** aktualisieren aus. Wählen Sie die Patch-Datei aus, und laden Sie sie auf die Appliance hoch.



Die Patch-Datei wird von der Appliance geprüft. Nur eine gültige Patchdatei kann das System auf eine andere Version aktualisieren als die aktuell verwendete Version.

Bei einem Upgrade werden Lizenzdateien und Systemeinstellungen beibehalten. Die aktualisierte Einheit erfordert keine Neukonfiguration, außer für alle neuen Funktionen, die mit der neuen Version hinzugefügt wurden.

### Änderungsfreigabe

Auf der Änderungsfreigabeseite wird die aktuell installierte Version angezeigt. Wenn Sie die Release-Version ändern möchten, klicken Sie auf **Freigabeoption ändern**, wählen Sie die Version aus der Dropdown-Liste aus, und klicken Sie auf **Ändern**.





## Versionstyp ändern

Mit der Option **Versionstyp ändern** können Sie eine Debug-Version der Version auswählen. Sie können den Versionstyp aus der Dropdown-Liste **Typ** auswählen und auf **Ändern** klicken. Im Folgenden sind die möglichen Debug-Versionen:

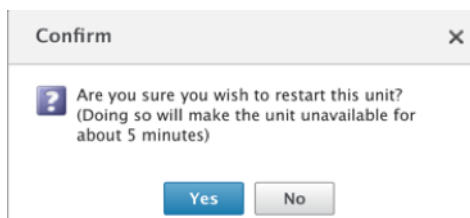
- Standard
- Ebene 1
- Ebene 2
- Standard-MC
- Stufe 1 MC
- Stufe 2 MC

Sie müssen diese Aktion ausführen, wie vom Support-Team angewiesen.

## System neu starten

Sobald ein Patch installiert ist, wird in einer Popup-Meldung gefragt, ob die Appliance neu gestartet werden kann. Der Patch wird erst angewendet, wenn die Appliance neu gestartet wird. Wenn Sie das System nicht sofort neu starten möchten, wird oben auf jeder Seite eine Erinnerung angezeigt.

Klicken Sie auf **System neu starten**, um die SD-WAN WANOP Appliance neu zu starten. Dieser Vorgang dauert einige Minuten.



## Backup-Einstellungen

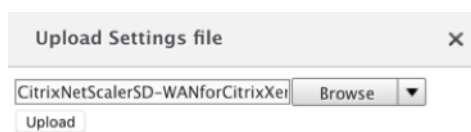
Sie können die Einheitenkonfiguration sichern, indem Sie sie als Textdatei speichern.

Klicken **Sie auf Einstellungen speichern**, eine Textdatei wird auf Ihr lokales Laufwerk heruntergeladen. Lizenzdateien, SSH-Parameter und die IP-Adressen auf der Seite Management IP können nicht gespeichert werden. Die Datei ist eine gewöhnliche Textdatei, sollte aber nicht manuell bearbeitet werden.

## Einstellungen wiederherstellen

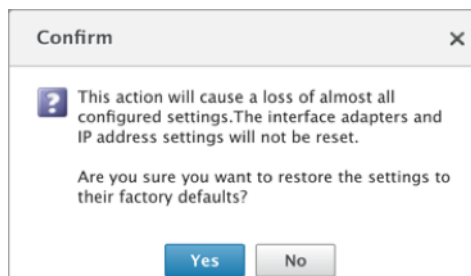
Sobald die Datei gespeichert ist, kann sie auf derselben SD-WAN WANOP Appliance wiederhergestellt werden.

Die Appliance verwaltet Kopien älterer Versionen. **Wiederherstellungseinstellungen** Option hilft, konfigurierte Einstellungen wiederherzustellen. Lizenzen, SSH-Parameter und die IP-Adressen auf der Management-IP-Seite werden nicht von der neueren Version in die ältere kopiert. Stattdessen wird die Appliance auf die Einstellungen zurückgesetzt, die zum Zeitpunkt der Aktualisierung der älteren Version in Kraft waren.



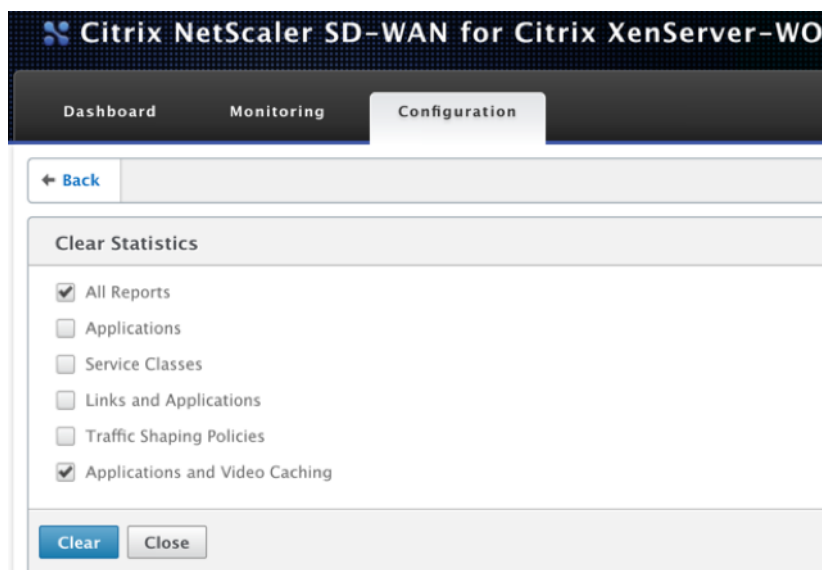
## Auf Werkseinstellungen zurücksetzen

Auf**Werkseinstellungen zurücksetzen** Option ermöglicht das Zurücksetzen der Einstellungen. Es setzt alle Parameter außer IP-Adressen, Bandbreiteneinstellungen und Lizenzen auf die Werkseinstellungen. Klicken Sie **auf Auf Werkseinstellungen zurücksetzen**. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**, wenn die Einstellungen auf die Werkseinstellungen zurückgesetzt werden sollen.



## Löschen von Statistiken

Seite **Statistiken löschen** ermöglicht das Zurücksetzen der Statistiken der SD-WAN WANOP Appliance. Außerdem können Berichte erstellt werden, die am Anfang des gewünschten Stichprobenfensters beginnen. Wählen Sie die Statistikoptionen aus, die Sie von der Appliance löschen möchten, und klicken Sie auf **Löschen**.



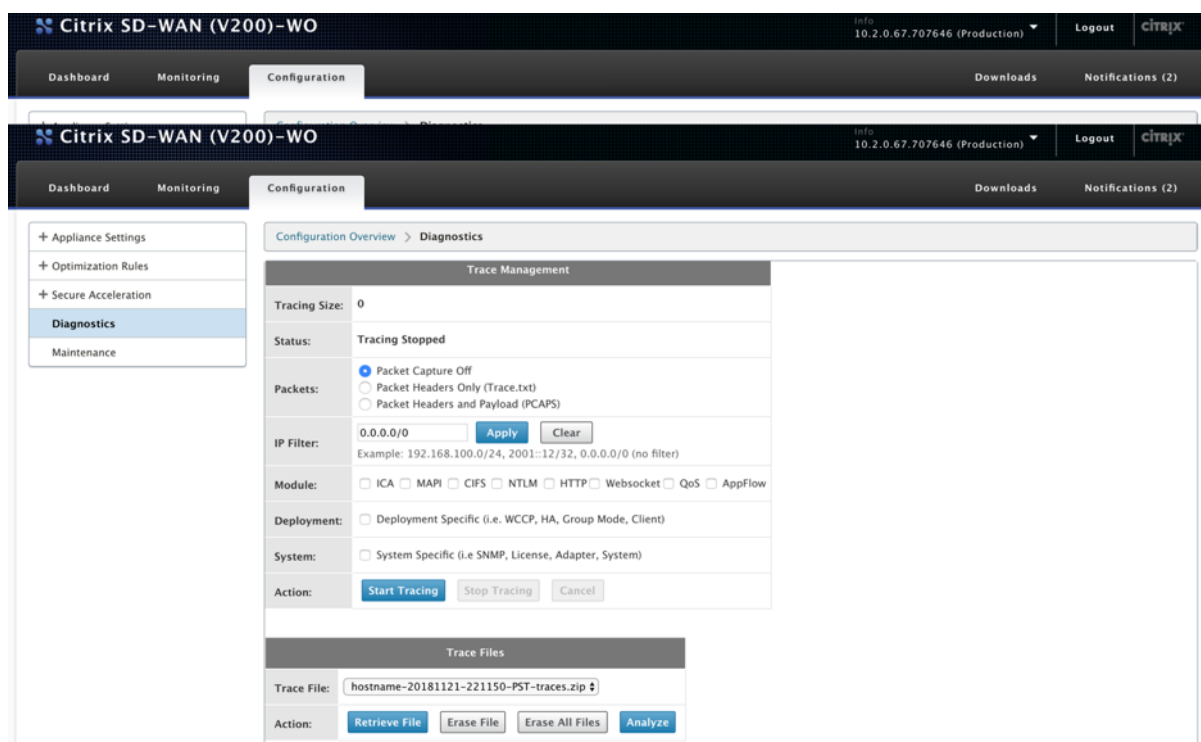
## Diagnose

April 19, 2021

Dieser Abschnitt enthält Diagnosetools, um Netzwerkprobleme in Ihrem SD-WANOP-Netzwerk zu identifizieren und diese zu beheben. Sie können auch Systemprotokolldateien, Systeminformationen und andere notwendige Details abrufen, die das Citrix SD-WAN -Support-Team bei der Diagnose und Behebung von Netzwerkproblemen unterstützen.

Im Folgenden finden Sie das Diagnose-Tool, das in SD-WAN WANOP verfügbar ist:

- Ablaufverfolgung
- Paketanalysator
- Bypasskartentest
- Kurs abrufen
- Leitungsprüfer
- Ping
- Traceroute
- Systeminformationen
- Diagnosedaten



## Ablaufverfolgung

Das **Tracing-Tool** wird verwendet, um die Pakete zu beobachten, die über das SD-WANOP-Netzwerk fließen. Es kann jedes Paket öffnen und das verwendete Protokoll, die IP-Adresse der Quelle und des Ziels sowie andere Nutzlastinformationen identifizieren. Diese Informationen werden vom Citrix Support-Team verwendet, um die Ursache von Netzwerkproblemen zu ermitteln.

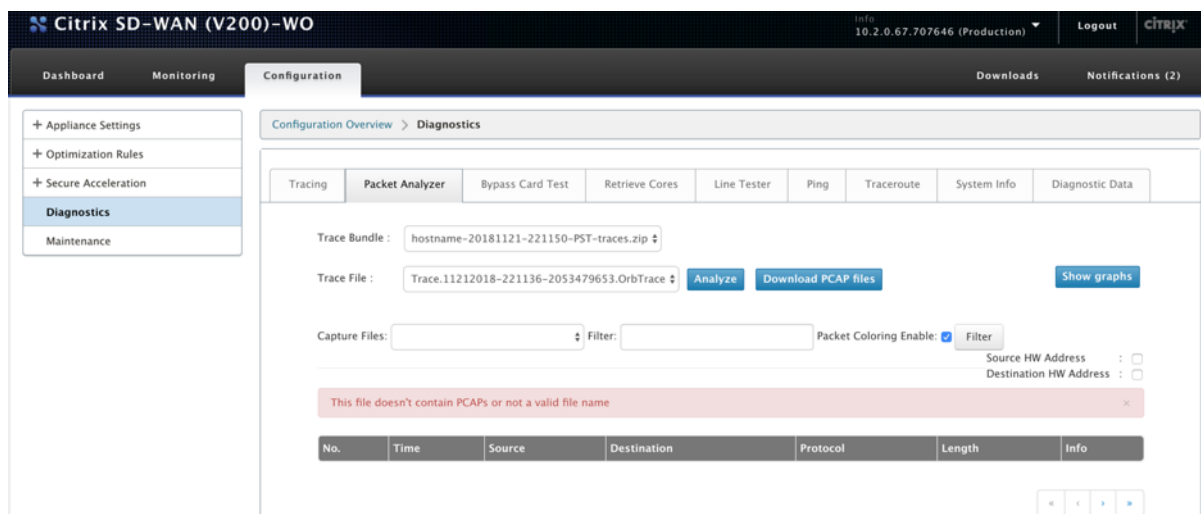
Sie können auswählen, ob **nur Paketkopfzeilen** oder **Paketkopf- und Nutzlast** verfolgt werden sollen. Sie können das Modul auswählen, das verfolgt werden soll, und angeben, ob die Ablaufverfolgung bereitstellungsspezifisch oder systemspezifisch sein soll.

Klicken Sie auf **Ablaufverfolgung starten**. Die Appliance beginnt mit der Verfolgung der Pakete. Die Ergebnisse werden

in ein ZIP-Archiv gepackt, wenn Sie auf **Ablaufverfolgung beenden** klicken. Dieses Archiv kann über die Option **Datei abrufen** auf Ihren

Computer heruntergeladen werden. Sie können diese Dateien dann an das Support-Team weiterleiten. Die Trace-Dateien liefern auch Daten zur Absturzanalyse.

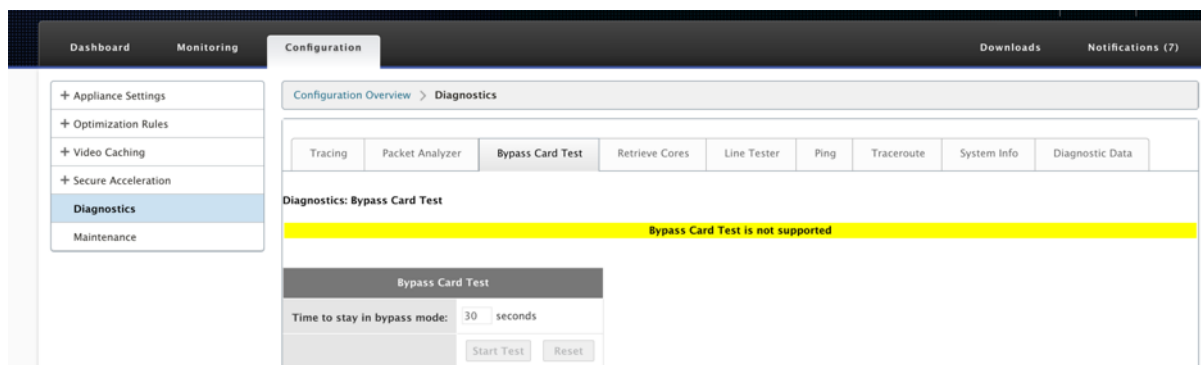
Klicken Sie auf **Analysieren**, um weitere Informationen zu den Paketen auf der Registerkarte **Packet Analyzer** anzuzeigen.



Sie können die Uhrzeit, die Quelladresse, die Zieladresse, das Protokoll, die Länge und die Nutzlastinformationen anzeigen.

## Bypasskartentest

Sie können die Fail-to-Wire-Funktionalität der Ethernet-Schnittstelle für eine Appliance-Bereitstellung im Inlinemodus (Fail-to-Wire-Modus) testen. Geben Sie die Anzahl der Sekunden ein, in denen die Appliance im Umgehungsmodus verbleibt, und klicken Sie auf **Test starten**. Während dieser Zeit wird die Appliance umgangen. Der normale Betrieb wird danach wieder aufgenommen.

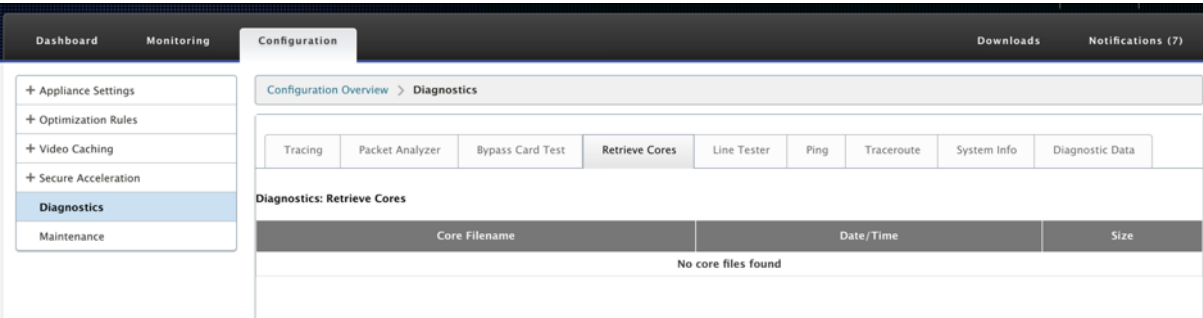


## Kerne abrufen

**Kerndateien** werden erstellt, wenn die SD-WAN WANOP Appliance abnormal beendet oder abstürzt. Die Appliance wird nach einem Absturz automatisch neu gestartet. Bei anhaltenden Abstürzen ist die Beschleunigung deaktiviert, die Verwaltungsschnittstelle bleibt jedoch aktiv.

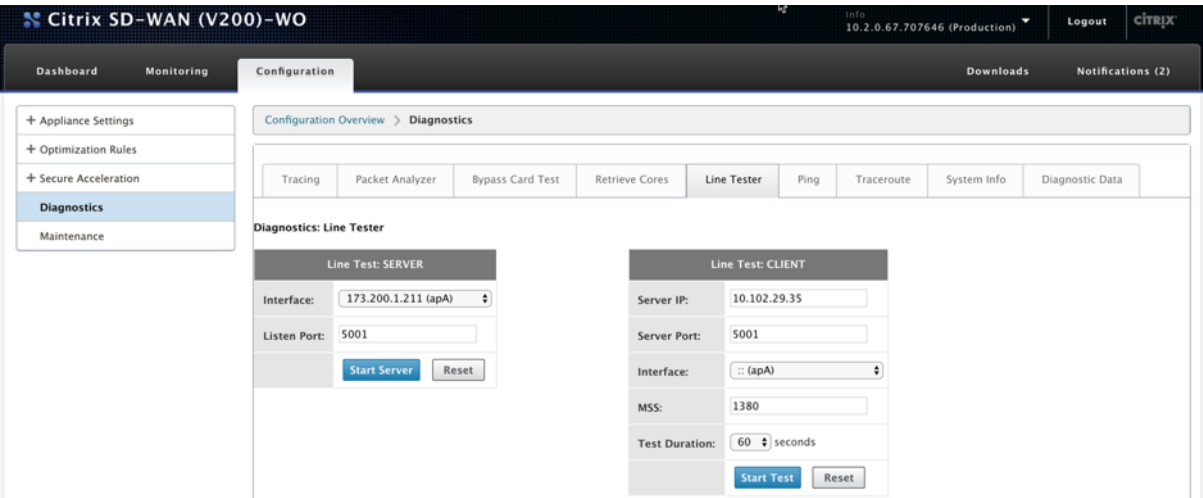
Sie können die erforderlichen Kerndateien auswählen und abrufen, die während des Absturzes der Appliance oder bei einem ungewöhnlichen Verhalten der Appliance erstellt wurden. Die abgerufenen

Dateien werden in einem ZIP-Archiv gespeichert. Sie können dies mit dem Support-Team zur weiteren Analyse teilen.



### Leitungsprüfer

Die Funktion **Line Test: SERVER** startet einen iperf-Server auf der Appliance, der im TCP-Modus ausgeführt wird. Diese Option kann verwendet werden, um die Konnektivität zwischen WANOP-Appliances und Fehlerbehebung des Netzwerkverkehrs zu überprüfen. Um iperf-Tests auszuführen, muss ein System (eine Appliance oder ein anderer Host) iperf als Server ausführen, und ein anderes muss sich als Client mit ihm verbinden.

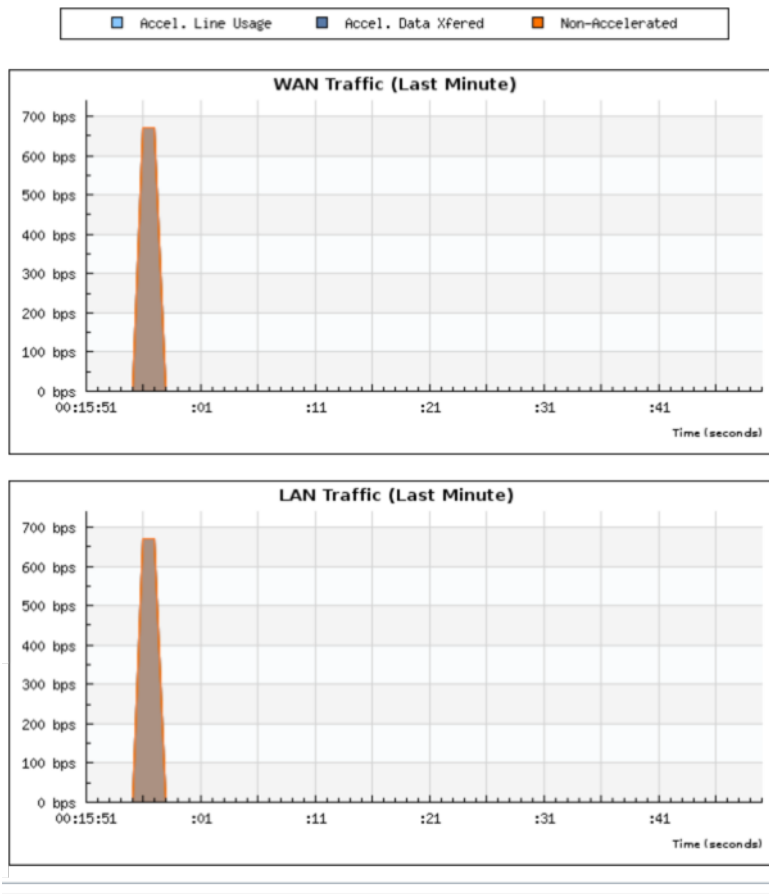


Sie können die standardmäßige **Line Tester Server-Schnittstelle** und Portnummer verwenden. Klicken Sie auf **Server starten**, um einen iperf-Server auf der Appliance zu starten.



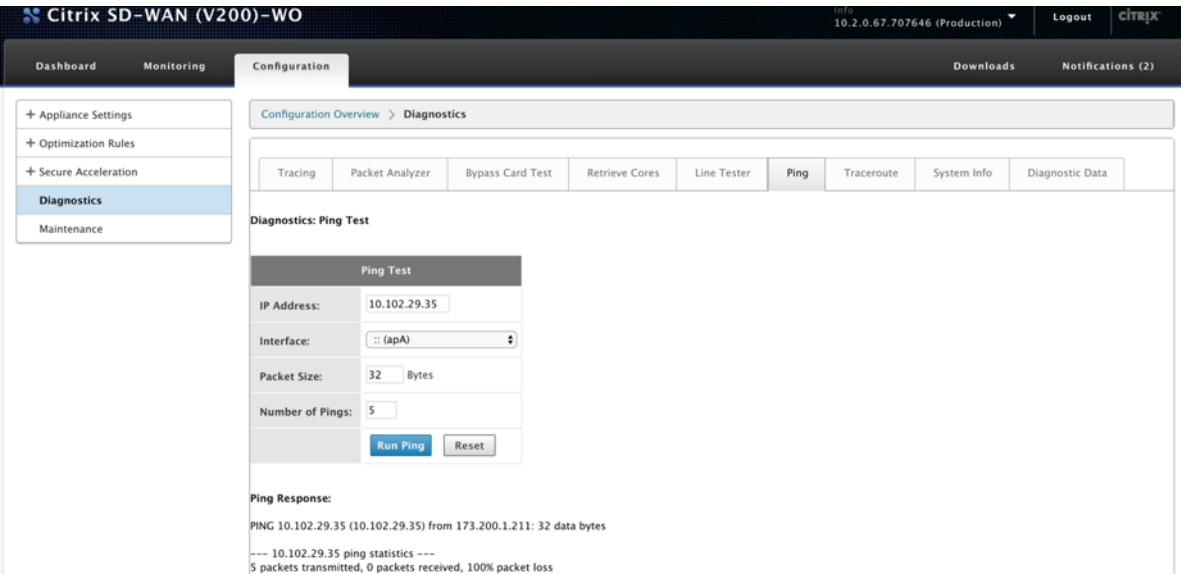
Die Funktion **Line Test: CLIENT** startet einen iperf Client auf dem Gerät, der im TCP-Modus ausgeführt wird. Sie können auch die Portnummer des iperf-Servers und die Länge des Tests angeben. Wenn der Test abgeschlossen ist, wird die Verbindungsgeschwindigkeit gemeldet. Klicken Sie auf **Test starten**, um das WAN- und LAN-Datenverkehrsergebnis anzuzeigen.

Test Results(COMPLETE)



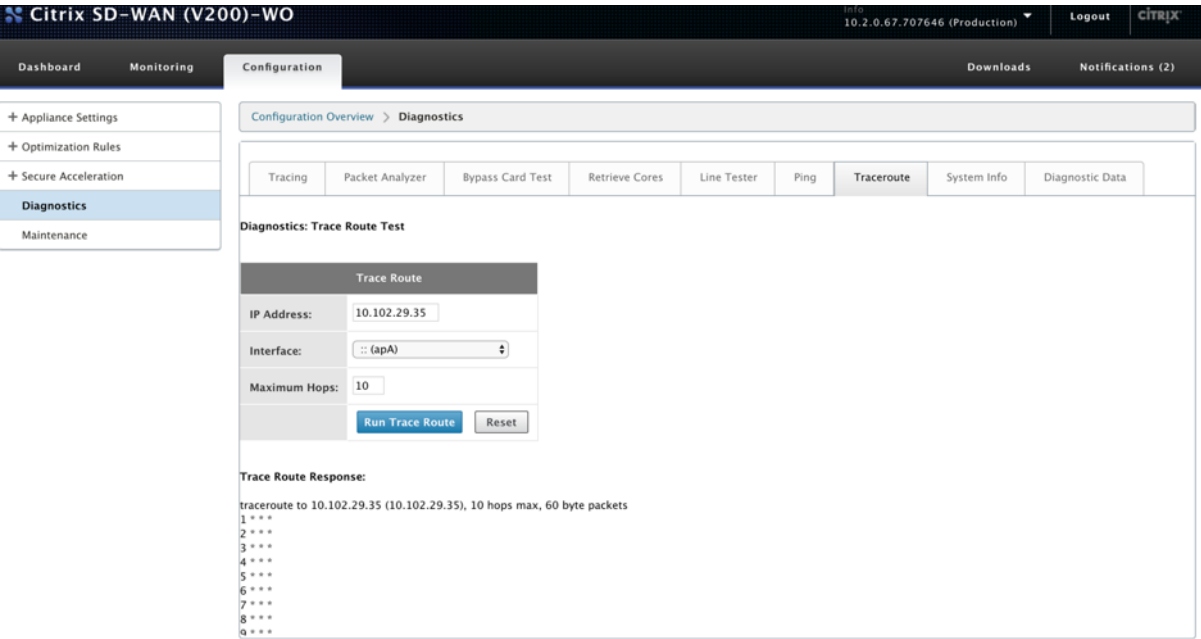
## Ping

**Ping** ermöglicht es Ihnen, die Konnektivität der Netzwerkelemente in Ihrem SD-WAN-Netzwerk zu überprüfen. Geben Sie die IP-Adresse des Netzwerkelements ein, und klicken Sie auf **Ping ausführen**, um das Ergebnis anzuzeigen.



Traceroute

Mit**Traceroute** können Sie die Route zwischen Ihrer SD-WAN-Appliance und jedem anderen Netzwerkelement in Ihrem SD-WAN-Netzwerk oder im Internet aufzeichnen. Es berechnet und zeigt die Zeit, die jeder Hop brauchte.



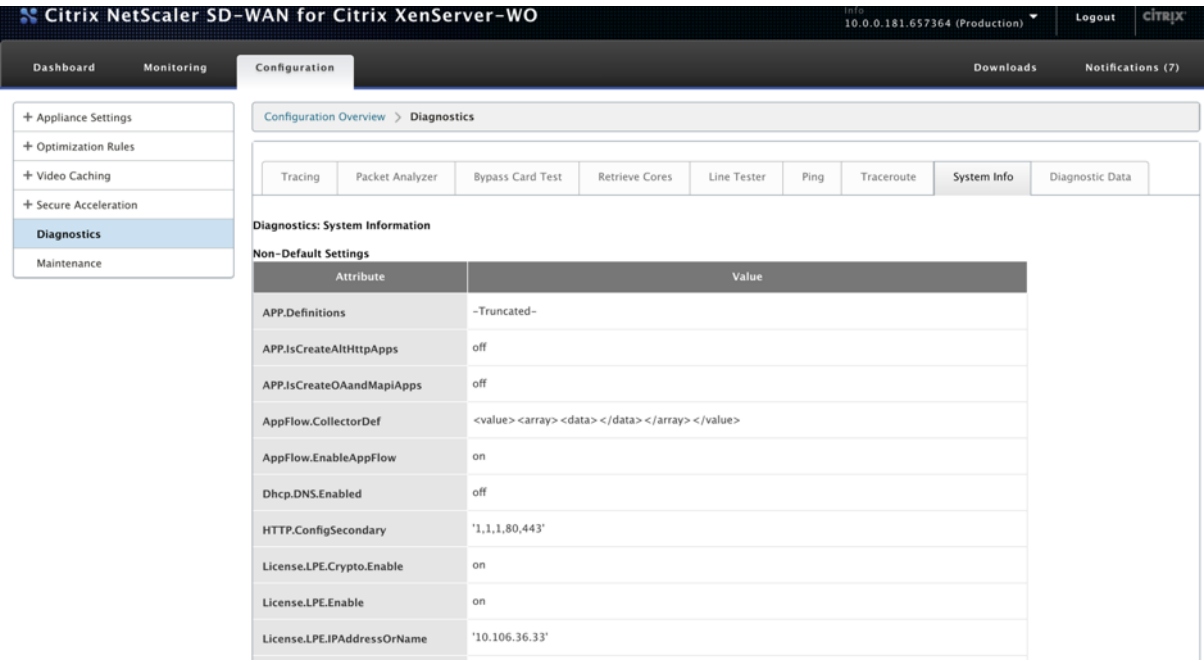
Systeminfo

Die **Systeminfo** listet alle Parameter auf, die nicht auf ihre Standardwerte gesetzt sind. Diese Informationen sind schreibgeschützt. Es wird vom Support verwendet, wenn eine Art von Fehlkonfiguration



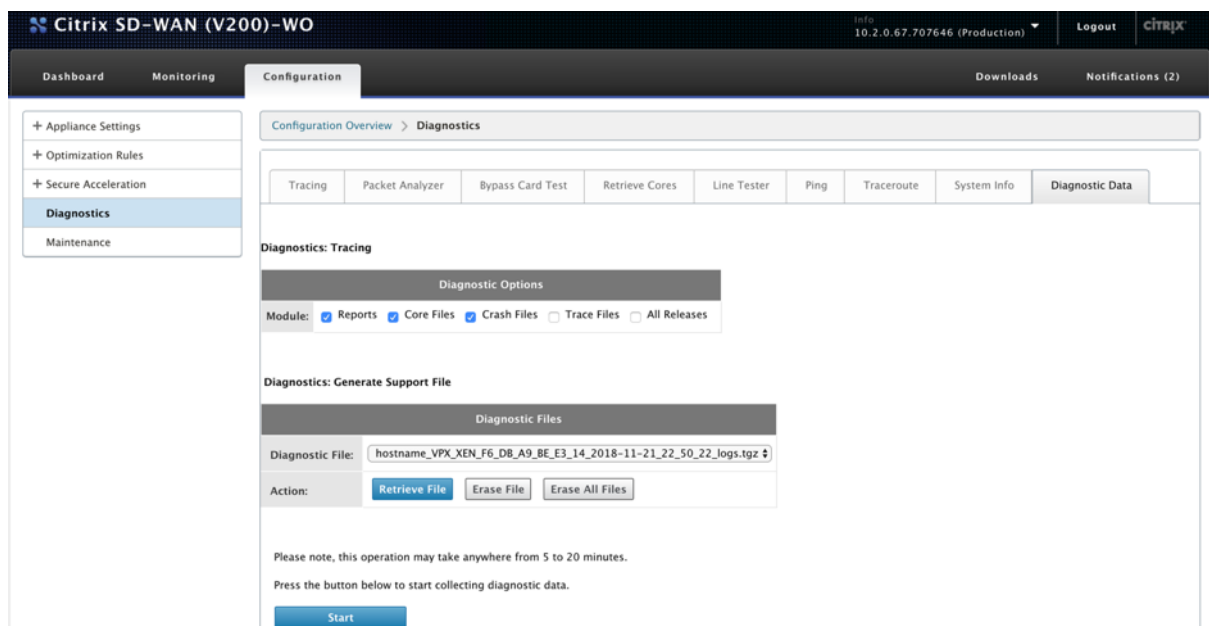
vermutet wird. Wenn Sie ein Problem melden, werden Sie möglicherweise aufgefordert, einen oder mehrere Werte auf dieser Seite zu überprüfen.

Es enthält **nicht standardmäßige Einstellungen, detaillierte Informationen für den primären Adapter, detaillierte Informationen für Adapter APA.2**und **detaillierte Informationen für Adapter APA.1.**



## Diagnosedaten

Mit**Diagnosedaten** können Sie Diagnosedaten für die Analyse durch das Citrix Support-Team verpacken. Wählen Sie die erforderlichen Diagnosedateien aus, und klicken Sie auf **Start**. Klicken Sie dann auf **Datei abrufen**, um das ZIP-Archiv herunterzuladen und es für Citrix Support freizugeben.



## Problembehandlung

April 19, 2021

Die folgenden Themen enthalten eine Liste der Probleme, die Ursache für das Problem und die Schritte zur Lösung einiger Citrix SD-WAN WANOP-Features.

[CIFS und MAPI](#)

[Citrix SD-WAN WANOP-Plug-In](#)

[RPC über HTTPS](#)

[Video-Caching](#)

[Citrix Virtual Apps and Desktops Beschleunigung](#)

## CIFS und MAPI

April 19, 2021

- **Problem:** Ein Domänencontroller wird aus dem Netzwerk entfernt. Die Citrix SD-WAN WANOP-Appliance kann die Domäne jedoch nicht verlassen.

**Ursache:** Dies ist ein bekanntes Problem mit der Appliance.

**Problemumgehung:** Ändern Sie auf der Seite Windows-Domäne den DNS in den DNS, über den Sie die beabsichtigte Domäne auflösen können. Verwenden Sie als Nächstes die Option „**Domäne erneut beitreten**“, damit die Citrix SD-WAN WANOP Appliance dieser Domäne beitrifft. Versuchen Sie nun, von der Domain zu verlassen.

- **Problem:** MAPI-Verbindungen sind nicht optimiert und die folgende Fehlermeldung wird angezeigt:

Nicht-StandardEinstellung in Outlook wird nicht unterstützt

**Ursache:** Dies ist ein bekanntes Problem mit Version 6.2.3 und früheren Versionen.

**Lösung:** Aktualisieren Sie die Appliance auf die neueste Version.

- **Problem:** Die Appliance hat die MAPI-Verbindungen optimiert. Die Überwachungsseiten zeigen jedoch die Anzahl der gesendeten und empfangenen Bytes als Null an.

**Ursache:** Dies ist ein bekanntes Problem mit der Appliance.

**Lösung:** Dies ist ein gutartiges Problem und hat keinen Einfluss auf die Funktionalität der Appliance. Sie können es ignorieren.

- **Problem:** Es konnte kein sicheres Peering zwischen Citrix SD-WAN WANOP-Appliances hergestellt werden.

**Ursache:** Das sichere Peering mit der Partner-Appliance ist nicht ordnungsgemäß konfiguriert.

**Lösung:** Gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass Sie die entsprechende Kombination von Zertifizierungsstellen- und Serverzertifikaten auf die Appliance hochgeladen haben.
  2. Navigieren Sie zur Seite **Citrix SD-WAN WANOP > Configuration > SSL-Einstellungen > Secure Partners**.
  3. Wählen Sie im Abschnitt **Partnersicherheit** unter **Zertifikatüberprüfung** die Option **Keine - alle Anforderungen zulassen** aus, um sicherzustellen, dass das Zertifikat nie abläuft.
  4. Stellen Sie sicher, dass die Appliance ein sicheres Peering mit der Partner-Appliance einrichten kann.
  5. Stellen Sie sicher, dass der Abschnitt „**Listen On**“ einen Eintrag für die IP-Adresse der vorgesehenen Citrix SD-WAN WANOP Appliance enthält.
- **Problem:** Beim Herstellen einer Verbindung mit einem Exchange-Cluster werden Outlook-Benutzer mit optimierten Verbindungen gelegentlich umgangen oder aufgefordert, Anmeldeinformationen einzugeben.

**Ursache:** Die MAPI-Optimierung erfordert, dass jeder Knoten im Exchange-Cluster mit dem ExchangemDB-Dienstprinzipalnamen (SPN) verknüpft ist. Im Laufe der Zeit fügen Sie dem

Cluster zusätzliche Knoten hinzu, da Sie mehr Kapazität benötigen. Manchmal ist die Konfigurationsaufgabe jedoch möglicherweise nicht abgeschlossen, sodass einige Knoten im Cluster ohne SPN-Einstellungen bleiben. Dieses Problem ist am häufigsten in Exchange-Clustern mit Exchange Server 2003 oder Exchange Server 2007.

**Lösung:** Führen Sie auf jedem Exchange-Server in der Einrichtung die folgenden Schritte aus:

1. Greifen Sie auf den Domänencontroller zu.
2. Öffnen Sie die Eingabeaufforderung.
3. Führen Sie die folgenden Befehle aus:

```
pre codeblock setspn -A exchangeMDB/Exchange1 Exchange1
setspn -A exchangeMDB/Exchange1.example.com Exchange1 <!--
NeedCopy-->
```

- **Problem:** Beim Versuch, eine Verbindung mit Outlook herzustellen, wird die Meldung Verbindungsversuchen angezeigt, und dann wird die Verbindung beendet.

**Ursache:** Die clientseitige Citrix SD-WAN WANOP-Appliance enthält Einträge in der Sperrliste, die auf der serverseitigen Appliance nicht vorhanden sind.

**Lösung:** Entfernen Sie die Sperrlisteneinträge von beiden Appliances, oder (empfohlen) aktualisieren Sie die Software der Appliances auf Version 6.2.5 oder höher.

- **Problem:** Die Appliance kann der Domäne nicht beitreten, selbst nachdem die Prüfungen vor der Domäne bestanden haben.

**Ursache:** Dies ist ein bekanntes Problem.

**Lösung:** Gehen Sie folgendermaßen vor:

1. Greifen Sie mithilfe eines SSH-Dienstprogramms auf die Appliance zu.
2. Melden Sie sich mit den Stammanmeldeinformationen bei der Appliance an.
3. Führen Sie den folgenden Befehl aus:

```
/opt/wiewise/bin/domainjoin-cli treten <Domain_Name> administrator
```

- **Problem:** Die LDAPerror-Fehlermeldung wird angezeigt, wenn Sie einen Delegate-Benutzer zur Citrix SD-WAN WANOP-Appliance hinzufügen.

**Lösung:** Führen Sie einen der folgenden Schritte aus:

- Stellen Sie auf dem DNS-Server der Citrix SD-WAN WANOP-Appliance sicher, dass für jede IP-Adresse des Domänencontrollers eine Reverse-Lookup-Zone konfiguriert ist.
- Stellen Sie sicher, dass die Systemuhr des Clientcomputers mit der Systemuhr des Active Directory -Servers synchronisiert ist. Bei Verwendung von Kerberos müssen diese Uhren synchronisiert werden.

- Aktualisieren Sie den Delegatbenutzer auf der Seite Windows-Domäne, indem Sie das Kennwort für den Delegatbenutzer erneut angeben.

- **Problem:** Die Fehlermeldung Time Skew wird angezeigt, wenn Sie einen Delegate-Benutzer zur Citrix SD-WAN WANOP-Appliance hinzufügen.

**Lösung:** Stellen Sie sicher, dass die Appliance der Domäne beigetreten ist. Wenn nicht, verbinden Sie die Appliance mit der Domäne. Dadurch wird die Appliance-Zeit mit der Domain-Server-Zeit synchronisiert und das Problem behoben.

- **Problem:** Der Client wird vorübergehend zur Beschleunigung ausgeschlossen. Die letzte Fehlermeldung (Kerberos-Fehler.) wird angezeigt, wenn Sie einen delegierten Benutzer zur Citrix SD-WAN WANOP-Appliance hinzufügen.

**Ursache:** Der Delegatbenutzer ist für die Authentifizierung **Nur Kerberos verwenden** konfiguriert.

**Lösung:** Stellen Sie sicher, dass auf dem Domänencontroller die Authentifizierungseinstellung des Delegatbenutzers auf **Beliebiges Authentifizierungsprotokoll verwenden** lautet.

- **Problem:** Die Fehlermeldung Delegate user not ready wird angezeigt, wenn Sie einen Delegate-Benutzer zur Citrix SD-WAN WANOP-Appliance hinzufügen.

**Auflösung:** Wenn die Meldung nur auf der clientseitigen Appliance angezeigt wird, ignorieren Sie sie. Wenn die Meldung jedoch auf der serverseitigen Appliance angezeigt wird, führen Sie das auf der Seite **Windows-Domäne** verfügbare Vorprüfungstool für Delegaten aus, und konfigurieren Sie dann den Delegatbenutzer auf der serverseitigen Appliance.

- **Problem:** Der letzte Fehler (Der Server ist nicht für die Kerberos-Authentifizierung delegiert. Bitte fügen Sie den Delegatbenutzer, die Prüfliste für Dienste und den Server hinzu, der zur Delegierung zugelassen ist.) UR:4-Fehlermeldung wird angezeigt, wenn Sie der Citrix SD-WAN WANOP-Appliance einen Delegatbenutzer hinzufügen.

**Lösung:** Stellen Sie sicher, dass der Delegatbenutzer korrekt auf dem Domänencontroller konfiguriert ist und dass Sie dem Domänencontroller entsprechende Dienste hinzugefügt haben.

- **Problem:** Die Appliance kann der Domäne nicht beitreten.

**Lösung:** Führen Sie das auf der Seite Windows-Domäne verfügbare Domänenvorprüfungstool aus, und beheben Sie ggf. die Probleme. Wenn das Domänenvorprüfungstool keine Probleme meldet, wenden Sie sich an den technischen Support von Citrix, um weitere Unterstützung bei der Lösung des Problems zu erhalten.

## Citrix SD-WAN WANOP-Plug-In

April 19, 2021

- **Problem:** Ich habe Probleme mit der Signalkanalkonnektivität. Wie kann ich diese Probleme lösen?

**Lösung:** Um Probleme mit der Signalkanalkonnektivität zu beheben, führen Sie die folgenden Schritte zur Fehlerbehebung durch:

- Stellen Sie sicher, dass Sie die Signalisierungs-IP-Adresse korrekt konfiguriert haben. Sie können dies tun, indem Sie die signalisierende IP-Adresse pingen und die Antwort überprüfen.
  - Stellen Sie sicher, dass der Signalstatus auf der WANOP-Appliance aktiviert ist.
  - Stellen Sie sicher, dass die im Netzwerk installierte Firewall die WANOP TCP-Optionen nicht entfernt.
  - Stellen Sie sicher, dass eine gültige WANOP-Plug-In-Lizenz auf der WANOP-Appliance installiert ist.
  - Stellen Sie sicher, dass die Konfiguration der Signalkanalquellenfilterung die IP-Adresse der Clientquelle nicht blockiert.
  - Wenn Sie die LAN-Erkennung aktiviert haben, stellen Sie sicher, dass die RoundTrip-Zeit zwischen dem WANOP-Plug-In und der WANOP-Appliance ein akzeptabler Wert ist.
- **Problem:** Bei einer WANOP 4000-Appliance kann ich das WANOP-Plug-In nicht deaktivieren.  
**Ursache:** Dies ist ein bekanntes Problem.  
**Auflösung:** Keine. Sie können das WANOP-Plug-In auf einer WANOP 4000-Appliance nicht deaktivieren.
  - **Problem:** Beim Herstellen einer Verbindung mit der WANOP-Appliance mithilfe des WANOP-Plug-Ins wird der folgende Fehlermeldungseintrag auf der Registerkarte Warnungen protokolliert:  
  
Mehr WANOP-Plug-Ins als das aktuelle Limit von <Number> haben versucht, eine Verbindung zu dieser Appliance herzustellen.  
  
**Ursache:** Die Anzahl der Verbindungen mit der WANOP-Appliance hat das Limit für lizenzierte Benutzer überschritten.  
  
**Lösung:** Warten Sie entweder, bis ein Benutzer die Verbindung getrennt hat, oder beenden Sie eine Verbindung.

- **Problem:** Falsche Signalisierungs-IP-Adresse ist auf einer WANOP 4000- oder 5000-Appliance konfiguriert.

**Lösung:** Führen Sie folgende Schritte aus, um die Signalisierungs-IP-Adresse auf einer WANOP 4000- oder 5000-Appliance zu aktualisieren:

1. Melden Sie sich bei der Citrix Instanz der WANOP Appliance an.
2. Navigieren Sie zur Seite **Traffic Management > Load Balancing > Virtuelle Server > BR\_LB\_VIP\_SIG**.
3. Aktualisieren Sie die signalisierende IP-Adresse.
4. Speichern Sie die Konfiguration.

- **Problem:** CIFS- und ICA-Verkehr wird nicht beschleunigt.

**Lösung:** Um dieses Problem zu beheben, führen Sie die folgenden Schritte zur Fehlerbehebung durch:

- Stellen Sie sicher, dass Beschleunigungsregeln für IP-Adresse und Portnummern für das WANOP-Plug-In korrekt definiert sind.
- Stellen Sie sicher, dass CIFS- oder ICA-Verbindungen hergestellt werden, nachdem die Signalverbindung erfolgreich war.
- Überprüfen Sie die Beschleunigungsrichtlinie für die verwendete Serviceklasse.

## RPC über HTTPS

April 19, 2021

- **Problem:** Nach dem Upgrade der Software der Appliance auf Version 7.3 haben die Überwachungsberichte keine spezielle Kategorie für RPC-über-HTTPS-Verbindungen.

**Ursache:** Wenn Sie die Appliance auf Version 7.3 aktualisieren, gehören die RPC-über-HTTPS-Anwendungen nicht zu ihrer eigenen Serviceklasse. Daher werden alle RPC-über-HTTPS-Verbindungen in den Berichten als TCP-Andere Verbindungen aufgeführt.

**Lösung:** Um diese Verbindungen als RPC-über-HTTPS-Verbindungen zu kategorisieren, erstellen Sie eine Serviceklasse für diese Anwendungen.

- **Problem:** Nach dem Erstellen einer Dienstklasse für RPC über HTTPS wird der gesamte HTTP- und HTTPS-Datenverkehr als RPC über HTTP kategorisiert.

**Ursache:** Sie haben die Ziel-IP-Adresse nicht zu der Dienstklasse hinzugefügt, die Sie für RPC-über-HTTPS-Anwendungen erstellt haben.

**Lösung:** Ändern Sie die Dienstklasse, die Sie für RPC über HTTPS-Anwendungen erstellt haben, indem Sie die Ziel-IP-Adressen Ihrer Server hinzufügen.

## Video-Caching

April 19, 2021

- **Problem:** Nach dem Hinzufügen eines Eintrags zur Liste der Vorbestückungsvorgänge befindet sich der Eintrag weiterhin im Status Konfiguriert.

**Ursache:** Ein Vorbevölkerungsvorgang dauert etwa eine Minute in den Downloadstatus.

**Lösung:** Überprüfen Sie den Status des Eintrags nach einer Minute oder aktualisieren Sie die Seite, um zu überprüfen, ob sich der Status in Herunterladen ändert.

- **Problem:** Nach dem Hinzufügen eines Eintrags zur Liste der Vorbevölkerungsaufgaben zeigt der Status des Eintrags FEHLER 403 an. Die Website funktioniert jedoch in einem Webbrowser einwandfrei.

**Ursache:** Die IP-Adresse des Citrix SD-WAN WANOP APA hat keinen Zugriff auf den Videosever.

**Lösung:** Um dieses Problem zu beheben, überprüfen und aktualisieren Sie Folgendes:

- Zugriffsregeln über die Firewalls hinweg
- Quell-IP-Adressbeschränkungen in der httpd.conf-Datei des Videosevers

**Ursache:** Der Videosever unterstützt die HEAD-Methode nicht.

**Lösung:** Der Videosever muss die IP-Adresse von Citrix SD-WAN WANOP für diese Methode zulassen.

**Ursache:** Die Verzeichnisliste für Ordner ist auf dem Videosever nicht aktiviert.

**Auflösung:** Der Videosever muss die Verzeichnisliste für die Ordner aktivieren.

- **Problem:** Nach dem Erstellen von Einträgen für Vorgänge vor der Auffüllung können Sie keine Einträge ändern oder löschen.

**Ursache:** Möglicherweise haben Sie für den Eintrag auf **Jetzt starten** geklickt.

**Auflösung:** Dies ist von Design. Sie können einen Eintrag nicht ändern oder löschen, nachdem Sie für den Eintrag auf **Jetzt starten** geklickt haben und sich der Eintrag im Status Warteschlange, Start oder Download befindet. Sie können den Eintrag erst löschen, nachdem der Download abgeschlossen ist.



- **Problem:** Nach dem Erstellen von Einträgen für Propopulationsaufgaben wird Video nicht heruntergeladen und zwischengespeichert. Der Status des Eintrags wird nicht heruntergeladen.

**Ursache:** Der Eintrag für die Vorbevölkerung enthält keine absolute URL für das Video.

**Lösung:** Führen Sie das folgende Verfahren aus, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass der Eintrag für die Vorbevölkerung die tatsächliche URL des Videos enthält `http://10.102.29.16/Citrix SD-WAN WANOP\\_demo.mp4`, z. B. keine HTML-Datei. Die Citrix SD-WAN WANOP Appliance kann den Inhalt der HTML-Datei nicht durchsuchen, um den Videolink zu finden.
2. Stellen Sie sicher, dass das HTTP-Protokoll zum Bereitstellen des Videos verwendet wird. Sie können dies überprüfen, indem Sie die Option Quelle anzeigen des Webbrowsers verwenden.
3. Sie können die absolute URL des Videos abrufen, indem Sie die Option Entwicklertools des Webbrowsers verwenden.

## Citrix Virtual Apps and Desktops Beschleunigung

April 19, 2021

- **Problem:** Nach dem Upgrade einer Appliance auf Version 7.3.1 werden die ICA-Verbindungen nicht als Citrix Receiver für HTML5-Verbindungen auf den Seiten der ICA-Überwachung kategorisiert.

**Ursache:** Die auf der Appliance definierte Dienstklasse ist **HTTP (Privat)** anstelle von Web (Privat). Wenn Sie eine Appliance auf Version 7.3.1 aktualisieren, wird die **ALTHHTTP-Anwendung** dieser Serviceklasse nicht hinzugefügt. Obwohl ICA-Verbindungen über Citrix Receiver für HTML5 optimiert sind, werden diese auf den Seiten der ICA-Überwachung nicht als Citrix Receiver für HTML5-Verbindungen kategorisiert.

**Lösung:** Führen Sie folgende Schritte aus, um ICA-Verbindungen über Citrix Receiver für HTML5 zu kategorisieren:

1. Navigieren Sie zur Seite **Konfiguration > Optimierungsregeln > Serviceklassen**.
2. Bearbeiten Sie die **HTTP-Dienstklasse (Private)**.
3. Klicken Sie auf **Regel hinzufügen**.
4. Klicken Sie unter Filterregeln unter Anwendungen auf **Beliebig**.

5. Wählen Sie in der Liste Anwendungen die Option **ALTTTP** aus.
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Save**.
8. Nehmen Sie nach Bedarf weitere Änderungen an der Filterregel vor.
9. Klicken Sie auf **Save**.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).