

# Contents

Remote

  MultiPoint Services

    Planen einer MultiPoint Services-Bereitstellung

      Einführung in MultiPoint Services

      Erste Schritte mit MultiPoint Services

      Allgemeine Verwendungsszenarien

      MultiPoint-Stationen

      Auswählen von Hardware für Ihr MultiPoint Services-System

      Hardwareanforderungen und Empfehlungen zur Leistung

      Variablen mit Auswirkung auf die Leistung von MultiPoint Services-Systemen

      MultiPoint Services-Standortplanung

      Überlegungen zu Netzwerk und Benutzerkonten

      Speichern von Dateien mit MultiPoint Services

      Schützen des Systemvolumes mit Datenträgerschutz

      Unterstützung der Virtualisierung von MultiPoint Services

      Überlegungen zu Anwendungen

      Prüfliste vor der Bereitstellung

      Glossar

  Migrieren von MultiPoint Services

    Vorbereiten der Migration zu MultiPoint Services

    Arbeitsblatt für die Planung der Migration

    Migrieren zu MultiPoint Services

    Aufgaben nach der Migration

  Bereitstellen von MultiPoint Services

    Bereitstellen eines neuen MultiPoint Services-Systems

      Erfassen der für die Installation benötigten Hardware und Gerätetreiber

      Einrichten des physischen Computers und der primären Station

      Installieren von MultiPoint Services

      Aktualisieren und Installieren von Gerätetreibern bei Bedarf

- Festlegen des Datums, der Uhrzeit und der Zeitzone
- Hinzufügen des MultiPoint-Servers zu einer Domäne (optional)
- Updates installieren
- Anfügen weiterer Stationen an den MultiPoint-Server
  - Einrichten einer Station mit direkter Videoverbindung
  - Einrichten einer verbundenen USB-Station ohne Clients
  - Einrichten einer mittels RDP über LAN verbundenen Station
- Verwalten von Clientzugriffslizenzen mit MultiPoint Services
- Installieren von Software auf Ihrem MultiPoint Services-System
- Optionale Konfigurationsaufgaben für eine MultiPoint Services-Bereitstellung
  - Einrichten einer Station mit geteiltem Bildschirm
  - Hinzufügen von Druckern
  - Erstellen virtueller Windows 10 Enterprise-Desktops für Stationen
- Vorbereiten des MultiPoint Services-Systems für Benutzer
  - Planen von Benutzerkonten für eine MultiPoint Services-Umgebung
  - Beispielszenarien: MultiPoint Services-Benutzerkonten
  - Erstellen lokaler Benutzerkonten
  - Einschränken des Benutzerzugriffs auf den MultiPoint-Server
  - Konfigurieren von Stationen für die automatische Anmeldung
  - Zulassen mehrerer Sitzungen für ein Konto
  - Aktivieren der Dateifreigabe in MultiPoint Services
- Systemverwaltung in MultiPoint Services
  - Konfigurieren von Datenträgerschutz in MultiPoint Services
  - Installieren der Serversicherung im MultiPoint-System
  - Konfigurieren von Gruppenrichtlinien für eine Domänenbereitstellung
- Verwalten von MultiPoint Services
  - Verwalten des MultiPoint Services-Systems
  - Überlegungen zu Datenschutz und Sicherheit
- Verwalten der Stationshardware
  - Anzeigen des Hardwarestatus
  - Arbeiten mit USB-Geräten
  - Arbeiten mit Videogeräten

## Einrichten einer Station

Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers

Bearbeiten von Servereinstellungen

Neustarten oder Herunterfahren von MultiPoint-Systemen

Wechseln zwischen Modi

Aktivieren oder Deaktivieren des Datenträgerschutzes

Verwalten der Clientzugriffslizenzen

Neuzuordnen aller Stationen

Speichern der Verbindungseinstellungen in einer Datei

Hinzufügen oder Entfernen von Computern

Verwalten von Benutzerstationen

Anzeigen des Benutzerverbindungsstatus

Abmelden oder Trennen von Benutzersitzungen

Anhalten von Benutzersitzungen im aktiven Zustand

Beenden einer Benutzersitzung

Einrichten einer Station für das automatische Anmelden

Teilen einer Benutzerstation

Verwalten von Benutzerkonten

Überlegungen zu Benutzerkonten

Erstellen eines Administratorkontos

Erstellen eines Standardbenutzerkontos

Erstellen eines Kontos für MultiPoint-Dashboardbenutzer

Aktualisieren oder Löschen eines Benutzerkontos

Verwalten von virtuellen Desktops

Verwalten von Benutzerdateien

Schützen von Dateien

Freigeben von Dateien

Speichern und Freigeben von Dateien auf einem USB-Flashlaufwerk

Verwalten von Benutzerdesktops mit dem MultiPoint-Dashboard

Blockieren einer Station oder Aufheben der Blockierung einer Station

Einschränken des Webzugriffs

Blockieren oder Aufheben der Blockierung von USB-Speicher

- Projizieren einer Station auf andere Stationen
- Starten oder Schließen von Anwendungen auf einer Station
- Kommunizieren per Chat
- Übernehmen der Steuerung einer Benutzersitzung
- Anzeigeoptionen für Sitzungsminiaturansichten im MultiPoint-Dashboard
- Abmelden von Benutzersitzungen
- Verwalten von MultiPoint-Systemen mit dem MultiPoint-Dashboard
  - Neustarten oder Herunterfahren
  - Neuzuordnen ausgewählter MultiPoint-Systeme
- Remoteserver-Verwaltungstools
- Remotedesktopdienste
- Remotezugriff
  - Always On VPN
    - Always On VPN-Bereitstellung für Windows Server und Windows 10
    - Always On VPN-Features
    - Always On VPN-Verbesserungen
    - Übersicht über die Always On VPN-Technologie
    - Erweiterte Features von Always On VPN
    - Bereitstellen von Always On VPN
      - Schritt 1: Planen der Always On VPN-Bereitstellung
      - Schritt 2: Konfigurieren der Always On VPN-Serverinfrastruktur
      - Schritt 3: Konfigurieren des RAS-Servers für Always On VPN
      - Schritt 4: Installieren und Konfigurieren des NPS-Servers
      - Schritt 5: Konfigurieren von DNS und Firewalleinstellungen
      - Schritt 6: Konfigurieren von Always On VPN-Verbindungen für den Windows 10-Client
      - Schritt 7: Bedingter Zugriff für VPN-Konnektivität mit Azure AD
        - Schritt 7.1: Konfigurieren von EAP-TLS für das Ignorieren der Zertifikatssperlisten-Überprüfung
        - Schritt 7.2: Erstellen von Stammzertifikaten für die VPN-Authentifizierung mit Azure AD
        - Schritt 7.3: Konfigurieren der Richtlinie für bedingten Zugriff
        - Schritt 7.4: Bereitstellen von Stammzertifikaten für bedingten Zugriff auf der

lokalen AD-Instanz

Schritt 7.5: Erstellen von OMA-DM-basierten VPNV2-Profilen für Windows 10-Geräte

Problembehandlung bei Always On VPN

Border Gateway Protocol (BGP)

BGP-Befehlsreferenz für Windows PowerShell

RAS-Gateway

GRE-Tunneling in Windows Server

GRE-Tunneling für RAS-Gateway: Durchsatz und Leistung

RAS-Serverrolle: Dokumentation

Bereitstellen des Remotezugriffs in einem Unternehmen

Bereitstellen des Remotezugriffs in einem Cluster

Planen einer Clusterbereitstellung mit Remotezugriff

Konfigurieren eines Clusters mit Remotezugriff

Bereitstellen mehrerer RAS-Server in einer Bereitstellung mit mehreren Standorten

Planen einer Bereitstellung mit mehreren Standorten

Konfigurieren einer Bereitstellung mit mehreren Standorten

Problembehandlung bei einer Bereitstellung für mehrere Standorte

Bereitstellen des Remotezugriffs mit OTP-Authentifizierung

Planen des Remotezugriffs mit OTP-Authentifizierung

Planen des Remotezugriffs mit OTP-Authentifizierung

Problembehandlung bei einer OTP-Bereitstellung

Bereitstellen von Remotezugriff in einer Umgebung mit mehreren Gesamtstrukturen

Planen einer Bereitstellung mit mehreren Gesamtstrukturen

Konfigurieren einer Bereitstellung mit mehreren Gesamtstrukturen

Verwalten des Remotezugriffs

Verwenden der Remotezugriffsüberwachung und Ressourcenerfassung

Überwachen der vorhandenen Last auf dem Remotezugriffsserver

Überwachen des Konfigurationsverteilungsstatus des Remotezugriffsservers

Überwachen des Betriebsstatus des Remotezugriffsservers und dessen Komponenten

## Identifizieren und Beheben von Betriebsproblemen auf dem Remotezugriffsserver

Überwachen der Aktivitäten und des Status von verbundenen Remoteclients

Erstellen eines Nutzungsberichts für Remoteclients mithilfe von Verlaufsdaten

## Remoteverwaltung von DirectAccess-Clients

Planen der Bereitstellung für die Remoteverwaltung von DirectAccess-Clients

Installieren und Konfigurieren der Bereitstellung für die Remoteverwaltung von DirectAccess-Clients

## Virtual Private Networking (VPN)

VPN-Gerätetunnel unter Windows 10

Technische Anleitung für Windows 10-VPN

Gewusst wie: Konfigurieren eines Diffie-Hellman-Protokolls über IKEv2-VPN-Verbindungen

Verwenden des einmaligen Anmeldens (Single Sign-On, SSO) über VPN- und WLAN-Verbindungen

## DirectAccess

DirectAccess-Bereitstellungspfade in Windows Server

Erforderliche Komponenten für die Bereitstellung von DirectAccess

DirectAccess: Nicht unterstützte Konfigurationen

DirectAccess-Testumgebung: Leitfäden

Testumgebungsanleitung: Veranschaulichen von DirectAccess in einem Cluster mit Windows NLB

Testumgebungsanleitung: Veranschaulichen einer DirectAccess-Bereitstellung für mehrere Standorte

Testumgebungsanleitung: Veranschaulichen von DirectAccess mit OTP-Authentifizierung und RSA SecurID

DirectAccess: Bekannte Probleme

DirectAccess-Kapazitätsplanung

DirectAccess-Offline-Domänenbeitritt

Problembehandlung von DirectAccess

Bereitstellen eines DirectAccess-Servers mit dem Assistenten für erste Schritte

Planen einer allgemeinen DirectAccess-Bereitstellung

Installieren und Konfigurieren von DirectAccess (allgemein)

Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen

Planen einer erweiterten DirectAccess-Bereitstellung

Installieren und Konfigurieren des erweiterten DirectAccess

Hinzufügen von DirectAccess zu einer vorhandenen Remotezugriffsbereitstellung (VPN)

Plan zum Aktivieren von DirectAccess

Aktivieren von DirectAccess

Webanwendungsproxy in Windows Server

Veröffentlichen von Anwendungen mit AD FS-Vorauthentifizierung

Veröffentlichen von Anwendungen mit SharePoint, Exchange und RDG

Problembehandlung: Webanwendungsproxy

#### **Frage TIP**

Suchen Sie nach Informationen zu älteren Versionen von Windows Server? Sehen Sie sich unsere [Windows Server-Bibliotheken](#) auf „[docs.microsoft.com](#)“ an. Sie können auch nach bestimmten Informationen [auf dieser Website suchen](#).

## **Remotedesktopdienste**

Mit Remotedesktopdiensten können Benutzer auf Windows-basierte Programme zugreifen, die auf einem Remotedesktop-Sitzungsshostserver (RD-Sitzungsshostserver) installiert sind, oder den gesamten Windows-Desktop verwenden. Mit Remotedesktopdiensten können Benutzer aus dem Unternehmensnetzwerk oder über das Internet auf einen RD-Sitzungsshostserver zugreifen.

## **Remotezugriff**

Der Remotezugriffs-Serverrolle umfasst DirectAccess und VPN (virtuelles privates Netzwerk), LAN-Routing (virtuelles lokales Netzwerk) sowie Webanwendungsproxy. Mit RAS können Sie Netzwerkkonnektivität für Remotemitarbeiter, ein Site-to-Site-VPN zum Verbinden von Remtestandorten über das Internet sowie das RAS-Gateway bereitstellen, das über mehrinstanzfähige und BGP-Funktionen (Border Gateway Protocol) für Unternehmen und Cloud-Dienstanbieter (Cloud Service Providers, CSPs) verfügt.

## **Webanwendungsproxy**

Der Webanwendungsproxy bietet Reverseproxyfunktion für Webanwendungen in Ihrem Unternehmensnetzwerk, damit Benutzer außerhalb des Unternehmensnetzwerks von allen Geräten sicher auf die Anwendungen zugreifen können.

## **MultiPoint Services**

In diesem Blogbeitrag wird erläutert, wie Sie Microsoft-Technologien einsetzen können, um Ihre Rechenzentrums- und Cloudinvestitionen gegen neue Bedrohungen zu schützen.

## **Remoteserver-Verwaltungstools**

Zur Erleichterung der Remoteserververwaltung können Sie Remoteserver-Verwaltungstools für Windows 10 herunterladen und installieren. Remoteserver-Verwaltungstools für Windows 10 beinhalten den Server-Manager, Microsoft Management Console-Snap-Ins (MMC), Konsolen, Windows PowerShell-Cmdlets und -Anbieter sowie Befehlszeilentools für die Verwaltung von Rollen und Features, die auf Windows Server ausgeführt werden.

## **OpenSSH**

OpenSSH ist die Open-Source-Version der Secure Scripting Host (SSH) Tools, die von Administratoren von Linux- und anderen Windows-fremden Produkten für die plattformübergreifende Verwaltung von Remotesystemen verwendet wird. OpenSSH wurde Windows hinzugefügt und ist in Windows 10 und Windows Server 2019 enthalten.

# MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Multipoint Services ist eine Lösung, die es mehreren Benutzern ermöglicht, die jeweils über eine eigene, unabhängige und vertraute Windows-Benutzeroberflächen verfügen.

Benutzerstationen bestehen aus einem Monitor, einer Tastatur und einer Maus und sind direkt über USB- oder Videokabel mit dem Hostcomputer verbunden. Da es sich bei Multipoint Services um ein echtes von Microsoft veröffentlichtes Softwareprodukt handelt, sind Sie bei ordnungsgemäßer Lizenzierung berechtigt, von Microsoft oder einem autorisierten Partner Support zu erhalten. Dadurch erhalten Sie die vollständigen Funktionen von Windows, den Zugriff auf alle neuesten Updates und das Vertrauen, dass Sie die erwartete Erfahrung erzielen.

Da Multipoint Services es mehreren Benutzern ermöglicht, einen Computer gemeinsam zu nutzen, können Sie eine kostengünstige Alternative zu herkömmlichen Computing-Szenarios bereitstellen, in denen jeder Benutzer über einen eigenen Computer verfügt. Multipoint Services bietet auch eine einfache Verwaltungs Lösung für die Multipoint Services-System Administration, die als Multipoint-Manager bekannt ist, sowie eine einfache Verwaltungs Lösung-für die-Day-Verwaltung, die als Multipoint-Dashboard bezeichnet wird.

# Planen einer MultiPoint Services-Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Mithilfe von MultiPoint Services können mehrere Stationen mit einem einzigen Computer verbunden werden. Dann können mehrere Benutzer diesen Computer gleichzeitig gemeinsam verwenden. Jede Station besteht aus einem stationshub, einem Monitor, einer Tastatur und einer Maus. Multipoint Services beinhaltet die Multipoint-Manager-Anwendung, die Sie als Administrator bei der Überwachung und Verwaltung von Multipoint-Stationen unterstützt, sowie in der Multipoint-Dashboardanwendung, die alltägliche Verwaltungsfunktionen bereitstellt.

Verwenden Sie die folgenden Informationen, um die Bereitstellung zu planen:

- [Einführung in MultiPoint Services](#)
- [Allgemeine Verwendungsszenarien](#)
- [MultiPoint-Stationen](#)
- [Auswählen von Hardware für Ihr MultiPoint Services-System](#)
- [Hardwareanforderungen und Empfehlungen zur Leistung](#)
- [MultiPoint Services-Standortplanung](#)
- [Überlegungen zu Netzwerk und Benutzerkonten](#)
- [Speichern von Dateien mit MultiPoint Services](#)
- [Schützen des System Datenträgers mit Datenträger Schutz](#)
- [Unterstützung der Virtualisierung von MultiPoint Services](#)
- [Überlegungen zu Anwendungen](#)
- [Prüfliste vor der Bereitstellung](#)

Weitere Informationen finden Sie auch im [Multipoint Services-Forum](#).

# Einführung in MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Die Multipoint Services-Rolle in Windows Server 2016 ermöglicht es mehreren Benutzern, die jeweils über eine eigene unabhängige und vertraute Windows-Benutzeroberflächen verfügen, gleichzeitig einen Computer gemeinsam zu nutzen. Es gibt mehrere Möglichkeiten, wie Benutzer auf Ihre Sitzungen zugreifen können. Eine Möglichkeit besteht darin, mithilfe der [Remote Desktop-Apps](#) mit beliebigen Geräten einen Remoting in den Server zu verwenden. Eine andere Möglichkeit ist die Verwendung von physischen Stationen, die Stationen an den Multipoint-Server angefügt sind:

- Direkt an videports auf dem Computer
- Über spezialisierte USB Zero-Clients (auch als Multifunktions-USB-Hubs bezeichnet) sowie über ähnliche USB-over-Ethernet-Geräte.
- Über das LAN (Local Area Network)

Diese Methoden werden weiter unten in diesem Dokument in [Multipoint Services-Stationen](#) ausführlicher beschrieben.

In diesem Dokument werden die folgenden Faktoren behandelt, die bei der Planung der Bereitstellung von Multipoint Services zu berücksichtigen sind:

- Welche Art von Desktops für Ihr Multipoint Services-System verwendet werden soll: benötigen Sie Sitzungen, virtuelle Computer oder Windows-PCs?
- [Auswählen von Hardware für Ihr Multipoint Services-System](#): welche Hardware Entscheidungen sollten Sie treffen?
- [Hardwareanforderungen und Empfehlungen zur Leistung](#): welche Hardware ist für Multipoint Services erforderlich?
- [Planung der Multipoint Services-Site](#): wo werden die Computer, auf denen Multipoint Services und deren Stationen ausgeführt werden, und wie werden Sie konfiguriert?
- [Netzwerküberlegungen und Benutzerkonten](#): die Netzwerkumgebung, in der das Multipoint Services-System bereitgestellt wird, kann sich darauf auswirken, wie Benutzerkonten verwaltet werden. Was ist Ihre Netzwerkumgebung? Wie werden Benutzerkonten verwaltet?
- [Speichern von Dateien mit Multipoint Services](#): wo werden Benutzer Dateien gespeichert, und wie wird darauf zugegriffen?
- [Prüfliste vor der Bereitstellung](#)

# Einstieg in Multipoint Services

09.04.2020 • 9 minutes to read • [Edit Online](#)

Das Multipoint Services-System ermöglicht vielen Benutzern die Verwendung mehrerer Stationen, die physisch verbunden sind, indem Sie Station Hubs nur auf einem Computer verwenden. Jede Station besteht in der Regel aus einem stationshub, einer Maus, einer Tastatur und einem Videomonitor. Jeder Benutzer an einer Multipoint Services-Station verfügt über eine eindeutige Windows Computing-Sitzung, die Sie mithilfe von Multipoint Manager verwalten können.

Die Komponenten eines Multipoint Services-Systems umfassen Folgendes:

- Multipoint Services-Systemsoftware, die mehrere Monitore, Tastaturen, Maus Geräte und andere Geräte auf dem Computer unterstützt.
- Mit der Multipoint-Manager-Anwendung können Sie Multipoint Services-Stationen überwachen und Aktionen ausführen.
- Wartungs-und Verwaltungs Tools.
- Die Multipoint-Dashboardanwendung, mit der Sie tägliche Aufgaben ausführen können, z. b. die Kommunikation mit anderen Benutzern.

Informationen zum Verwalten von Multipoint Services-Stationen mit Multipoint Manager und Multipoint Dashboard finden Sie in dieser Hilfedatei.

## Übersicht über den Multipoint-Manager

Der Multipoint-Manager bietet vier Registerkarten, die Sie beim Verwalten der Multipoint Services-Stationen verwenden können. Jede Registerkarte und die Aufgaben, die Sie für diese ausführen können, werden in den einzelnen Hilfe Themen ausführlicher beschrieben.

Die Registerkarten lauten wie folgt:

- **Registerkarte Home:** Wechseln Sie zum Ausführen von Verwaltungsaufgaben, zum Hinzufügen oder Entfernen von Multipoint-Servern, zum Neustarten oder Herunterfahren des Computers, zum Aktivieren des Datenträger Schutzes, zum Hinzufügen von Client Zugriffs Lizenzen, zum Neuzuordnen von Stationen und zum Abrufen von Weitere Informationen finden Sie im Thema [Verwalten von System Tasks mithilfe von Multipoint-Manager](#) .
- **Registerkarte Stationen:** Anzeigen des *Desktop* Status der Benutzer und *Beenden* oder *aussetzen* von Benutzersitzungen. Weitere Informationen finden Sie im Thema [Verwalten von Benutzer Stationen](#) .
- **Registerkarte Benutzer:** *Standardbenutzer Konten* und Administrator Kontenerstellen und verwalten. Weitere Informationen finden Sie unter [Verwalten von Benutzerkonten](#).
- **Registerkarte "virtuelle Desktops":** Aktivieren von virtuellen Desktop Rollen Weitere Informationen finden Sie im Thema [Verwalten virtueller Desktops](#) .

## Multipoint-Server Verwaltung und-Wartung

Nachdem das Multipoint Services-System eingerichtet wurde, können Sie Multipoint-Manager für die Verwaltung von Multipoint Services verwenden.

Zu den Aktionen, die Sie mithilfe von Multipoint Manager ausführen können, zählen die folgenden:

- **Benutzerkonten werden hinzugefügt:** Verwenden Sie Multipoint Manager, um Standard-und Administrator Benutzerkonten zu erstellen.
- **Bearbeiten von Servereinstellungen:** Sie können Ihr Multipoint Services-System so konfigurieren, dass es im Konsolenmodus gestartet wird, dass ein Konto über mehrere Sitzungen verfügt, jeder Station eine eindeutige IP-Adresse und andere Tasks zuweisen kann.
- **Wechseln in den Konsolenmodus:** Sie können das Multipoint Services-System in den Konsolenmodus ändern, um neue Software auf Ihrem Multipoint Services-System zu installieren. Sie können angeben, dass die Software von allen Benutzern ausgeführt werden kann. Dies ist abhängig von den Installations-und Lizenzierungsoptionen der Software.
- **Problembehandlung:** Wenn Sie Probleme mit Multipoint Services haben, finden Sie [im Abschnitt zur Problembehandlung](#) weitere Themen, die Ihnen helfen können, das Problem zu beheben.

## Übersicht über das Multipoint-Dashboard

Das Multipoint-Dashboard bietet eine Multifunktionsleisten-Benutzer Karte, in der Sie zwischen zwei Registerkarten für den Zugriff auf gängige tägliche Aufgaben wählen

Die Registerkarten lauten wie folgt:

- **Registerkarte Home:** Sperren oder Entsperren von Stationen, Festlegen von webeinschränkungs Optionen, Projekt Desktops auf andere Desktops, starten oder Schließen von Anwendungen, kommunizieren über Instant Messaging, unterstützen anderer Benutzer über die Remote Desktop Steuerung, Anpassen von Desktop-Miniaturansichten und aktivieren oder Deaktivieren von Instant Messaging und automatisches Starten von Anwendungen. Weitere Informationen finden Sie im Thema [Verwalten von Benutzer Desktops mithilfe des Multipoint-Dashboards](#).
- **Registerkarte Systeme:** Neustarten, Herunterfahren oder Neuzuordnen aller oder ausgewählter Systeme. Weitere Informationen finden Sie im Thema [Verwalten von Multipoint-Systemen mithilfe des Multipoint-Dashboards](#).

## Tägliche Verwendung Ihres Multipoint Server-Systems

Wenn Sie mit der täglichen Verwendung von Multipoint Services beginnen, finden Sie Informationen zur Verwendung von Multipoint Services, die Sie möglicherweise für die Benutzer in Ihrem Multipoint Services-System freigeben möchten. Diese Informationen umfassen Folgendes:

### Freigeben von Inhalten und Aufbewahrung von Inhalten:

- Ein Benutzer kann eine Datei oder ein Dokument in einem privaten Ordner speichern, der nur von diesem Benutzer angezeigt werden kann.
- Benutzer können auch Dokumente in einem öffentlichen Ordner speichern, auf den alle Benutzer im Multipoint Services-System zugreifen können.
- Es ist wichtig, dass Multipoint Services-Benutzer wissen, dass Administratoren Zugriff auf alle Dateien und Dokumente im System haben, auch wenn Sie privat im persönlichen Ordner eines Benutzers gespeichert sind.

Weitere Informationen zum Speichern und Verwalten von privaten und öffentlichen Inhalten finden Sie im Thema [Verwalten von Benutzer Dateien](#).

### Informationen zur Multipoint Services-Sitzung eines Benutzers:

- Jeder Benutzer verfügt über einen Benutzernamen und ein Kennwort sowie eine eindeutige Desktop *Sitzung* auf dem Multipoint Services-System.

- Ein *Standardbenutzer ist kein Administrator* des Multipoint Services-Systems. Standard Benutzer können einige Arten von Software nicht installieren, aber Sie können Dateien speichern und Desktop Einstellungen ändern, mit Ausnahme der Bildschirmauflösung. Alle vom Benutzer am Desktop vorgenommenen Änderungen sind bei der nächsten Anmeldung weiterhin vorhanden.
- Benutzer können die Verbindung mit einer Station trennen und sich wieder bei ihrer Sitzung auf einer anderen Station anmelden, ohne Ihre Arbeit zu verlieren. Weitere Informationen finden Sie im Thema [Anhalten von Benutzersitzungen im aktiven Zustand](#).
- Die Sitzung eines Standard Benutzers (oder alle Benutzersitzungen) kann vom Administrator über den Multipoint-Manager getrennt oder abgemeldet werden. Weitere Informationen finden Sie im Thema [Verwalten von Benutzer Desktops](#).
- Wenn ein Benutzer ein Kennwort vergisst, können Sie das Kennwort von der Registerkarte " **Benutzer** " zurücksetzen, die Standardfunktionen für die Windows-Benutzerkonten Verwaltung verwendet. Weitere Informationen finden Sie im Thema [aktualisieren oder Löschen eines Benutzerkontos](#) .

## Weitere Informationen

[Verwalten des Multipoint-Server Systems](#)

[Wichtige Informationen zur Software Lizenz Konformität](#)

[Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)

[Verwalten von Benutzerdateien](#)

[Verwalten von Benutzer Desktops](#)

[Aussetzen und Benutzersitzung aktiv lassen](#)

[Anzeigen des Benutzerverbindungsstatus](#)

[Verwalten der Stationshardware](#)

[Einrichten einer Station](#)

[Verwalten von Benutzerkonten](#)

[Aktualisieren oder Löschen eines Benutzerkontos](#)

[Verwalten von Benutzerdesktops mit dem MultiPoint-Dashboard](#)

[Verwalten von MultiPoint-Systemen mit dem MultiPoint-Dashboard](#)

[Problembehandlung](#)

# Allgemeine Verwendungsszenarien

09.04.2020 • 2 minutes to read • [Edit Online](#)

Multipoint Services bietet den einzelnen Benutzer Desktops die wichtigsten Elemente des Windows 10-Desktop Erlebnisses. Außerdem wird ein einfaches Verwaltungs Tool (Multipoint-Manager) angeboten, das Systemadministratoren für die Ermittlung und Steuerung mehrerer Multipoint-Server und-Clients verwenden können. Darüber hinaus umfasst Multipoint Services das Multipoint-Dashboard für die Echt Zeit Sichtbarkeit. Beispiele für die Möglichkeiten von Multipoint Services sind folgende:

- Bieten Sie jedem Benutzer ein persönliches Computing und private Ordner, ohne für jede Person einen separaten Computer zu benötigen.
- Verwalten mehrerer Multipoint-Systeme in einem Computerlabor, Classroom, Schulungs Center oder einer kleinen Geschäftsumgebung.
- Installieren Sie ein Programm einmal, und greifen Sie von einer beliebigen Station aus darauf zu.
- Überwachen Sie die Desktop Aktivität der einzelnen Benutzer.
- Blockieren Sie Bildschirme mit einer anpassbaren Meldung, um die Aufmerksamkeit der Gruppe zu erhalten.
- Beschränken Sie die Gruppe auf eine oder mehrere Websites.
- Projizieren Sie den Bildschirm auf die anderen Bildschirme, um eine bestimmte Aufgabe zu veranschaulichen.
- Kommunizieren Sie privat mit einem Standardbenutzer, der Hilfe bittet.
- Übernehmen Sie die Kontrolle über die Sitzung eines Benutzers, um eine Aufgabe zu veranschaulichen.
- Führen Sie alle oben aufgeführten Elemente für einen Benutzer aus, der einen herkömmlichen PC, Laptop oder andere mobile Geräte verwendet.

# Multipoint-Stationen

09.04.2020 • 13 minutes to read • [Edit Online](#)

In einer Multipoint Services-Systemumgebung sind *Stationen* die Benutzer Endpunkte zum Herstellen einer Verbindung mit dem Computer, auf dem Multipoint Services ausgeführt wird. Jede Station bietet dem Benutzer eine unabhängige Windows 10-Benutzeroberflächen. Die folgenden Stations Typen werden unterstützt:

- Direkt mit Videos verbundene Stationen
- Über USB-Verbindungen mit 0 (null) Clients verbundene Stationen (einschließlich USB-over-Ethernet-Clients)
- RDP-über-LAN-verbundene Stationen (für Rich Client- oder Thin Client-Computer)

Vollständige PCs, auf denen der Multipoint-Connector installiert ist, können auch über das Multipoint-Dashboard überwacht und gesteuert werden. Unter Windows 10 kann der Multipoint-Connector über die Systemsteuerung für Windows-Features aktiviert werden.

Multipoint Services unterstützt eine beliebige Kombination dieser Stations Typen. Es wird jedoch empfohlen, dass eine Station eine Station mit direkt Videoverbindung ist, die als primäre Station fungieren kann. Der Grund für diese Empfehlung ist, dass Sie Support Szenarien erwarten können. Beispielsweise für die Interaktion mit dem BIOS des Systems, bevor Multipoint Services ausgeführt wird.

## Primäre Stationen und Standard Stationen

Eine Station mit direkt-Video-Verbindung ist als *primäre Station* definiert. Die verbleibenden Stationen werden als *Standard Stationen* bezeichnet.

Die primäre Station zeigt die Startbildschirme an, wenn der Computer eingeschaltet ist. Er bietet Zugriff auf Systemkonfigurations- und Problem Behandlungsinformationen, die nur während des Starts verfügbar sind. Bei der primären Station muss es sich um eine Station mit direkt Videoverbindung handeln. Nach dem Start können Sie die primäre Station wie alle anderen Multipoint-Stationen verwenden.

## Direkt mit Videos verbundene Stationen

Der Computer, auf dem Multipoint Services ausgeführt wird, kann mehrere Videokarten enthalten, von denen jeder über einen oder mehrere videports verfügen kann. Dadurch können Sie Monitore für mehrere Stationen direkt in den Computer einbinden. Tastaturen und Mäuse sind über USB-Hubs verbunden, die mit jedem Monitor verknüpft sind. Diese Hubs werden als *Stations Hubs* bezeichnet. Andere Peripheriegeräte, wie z. B. Sprecher, Kopfhörer oder USB-Speichergeräte, können auch mit einem stationshub verbunden werden und sind nur für den Benutzer dieser Station verfügbar.

### IMPORTANT

Es sollte mindestens eine Station mit *direkt-Video-Verbindung* pro Server vorhanden sein, die als primäre Station fungiert, um den Startprozess anzuzeigen, wenn der Computer eingeschaltet ist.

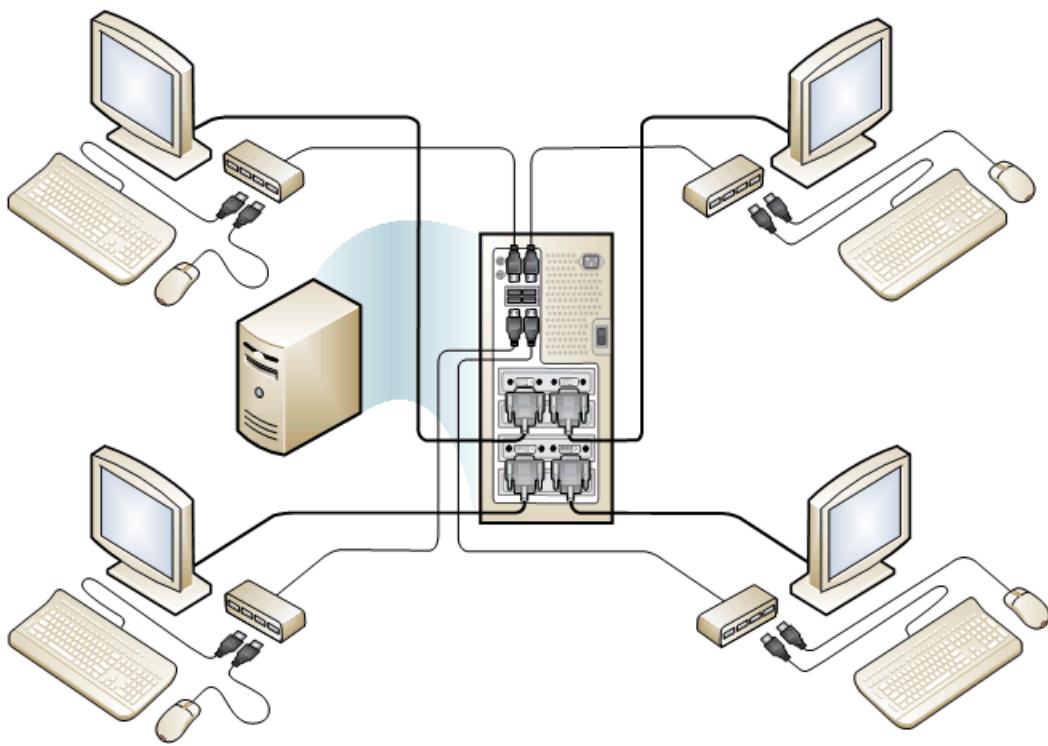


Abbildung 1 Multipoint Services-System mit vier direkt mit einem Video verbundenen Stationen

#### PS/2-Stationen

Mit Multipoint Services können Sie die PS/2-Tastatur und die Maus auf dem Motherboard einem direkt Video verbundenen Monitor zuordnen, um eine PS/2-Station zu erstellen. Eine hochauflösende, analoge Audiodatei auf der Hauptplatine ist das Audiomaterial, das mit dieser Art von Station verknüpft ist. Dies gilt nicht für Computer, bei denen keine PS/2-Jacks auf der Hauptplatine vorhanden sind.

#### An einem USB-Client angeschlossene Stationen

An einem USB-Client verbundene Stationen verwenden einen *USB Zero-Client* als stationshub. USB-Clients werden manchmal auch als multifunktionshub mit Video bezeichnet. Dabei handelt es sich um einen Hub, der über ein USB-Kabel mit dem Computer verbunden ist, und diese Hubs unterstützen in der Regel einen Videomonitor, eine Maus und Tastatur (PS/2 oder USB), Audiodaten und zusätzliche USB-Geräte. Dieses Handbuch bezieht sich auf diese spezialisierten Hubs als USB-Clients.

Das folgende Diagramm zeigt ein Multipoint-Server System mit einer primären Station (Direct Video Connected Station) und zwei zusätzlichen, mit dem USB-Client verbundenen Stationen.

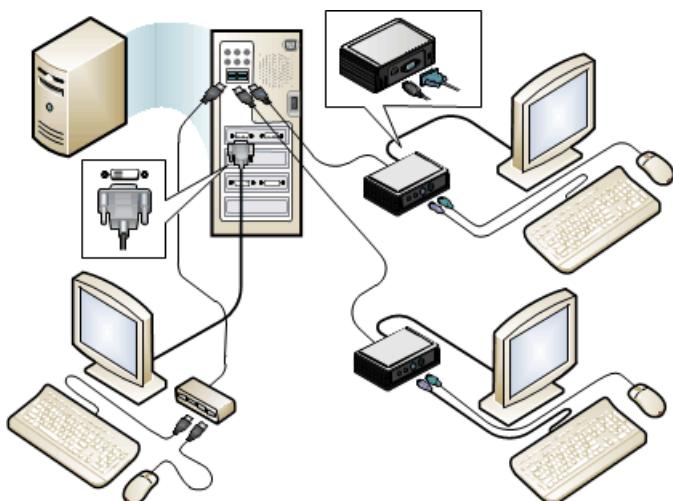


Abbildung 2 Multipoint Services-System mit einer primären Station und zwei an einem USB-Client verbundenen Stationen

### **USB-over-Ethernet-Clients (null)**

USB-over-Ethernet-Clients stellen eine Variation von USB-Clients dar, die USB-über-LAN an das Multipoint Services-System senden. Diese Typen von USB-Clients funktionieren ähnlich wie andere USB-Clients, sind aber nicht durch maximale Länge der USB-Kabellänge beschränkt. Bei USB-over-Ethernet-Clients handelt es sich nicht um herkömmliche Thin Clients, und Sie werden als virtuelle USB-Geräte im Multipoint Services-System angezeigt. Wenn Sie diese Geräte verwenden, finden Sie unter Gerätshersteller spezifische Empfehlungen zur Leistung und Website Planung. Die meisten Geräte verfügen über ein Drittanbieter-Plug-in für Multipoint Manager, mit dem Sie Geräte dem Multipoint Services-System zuordnen und verbinden können.

## **Verbundene RDP-over-LAN-Stationen**

Thin Clients und herkömmliche Desktop-, Laptop- oder Tablet Computer können eine Verbindung mit dem Computer herstellen, auf dem Multipoint Services über das lokale Netzwerk (Local Area Network, LAN) ausgeführt wird, indem Remotedesktopprotokoll (RDP) oder ein proprietäres Protokoll und der Remotedesktopprotokoll Anbieter verwendet werden. RDP-Verbindungen bieten eine Endbenutzer Umgebung, die mit jeder anderen Multipoint-Station vergleichbar ist, aber die Hardware des lokalen Client Computers verwendet. Erfahren Sie mehr über unsere Remote Desktop-Anwendungen, die in [Remotedesktop-Clients für Android, Ios, Mac und Windows](#) verfügbar sind.

Clients und Geräte, auf denen Microsoft RemoteFX ausgeführt wird, können eine umfangreiche Multimediaumgebung bereitstellen, indem Sie die Prozessor- und Video Hardwarefunktionen des lokalen Thin Client oder des lokalen Computers nutzen, um Videos mit hoher Definition über das Netzwerk bereitzustellen.

Wenn Sie über vorhandene LAN-Clients verfügen, können Sie mit Multipoint Services eine schnelle und kostengünstige Möglichkeit bereitstellen, um alle Benutzer gleichzeitig auf Windows 10 zu aktualisieren.

Aus Bereitstellungs- und Verwaltungs Sicht bestehen die folgenden Unterschiede bei der Verwendung von mit RDP-über-LAN verbundenen Stationen:

- Nicht beschränkt auf physische USB-Verbindungs Abstände
- Möglichkeit zur Wiederverwendung älterer Computer Hardware als Stationen
- Die Skalierung auf eine größere Anzahl von Stationen ist einfacher. Alle Clients in Ihrem Netzwerk können möglicherweise als Remote Station verwendet werden.
- Keine Hardwareproblem Behandlung über die Multipoint Manager-Konsole
- Keine Split-Screen-Funktionalität.

Weitere Informationen finden Sie unter [Split-Screen-Stationen](#) weiter unten in diesem Thema.

- Keine Stations umbenennen oder Konfigurieren der automatischen Anmeldung über die Multipoint Manager-Konsole

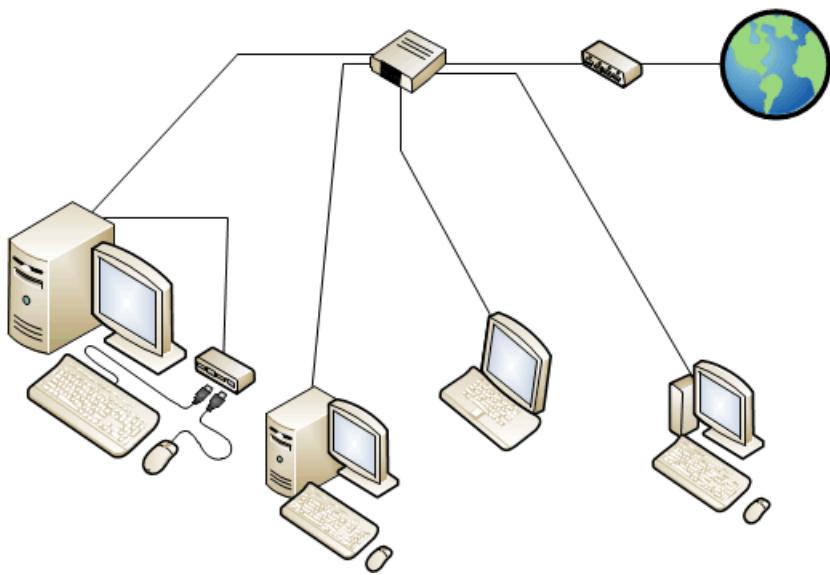


Abbildung 3 Multipoint Services-System mit per RDP über LAN verbundenen Stationen

## Zusätzliche Konfigurationsoptionen

### Stationen mit geteiltem Bildschirm

Multipoint Services bietet eine Split Screen-Option auf Computern mit direkt mit einem Video verbundenen Stationen oder an an einem USB-Client verbundenen Stationen. Ein geteilter Bildschirm bietet die Möglichkeit, eine zusätzliche Station pro Monitor zu erstellen. Anstatt zwei Monitore zu erfordern, können Sie einen Monitor mit zwei stationshub-Setups verwenden, um zwei Stationen mit einem Monitor zu erstellen. Sie können die Anzahl der verfügbaren Stationen schnell erhöhen, ohne zusätzliche Monitore, USB-Null-Clients oder Grafikkarten erwerben zu müssen.

Die Verwendung einer Split-Screen-Station bietet folgende Vorteile:

- Verringern von Kosten und Speicherplatz, indem mehr Benutzer in einem Multipoint Services-System untergebracht werden.
- Ermöglicht zwei Benutzern das parallele zusammenarbeiten mit einem Projekt.
- Ermöglicht es einem Lehrer, eine Prozedur auf einer Station zu veranschaulichen, während ein Student auf der anderen Station zusammenhält.

Jeder Multipoint Services-Stations Monitor mit einer Auflösung von mindestens 1024 x 768 kann in zwei Stations Bildschirme aufgeteilt werden. Für eine optimale Benutzer Darstellung auf dem Bildschirm wird ein breit Bildschirm mit einer Mindestauflösung von 1600 x 900 empfohlen. Es wird auch eine Mini Tastatur ohne einen Zahlenbereich empfohlen, damit die beiden Tastaturen in den Monitor eingefügt werden können.

Zum Erstellen von Split-Screen-Stationen richten Sie eine Station mit direktem bzw. einem USB-oder-Client-Verbindung ein. Dann fügen Sie einen zusätzlichen stationshub hinzu, indem Sie eine Tastatur und eine Maus an einen USB-Hub anschließen, der mit dem Server verbunden ist. Anschließend können Sie die Station in zwei Stationen konvertieren, indem Sie den Bildschirm mithilfe von Multipoint-Manager aufteilen und den neuen Hub der Hälfte des Monitors zuordnen. Die linke Hälfte des Bildschirms wird zu einer Station, und die Rechte Hälfte wird zu einer zweiten Station.

Nachdem eine Station aufgeteilt wurde, kann sich ein Benutzer an der linken Station anmelden, während sich ein anderer Benutzer an der rechten Station anmeldet.

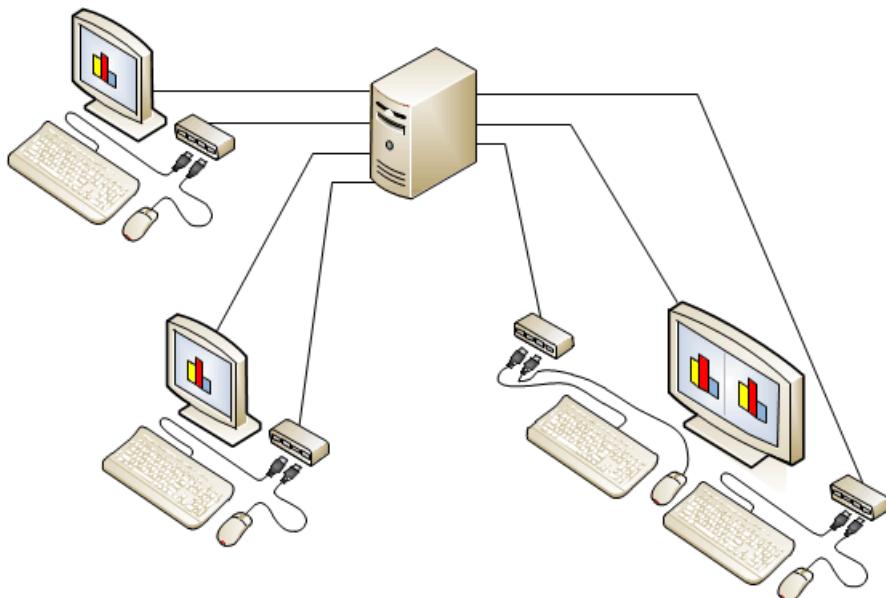


Abbildung 4 Multipoint Services-System mit unterteilten Bildschirm Stationen

## Stations Typvergleich

	DIREKTES VIDEO MIT VERBINDUNG	USB-NUL-CLIENT VERBUNDEN	RDP-OVER-LAN-VERBINDUNG
Videoleistung	Empfohlen für eine optimale Video Leistung		Verwenden von Thin Clients, die remotefx unterstützen, um die Videoqualität bei geringerer Netzwerkbandbreite zu steigern
Physische Einschränkungen	Begrenzt durch Grafik Kabellänge und USB-Hub und Kabellänge (empfohlene maximale Länge von 15 Metern)	Begrenzt durch USB-Hub und Kabellänge (empfohlene maximale Länge von 15 Metern)	Verteilung durch LAN-Verteilung
Zulässige Anzahl von Stationen	Begrenzt durch die Anzahl der verfügbaren PCIe-Slots auf den Hauptseiten der Videoanschlüsse Pro Grafikkarte	Die Gesamtanzahl kann durch den USB-Client Hersteller eingeschränkt werden. (Weitere Informationen finden Sie im Hinweis, der dieser Tabelle folgt.)	Begrenzt durch verfügbare Ports auf dem Netzwerk Switch
Geteilter Bildschirm	Ja	Ja	Nein
Peripherie Status der Multipoint Manager-Station, Konfiguration der automatischen Anmeldung, Stations umbenennen	Ja	Ja	Nein
Zugriff auf Serverstart Menüs	Ja	Nein	Nein

**NOTE**

Die Gesamtanzahl der USB-Clients, die mit dem Server verbunden sind, wird möglicherweise durch den Hersteller oder die Hardware Funktion des Computers beschränkt, auf dem Multipoint Services ausgeführt wird.

# Auswählen von Hardware für Ihr MultiPoint Services-System

09.04.2020 • 24 minutes to read • [Edit Online](#)

Wenn Sie ein Multipoint Services-System erstellen, sollten Sie einen Computer auswählen, der die Systemanforderungen für Windows Server 2016 erfüllt. Wenn Sie entscheiden, welche Komponenten ausgewählt werden sollen, berücksichtigen Sie Folgendes:

- Der Ziel Preisbereich ihrer gesamten Lösung.
- Die Typen von Verwendungs Szenarios, die Sie möglicherweise für das Multipoint Services-System erwarten, z. b. ob die Benutzer Multimedia-Programme ausführen und Textverarbeitungs-oder Produktivitäts Programme ausführen oder das Internet durchsuchen.
- Gibt an, ob Ihr Szenario große Verarbeitungs-oder Arbeitsspeicher Anforderungen hat.
- Die Anzahl der Benutzer, die das System gleichzeitig verwenden können. Wenn Sie planen, gleichzeitig viele Benutzer in Ihrem System zu verwenden, oder Benutzer, die System intensive Programme verwenden, sollten Sie für Ihr System mehr Rechenleistung planen.
- Der Typ der Stationen. Wie viele USB-Ports oder videports benötigen Sie?
- Zukünftige Erweiterungspläne. Planen Sie, dem Multipoint Services-System zu einem späteren Zeitpunkt Stationen hinzuzufügen? Verfügen Sie über genügend Videokarten Slots, USB-Anschlüsse oder Netzwerkads? Wie viele zusätzliche Benutzer müssen von Ihrer Hardware unterstützt werden?
- Physisches Layout. Weitere Informationen finden Sie unter [Planung von Multipoint Services-Websites](#).

Ein Multipoint Services-System umfasst in der Regel die folgenden Komponenten:

- Ein Computer, auf dem Multipoint Services ausgeführt wird, der CPU, RAM, Festplattenlaufwerke und Grafikkarten umfasst.
- Einen Monitor, einen stationshub, eine Tastatur und eine Maus für jede Station.
- Optionale Peripheriegeräte für die Multipoint Services-Stationen, einschließlich Referenten, Kopfhörer, Mikrofon oder Speichergeräte, die nur für den Benutzer der Station verfügbar sind.
- Optionale Peripheriegeräte, die für alle Benutzer des Multipoint Services-Systems verfügbar sind, die direkt mit dem Host Computer verbunden sind, z. b. Drucker, externe Festplattenlaufwerke und USB-Speichergeräte.

Verwenden Sie die folgenden Informationen, um Hardware Entscheidungen zu treffen:

- [Auswählen einer CPU](#)
- [Auswählen von Hardwarekomponenten](#)

## Auswählen einer CPU

Bei einem Multipoint Services-System handelt es sich um eine Umgebung mit mehreren-Benutzern, bei der alle Benutzer mit einem einzelnen Host Computer verbunden sind. Dadurch erhöht sich die CPU-Auslastung, da alle Benutzer denselben Computer gemeinsam verwenden. Einige Aufgaben, z. b. Multimedia-Programme (z. b. Medien Player oder Video-Bearbeiten von Software), haben größere Verarbeitungsanforderungen. Stellen Sie daher sicher, dass Sie eine CPU auswählen, mit der die Verarbeitungsanforderungen für die Anzahl der Benutzer und Typen von

Benutzer Szenarien, die unterstützt werden müssen, erfüllt werden können.

Multipoint Services erfordert eine x64--basierte CPU und muss die Systemanforderungen für den Computer erfüllen, wie unter [Hardware Anforderungen und Empfehlungen zur Leistung](#) beschrieben.

Die folgenden Prozessortypen wurden getestet, um in einem Multipoint Services-System mit hoch-Verarbeitungs Programmen wie Multimedia-Programmen verwendet zu werden:

- **Dual-Kern Prozessor:** Kann bis zu acht Stationen unterstützen.
- **Quad-Core-Prozessor:** Unterstützt bis zu 16 Stationen.
- **Quad-Core-Prozessor mit Multithreading:** Unterstützt bis zu 20 Stationen.
- **Sechs-Core-Prozessor mit Multithreading:** Von können bis zu 24 Stationen unterstützt werden.

Wählen Sie mit diesen Informationen eine CPU aus, die den Verarbeitungsanforderungen Ihres Multipoint Services-Systems entspricht.

**NOTE**

Wenn Sie Video intensive Anwendungen ausführen, wird empfohlen, mindestens einen Kern pro Station zu haben.

## Auswählen von Hardwarekomponenten

Beachten Sie bei der Erstellung eines Multipoint Services-Systems die folgenden Hardwarekomponenten, die Sie möglicherweise benötigen:

- Video Hardware
- Hardware der Multipoint Services-Station
  - *USB-Hubs*
  - USB-Clients
  - Tastatur und Maus Geräte
  - Monitor
- Peripheriegeräte
  - Audiogeräte, z. b. Sprecher und Kopfhörer
  - Mikrofone
  - USB-Massenspeicher Geräte

Wenn Sie die Hardwarekomponenten für das Multipoint Services-System ausgewählt haben, stellen Sie sicher, dass Sie die aktuellen 64--Bit-Treiber für die-Komponenten erhalten.

Die folgenden Themen enthalten ausführliche Informationen, die Ihnen bei der Auswahl von Komponenten für Ihr Multipoint Services-System helfen:

[Auswählen der Video Hardware](#)

[Auswählen von direkt-Video-verbundenen oder USB-Client Station-Geräten](#)

[Auswählen anderer Stations Peripheriegeräte](#)

[Auswählen von RDP--über-LAN-Connected Station-Hardware](#)

[Auswählen von Audiogeräten](#)

## Auswählen der Video Hardware

Die von Ihnen ausgewählte Video Hardware sollte die Anzahl der Monitore unterstützen, die Sie für die Anzahl der Benutzer benötigen, die an Multipoint Services-Stationen arbeiten möchten. Darüber hinaus können unterschiedliche Arten von Video Hardware eine höhere-Leistungs Lösung für Grafik-intensiven Programme, z. b. Multimedia-Inhalte, bereitstellen.

Wählen Sie die Video Hardware aus, die die maximale Anzahl von Monitoren für die Art der von Ihrem Multipoint Services-System benötigten Leistung unterstützen kann. Stellen Sie sicher, dass Sie die Leistung der Video Hardware, die Sie ausgewählt haben, überprüfen, um sicherzustellen, dass Sie Ihren Leistungsanforderungen entspricht.

#### **NOTE**

Sie müssen einen Videotreiber installieren, der die Erweiterung des Desktops auf mehrere Monitore unterstützt.

Die Video Hardware Optionen umfassen Folgendes:

- Interne Grafikkarten, die eine PCI- oder PCIe-Busschnittstelle verwenden
- Externe Videocontroller, die über USB verbunden sind

In den folgenden Abschnitten werden die Funktionen der einzelnen Video Hardwaretypen beschrieben. Sie können interne Grafikkarten und externe Videocontroller kombinieren, um das gewünschte System zu erstellen.

#### **Interne Grafikkarten**

Eine interne Grafikkarte wird an die Hauptplatine des Computers angeschlossen-. Die interne Grafikkarte ist eine Lösung, die die Leistung von Grafiken-intensiven Multimedia-Programmen unterstützen kann. Eine interne Grafikkarte erfordert jedoch einen verfügbaren PCI- oder PCIe-Slot, um in die Hauptplatine zu integrieren. Viele High--Leistungs Grafikkarten erfordern einen PCIe-Slot, aber es gibt eine begrenzte Anzahl von PCIe-Slots auf einem Motherboard. Sie sollten wissen, welche Art von Grafikkarten Slots auf Ihrem Computer verfügbar sind, damit Sie den richtigen Typ von Grafikkarten erwerben können.

Die Anzahl der Monitore, die eine Verbindung mit den einzelnen Grafikkarten herstellen können, hängt von der GPU, die auf der Karte verwendet wird, und der Anzahl der unterstützten Ports ab, die in der Regel zwischen 2 und 6 liegen.

Wenn Sie interne Grafikkarten auswählen, wählen Sie Grafikkarten aus, die die Anzahl der Monitore unterstützen, die zum Erstellen der gewünschten Anzahl an direkt mit dem Video verbundenen Stationen erforderlich sind. Die maximale Anzahl von Monitoren, die unterstützt werden können, entspricht der Anzahl der internen Grafikkarten, die an die Hauptplatine angeschlossen werden-, multipliziert mit der Anzahl der Überwachungsparts auf den einzelnen Grafikkarten. Wenn Sie z. b. über zwei interne Grafikkarten verfügen und jede Karte über zwei Überwachungsparts verfügt, können Sie bis zu vier Monitore unterstützen.

#### **Externe Videocontroller**

USB-Clients enthalten einen externen Videocontroller, um eine Verbindung zwischen einem Monitor und dem Client herzustellen. Der USB Zero-Client kann auch Verbindungen für Kopfhörer, Referenten, ein Mikrofon oder andere Peripheriegeräte enthalten.

Wählen Sie einen USB-Client aus, wenn Sie die Unterstützung für zusätzliche Monitore aktivieren möchten, ohne den Computer zu öffnen, oder wenn Sie mehr Stationen als verfügbare Video Ausgaben unterstützen möchten. Wenn Sie z. b. zuvor vier Monitore an interne Grafikkarten-angeschlossen haben und zwei weitere Monitore hinzufügen möchten, können Sie in zwei externen Video Controllern an den Computer anschließen und Platz für zwei weitere Monitore haben. Auf diese Weise können Sie einen USB-Zero-Client mit dem Videocontroller kombinieren und keine zusätzlichen PCI- oder PCIe-Slots auf der Hauptplatine verwenden.

## **Auswählen von direkt-Video-verbundenen oder USB-Client Station-**

# Geräten

Eine Multipoint Services-Station besteht aus einem stationshub oder einem USB-Null-Client mit einer Tastatur-und Maus-in und einem Monitor, der mit dem Host Computer verbunden-ist, oder in einem USB-Null-Client. Andere Peripheriegeräte können-an den stationshub oder den USB-Client angeschlossen werden, sind jedoch nicht erforderlich, um eine Multipoint-Station zu erstellen. Diese anderen Peripheriegeräte werden unter [Auswählen anderer Station-Peripheriegeräte](#)beschrieben.

Die Geräte, die Sie zum Erstellen einer Multipoint Services-Station auswählen, müssen die Mindestanforderungen erfüllen, um mit Multipoint Services arbeiten zu können. Ausführliche Informationen zu den Anforderungen für die folgenden Multipoint Services-Stations Geräte finden Sie in diesem Thema:

- [Auswählen von USB-Hubs](#)
- [Auswählen von USB-Clients](#)
- [Auswählen von Tastaturen und Maus Geräten](#)
- [Auswählen von Monitoren](#)

## Auswählen von USB-Hubs

Die in einem Multipoint Services-System verwendeten USB-Hubs können ein generischer USB-Hub sein. Solche Hubs verfügen in der Regel über vier oder mehr USB-Anschlüsse, sodass mehrere USB-Geräte mit einem einzelnen USB-Anschluss auf dem Computer verbunden werden können. Einige andere Geräte, wie z. b. Tastaturen und Videomonitore, können auch einen USB-Hub in Ihren Entwurf integrieren.

Ein weiterer Aspekt ist die Verwendung eines *extern betriebenen* Hubs anstelle eines *Bus---gestützten* Hubs. Bei einem Bus--Hub muss die Menge der aktuellen, die vom Host Computer bereitgestellt wird, ausreichen, damit alle Peripheriegeräte, die mit dem Hub verbunden sind, an den Hub-angeschlossen werden, ohne dass die Systemleistung beeinträchtigt wird. Ein extern gestützter Hub ermöglicht es Ihnen, mehr Peripheriegeräte zu verbinden und ausreichend Leistung für alle bereitzustellen. Die Verwendung extern gestützter Hubs kann dabei helfen, Leistungsprobleme, Port Ausfälle und andere vorübergehende Probleme zu vermeiden.

Wenn Sie einen USB-Hub für Ihr Multipoint Services-System auswählen, sollten Sie dessen Verwendung in Erwägung gezogen. Der Hub kann als *stationshub*, als *Zwischenhub*oder als *downstreamhub downstream hub*verwendet werden. In der folgenden Tabelle finden Sie Beschreibungen zu den einzelnen Hub-Typen. Wir empfehlen, dass alle USB-Geräte USB-2,0 oder höher sind.

	FAHRZEUGE
Stationshub	Kann Bus-untergebracht werden, es sei denn, hochgeschaltete Geräte werden-darin angeschlossen, oder es wird ein downstreamhub verbunden.
Zwischenhub	Sollte extern eingeschaltet werden
Downstream-Hub	Kann abhängig von den Geräten, die mit dem Hub verbunden-sind, extern oder per Busbetrieb betrieben werden.
Aktives USB-Extender-Kabel	Aktive USB-Kabel, die einen USB-Hub enthalten, werden in der Regel durch busgestützte Daher empfiehlt es sich nicht, Station Hubs mit dem Computer zu verbinden.

## Auswählen von USB-Clients

Ein USB-Null-Client ist ein USB-Hub, der eine Videoausgabe enthält. Daher kann ein Monitor über eine USB-Verbindung mit dem Computer verbunden werden. Weitere Informationen zur Verwendung von USB-Clients für Videos finden Sie unter [Auswählen von Video Hardware](#) in diesem Dokument. Ein USB-Null-Client kann auch die Verbindung einer Vielzahl von USB-und nicht--USB-Geräten mit dem Hub ermöglichen. USB-Clients werden von

bestimmten Hardwareherstellern erstellt und erfordern die Installation eines Geräts-bestimmten Treibers.

## Auswählen von Tastaturen und Maus Geräten

Die Tastatur-und Maus Geräte, die Sie an die Station-anschließen, sind in der Regel USB-Geräte. Einige USB-Null-Clients stellen PS/2 Ports bereit. in diesem Fall sollten die Tastatur und die Maus PS/2 verwenden, um eine Verbindung mit dem stationshub herzustellen. Sie können auch eine PS/2-Tastatur und-Maus verwenden, wenn Sie eine "PS/2 Direct-Video-Connected Station einrichten.

Eine Tastatur mit einem internen Hub kann als stationshub verwendet werden. Allerdings müssen alle anderen Stations Geräte mithilfe von Ports auf der Tastatur eine Verbindung mit dem internen Hub herstellen. Wenn eine solche Tastatur über einen anderen Hub mit dem Computer verbunden ist, wird dieser Hub als Zwischenhub behandelt.

Wenn Sie die Bildschirm Stationen Split-verwenden, empfiehlt es sich, eine Mini Tastatur zu verwenden, die nicht über einen Zahlenbereich verfügt, sodass die beiden Tastaturen in den Monitor eingefügt werden können.

## Auswählen von Monitoren

Für jede Multipoint Services-Station sollte ein Monitor bereitgestellt werden, es sei denn, ein Split--Bildschirm ist geplant. Monitore werden mit der Grafikkarte auf dem Computer, dem USB-Null-Client oder dem LAN--basierten Client verbunden. Alle Monitor Typen, die von der Grafikkarte, dem USB Zero-Client oder dem LAN--basierten Client unterstützt werden, können verwendet werden, einschließlich CRT-Monitoren.

Einige besondere Monitore umfassen einen internen LAN--basierten Client oder einen USB-Client. Diese Monitore enthalten in der Regel Audioeingaben/Ausgabe-und internen USB-Hubs zum Verbinden von Tastaturen und Mäusen. Sie stellen eine Verbindung mit dem Server über eine USB-oder LAN-Verbindung her.

### Anzeigeauflösung

Die unterstützte Mindestauflösung für den Anzegebereich einer Station beträgt 512 x 768 Pixel. Wenn das Multipoint Services-System gestartet wird und feststellt, dass der Anzegebereich einer Station kleiner als die minimale Auflösung ist, wird ein leerer Bildschirm auf dieser Station angezeigt, und die Station kann nicht verwendet werden.

Wenn ein Anzeige Monitor von zwei Stationen als geteilte-Bildschirm Stationen gemeinsam genutzt wird, ist die Mindestanforderung für die Anzeige 1024 x 768, sodass die resultierenden einzelnen Stations Bildschirmbereiche mindestens 512 x 768 sind. Für eine optimale Aufteilung-Bildschirm Benutzer wird empfohlen, dass ein breiter Bildschirm mit einer minimalen Auflösung von 1600 x 900 empfohlen wird.

## Auswählen anderer Stations Peripheriegeräte

Multipoint Services unterstützt Peripheriegeräte, die mit einem stationshub, einem USB-Null-Client oder direkt mit dem Computer verbunden sind. Geräte, die an einen stationshub angeschlossen sind, werden dieser bestimmten Station zugeordnet. Andere Geräte sind für jede Station verfügbar, wenn Sie direkt an den Computer angeschlossen sind. LAN-Clients können auch Peripheriegeräte unterstützen.

### IMPORTANT

Eine Tastatur kann nicht mit einem downstreamhub verbunden werden (z. b. ein Hub, der an einen stationshub angeschlossen ist). Wenn Sie eine Tastatur an einen Downstream-Hub anschließen, sind alle Peripheriegeräte, die an den downstreamhub-angeschlossen sind, für diese Station nicht mehr verfügbar. Dieses Verhalten ermöglicht die Unterstützung von Daisy-verketteten Stations Hubs.

**Für alle Stationen verfügbar** Ein USB-Gerät, das mit dem Computer verbunden ist (z. b. nicht über einen stationshub) ist für alle Stationen verfügbar. Abhängig vom Gerät kann es von mehreren Benutzern gleichzeitig verwendet werden, oder es kann jeweils nur ein Benutzer darauf zugreifen. In der folgenden Tabelle wird erläutert, wie auf USB-Geräte zugegriffen werden kann.

#### **NOTE**

Die Spalte "verbunden mit Host Computer" in der Tabelle bezieht sich auf das Verhalten, wenn der Computer, auf dem Multipoint Services ausgeführt wird, im Stations Modus mit Stationen ausgeführt wird. Wenn Sie im Konsolenmodus ausgeführt werden, Verhalten sich die Peripheriegeräte, die an einem beliebigen Ort angeschlossen sind, genauso wie ein Standard Server in einer Konsolen Sitzung.

	VERBUNDEN MIT HOST COMPUTER	VERBUNDEN MIT STATIONSHUB ODER DOWNSTREAMHUB
Tastatur	Nicht funktionsfähig, es sei denn, Sie ist Teil einer PS/2-Station.	Für einzelne Station verfügbar Es kann keine Verbindung mit einem Downstream-Hub hergestellt werden.
Maus	Nicht funktionsfähig, es sei denn, Sie ist Teil einer PS/2-Station.	Für einzelne Station verfügbar
Redner/Kopfhörer	Nicht funktionsfähig, es sei denn, Sie ist Teil einer PS/2-Station.	Für einzelne Station verfügbar
USB-Speichergerät	Für alle Stationen verfügbar	Für einzelne Station verfügbar
HID-Consumersteuerelement	Nicht funktionsfähig	Für einzelne Station verfügbar
Andere USB-Geräte, z. b. Kameras, Dokument Leser und DVD-Laufwerke	Verfügbar für alle Stationen, sofern von Windows Server 2012 unterstützt	Verfügbar für alle Stationen, wenn dies von Windows Server 2008 R2 unterstützt wird Remotedesktopdienste

## Auswählen von RDP--über-LAN-Connected Station-Hardware

Jeder LAN-Client, der mithilfe von Remotedesktopprotokoll eine Verbindung mit Remotedesktopdienste herstellen kann, kann zu einer Multipoint Services-Station werden.

Wenn Sie möchten, dass der LAN-Client nur als Multipoint-Station verwendet werden kann, können Sie Ihren LAN-Client "Sperren". Konfigurieren Sie z. b. ihren Thin Client so, dass er nur eine Verbindung mit einer Multipoint Services-Sitzung herstellen kann, oder konfigurieren Sie die Desktop Computer so, dass der Zugriff auf Desktop Symbole und Start Menü Elemente (z. b. ein Webbrower) entfernt wird, um direkten Internet Zugriff zu verhindern. Sie können diese Konfigurationen mit ihren LAN-Client Konfigurationstools oder-Gruppen oder lokalen Richtlinien vornehmen.

## Auswählen von Audiogeräten

Es ist wichtig sicherzustellen, dass Sie bei der Auswahl von Audiogeräten mit dem stationshub, dem USB-Client oder dem LAN-Client verbunden werden können. Einige USB-Hubs, USB-Clients und LAN-Clients verfügen über einen analogen AudioJack, der mit herkömmlichen, analogen Audiogeräten verwendet werden kann (z. b. Kopfhörer oder Earbuds). Bei Station Hubs, die keine analogen Geräte enthalten, können USB-Audiogeräte verwendet werden.

Wenn Sie ein PS-/2--Video-Connected Station mithilfe von PS/2-Ports auf der Hauptplatine des Computers für Tastatur und Maus konfiguriert haben, müssen Sie die analoge Audiodatei auf der Hauptplatine des Computers verwenden, damit das Audiogerät für diese Station verfügbar ist, wenn das Multipoint Services-System im Stations Modus ausgeführt wird.

Wenn Sie nicht über eine "PS/2 Direct--Video-verbundene Station verfügen, ist das hostaudiogerät auf dem System-Motherboard nur verfügbar, wenn das Multipoint Services-System im Konsolenmodus ausgeführt wird.

# Hardwareanforderungen und Empfehlungen zur Leistung

09.04.2020 • 6 minutes to read • [Edit Online](#)

In diesem Thema wird die Hardware beschrieben, die zum Ausführen eines Multipoint Services-Systems und zum unterstützen von Anwendungsszenarien für Benutzer erforderlich ist. Das Benutzer Szenario wirkt sich direkt auf die CPU-, RAM-und Netzwerk Bandbreitenanforderungen aus.

## Optimieren der Multipoint Services-Systemleistung

Die Leistung des Multipoint Services-Systems wird direkt von der Kapazität der CPU, der GPU und der RAM-Kapazität, die auf dem Computer verfügbar ist, auf dem Multipoint Services ausgeführt wird, beeinträchtigt.

### Anwendungen und Internet Inhalte

Da Multipoint Services eine Lösung für die gemeinsame Nutzung von Ressourcen ist, können sich der Typ und die Anzahl der Anwendungen, die auf den Stationen ausgeführt werden, auf die Leistung Ihres Multipoint Services-Systems auswirken. Es ist wichtig, die Typen von Programmen zu beachten, die bei der Planung Ihres Systems regelmäßig verwendet werden. Beispielsweise erfordert eine grafikintensive Anwendung einen leistungsfähigeren Computer als eine Anwendung, z. B. ein Textverarbeitungs Tool. Das über Laden des Computers mit Grafikintensiven Anwendungen führt wahrscheinlich zu Verzögerungen beim gesamten System.

Der Inhaltstyp, auf den Anwendungen zugreifen, wirkt sich auch auf die Leistung des Systems aus. Wenn mehrere Stationen Webbrowser für den Zugriff auf Multimedia-Inhalte verwenden, wie z. B. vollbewegungs-Video, können vor der Beeinträchtigung der Systemleistung weniger Stationen verbunden werden. Wenn dagegen mehrere Stationen Webbrowser verwenden, um auf statische Webinhalte zuzugreifen, können mehr Stationen ohne erhebliche Auswirkung auf die Leistung verbunden werden.

### Hardware-Empfehlungen

Verwenden Sie die Richtlinien in der folgenden Tabelle, wenn Sie Ihr System planen und testen, um eine gute Leistung mit Ihrem Multipoint Services-System zu erzielen. Dies sind die grundlegenden Anforderungen für die Multipoint-Dienste. Die tatsächliche Konfigurations Größe hängt von Ihrer Systemkonfiguration, der Arbeitsauslastung, die Sie ausführen, und der Hardware Funktion ab. Sie sollten stets validieren, indem Sie Ihre Anwendungen und Hardware testen.

#### NOTE

2C = 2 Kerne, 4C = 4 Kerne, 6C = 6 Kerne, MT = Multithreading. Die Prozessorgeschwindigkeit muss mindestens 2,0 Gigahertz (GHz) betragen.

### Empfohlene Hardware für die Ausführung von Standard-Multipoint-Server Stationen

Anwendungsszenario	Bis zu 5 Stationen	6-8-Stationen	9-12-Stationen	13-16-Stationen	17-20-Stationen	21-24-Stationen
Fak Office, Webbrows er, Branchen Anwendungen	CPU: 2C RAM: 2 GB	CPU: 2C RAM: 4 GB	CPU: 4C RAM: 6 GB	CPU: 4C RAM: 8 GB	CPU: 4C + MT oder 6C RAM: 10 GB	CPU: 6C + MT RAM: 12 GB
Mischen Office, Webbrows er, Branchen Anwendungen und gelegentlich von einigen Benutzern verwendet e Video Verwendung	CPU: 2C RAM: 2 GB	CPU: 2C RAM: 4 GB	CPU: 4C RAM: 6 GB	CPU: 4C + MT oder 6C RAM: 8 GB	CPU: 6C + MT RAM: 10 GB	CPU: 6C + MT RAM: 12 GB
Video intensiv Office, Webbrows er, Branchen Anwendungen und häufig von allen Benutzern verwende nde Videos : Videotests wurden mit dem Video "360p H. 264" bei der systemeigenen Auflösung ausgeführ t.	CPU: 4C + MT RAM: 2 GB	CPU: 6C + MT RAM: 4 GB	CPU: 8C + MT RAM: 6 GB	CPU: 12C + MT RAM: 8 GB	CPU: 16C + MT RAM: 10 GB  -Thin Client: remotefx -USB- Video nicht empfehlen swert	CPU: 20C + MT RAM: 12 GB  -Thin Client: remotefx -USB- Video nicht empfehlen swert

## Empfohlene Hardware für die Ausführung vollständiger virtueller Windows 10-Desktops

Das Ausführen einer vollständigen virtuellen Betriebssystem Instanz für jede Station ist Rechen intensiver als die Ausführung der standardmäßigen Multipoint Desktop-Sitzungen, sodass die Host Hardwareanforderungen pro

Station höher sind:

1. CPU: 1 Kern oder Thread pro Station
2. Solid State Drive (SSD)
  - a. Kapazitäts > = 20 GB pro Station + 40 GB für das WMS-Host Betriebssystem
  - b. Zufälliger Lese-/Schreib-IOPS-> = 3K pro Station
3. RAM-> = 2 GB pro Station + 2 GB für das WMS-Host Betriebssystem

Die BIOS-CPU-Einstellung wurde zum Aktivieren der Virtualisierung konfiguriert – Second Level Address Translation (slat)

Wenden Sie sich an Ihren Hardwarehersteller, um weitere Informationen zur Auswahl der optimalen Multipoint Services-Hardware für Ihre Anforderungen zu erhalten.

# Variablen mit Auswirkung auf die Leistung von MultiPoint Services-Systemen

09.04.2020 • 4 minutes to read • [Edit Online](#)

Viele Variablen können sich auf die Gesamtleistung Ihres Multipoint Services-Systems auswirken. Sie sollten diese beim Entwerfen Ihres Systems in Erwägung gezogen werden.

## Verwendung

- **Anwendungen** Der Typ und die Anzahl der Anwendungen, die gleichzeitig ausgeführt werden, insbesondere Grafiken-starker oder Speicher intensiver Anwendungen, wirken sich auf die Gesamtleistung des Systems aus. Weitere Informationen finden Sie unter [Anwendungen und Internet Inhalte](#).
- **Internet Nutzung** Stellen Sie sich vor, wenn Ihre Benutzer Multimedia-Inhalte oder Webseiten anzeigen, die Videos mit vollständiger Bewegung verwenden. Dieser Inhaltstyp kann das System überladen, wenn zu viele Benutzer gleichzeitig anzeigen.

### NOTE

Das Projektions Feature in Multipoint Services, das es Lehrkräften ermöglicht, ihre Bildschirme auf ihren Studenten Monitoren zu projizieren, ist nicht für das Projizieren von voll bewegungsvideos konzipiert. Die Projektions Funktion ist für Demonstrationszwecke konzipiert, wie z. b. die Darstellung einer Prozedur.

- **Hoch Geschwindigkeits Geräte** Wenn zu viele Benutzer gleichzeitig ein hoch Geschwindigkeits Gerät wie eine Webcam oder einen DVD-Player verwenden, wirkt sich dies auf die Gesamtleistung des Systems aus.

## Konfiguration

- **CPU, GPU und RAM** Weitere Informationen zu den Empfehlungen für CPU, GPU und RAM finden Sie unter [Optimieren der Multipoint Services-System Leistung](#) in diesem Handbuch.
- **Netzwerkbandbreite** Bei verbundenen RDP-over-LAN-Stationen sind die Netzwerkbandbreite und die Funktionsfähigkeit des Clients (z. b. ein Thin Client, ein Desktop-PC oder ein Laptop) wichtig, insbesondere dann, wenn das Video in der Sitzung des Benutzers ausgeführt wird. Wenn Sie USB-over-Ethernet-Clients verwenden, sollte auch die Netzwerkbandbreite berücksichtigt werden. Video Daten für alle Geräte werden über die gleiche Ethernet-Verbindung gesendet. Sie sollten daher bei der Verwendung dieser Geräte ein separates Gigabit-Ethernet-Netzwerk einrichten.
- **Remotefx** Bei verbundenen RDP-over-LAN-Stationen können Sie remotefx verwenden, um die Bereitstellung von Multimedia-Inhalten mit hoher Definition erheblich zu verbessern.
- **Bildschirmauflösung** Wenn Sie eine hohe voll Bild Grafik verwenden, sollten Sie die Auflösung des Monitors verringern, um die Leistung zu maximieren.
- **Anzahl der USB-Clients** Die Gesamtanzahl der USB-Clients auf einem einzelnen Stammhub auf dem Server wirkt sich direkt auf die Leistung des Videos aus. Weitere Informationen finden Sie unter [Layout für mit USB-Clients verbundene Stationen](#). Die Anzahl der unterstützten USB-over-Ethernet-Client Stationen kann geringfügig niedriger sein als die Anzahl der USB-Clients.
- **USB-Bandbreite** Beachten Sie beim Entwerfen des Systems die USB-Bandbreite. Dies ist insbesondere bei USB-Clients wichtig, von denen Videodaten über die USB-Verbindung gesendet werden. Um die Bandbreite

zu optimieren, minimieren Sie die Anzahl der Geräte, die mit einem einzelnen USB-Anschluss auf dem Server verbunden sind. Dies gilt für nicht verkettete Stationen und zwischen Hubs. Weitere Informationen finden Sie unter [Stations Hubs](#) und [zwischen Hubs](#).

- **USB-Typ** Die Verwendung von USB 3,0 anstelle von USB 2,0 erhöht die verfügbare Bandbreite zwischen dem Server und dem Zwischenhub, wenn Sie mehr als drei USB-Clients mit dem Hub verbinden oder wenn Sie USB-Geräte mit hoher Bandbreite verwenden.
- **Stationen** Die Gesamtanzahl der Stationen wirkt sich auf die Leistung aus. Wenn Sie über hohe Grafik-, Verarbeitungs-oder Video Anforderungen verfügen, empfiehlt es sich, die Gesamtanzahl der Stationen einzuschränken. Weitere Informationen finden Sie unter [Optimieren der Multipoint Services-System Leistung](#).

# MultiPoint Services-Standortplanung

09.04.2020 • 15 minutes to read • [Edit Online](#)

Berücksichtigen Sie den Speicherort, an dem ein oder mehrere Computer, auf denen Multipoint Services ausgeführt wird, und die zugehörigen Stationen bereitgestellt werden.

Der Computer, auf dem die Multipoint Services-Rolle ausgeführt wird, sollte bequemen Zugang zu einer Stromversorgung und zu den Peripheriegeräten haben, die direkt mit dem Computer verbunden sind, z. B. ein Drucker. Außerdem muss der Computer, auf dem Multipoint Services ausgeführt wird, über einen bequemen Zugriff auf eine Netzwerkverbindung verfügen. Für den Zugriff auf das Internet und ggf. ein LAN ist eine Netzwerkverbindung erforderlich.

Weitere zu berücksichtigende Faktoren sind:

- Wird das Multipoint Services-System in einem bestimmten Raum eingerichtet, oder wird es in einem Rollback oder einer Tabelle eingerichtet, sodass es von Ort zu Ort verschoben werden kann?

## NOTE

Wenn Sie die Verwendung einer mobilen Installation planen, können Sie die Stationen bei jedem erneuten Verbinden der Stationen mit Multipoint Services *Verknüpfen*, um sicherzustellen, dass jede Tastatur und Maus mit dem entsprechenden Monitor verknüpft ist.

- Befindet sich die primäre Station neben den anderen Stationen oder ist sie getrennt? Wenn z. B. das Multipoint Services-System in einem Classroom eingerichtet ist, befindet sich die primäre Station im Lehrpersonal und die Standard Stationen an einer anderen Stelle im Raum? Wenn der Computer, auf dem Multipoint Services ausgeführt wird, neu gestartet wird, kann die primäre Station auf die Startbildschirme zugreifen. Wenn Sie diese Zugriffsebene in einer Classroom-Einstellung in Betracht ziehen, empfiehlt es sich, die primäre Station am Schreibtisch der Lehrkräfte zu platzieren.
- Wie viele Stationen werden in den Raum passen?
- Benötigen Sie ein Netzwerk? Bei einer einzelnen Serverlösung, bei der direkte Video Verbindungen oder Verbindungen mit USB-Clients verwendet werden, ist kein Netzwerk erforderlich.
- Gibt es ausreichend Netzwerkverbindungen im Raum, um die erforderliche Anzahl von Computern zu unterstützen, auf denen Multipoint Services ausgeführt wird
- Wo befinden sich die Energie Outlets?
- Benötigen Sie ein zusätzliches Anzeigegerät, z. B. einen Projektor? Wenn Sie beabsichtigen, einen Projektor zu verwenden, wird er von der Obergrenze abhängen, oder er wird in einer Tabelle positioniert?
- Welche Art von Kabeln wird benötigt, und wie viele werden benötigt?
- Stellen Sie sich vor, wie Sie in Zukunft erweitern können. Werden Sie weitere Stationen hinzufügen?

## Stations Layout und-Konfiguration

Das physische Layout Ihrer Website kann sich auf die Auswahl des Stations Typs auswirken. Weitere Informationen zu den verschiedenen Stations Typen finden Sie in diesem Handbuch unter [Multipoint-Stationen](#). Mehrere Stations Typen sind in einem einzelnen Multipoint-Dienst zulässig. Dies bietet Ihnen zusätzliche Flexibilität, um Ihre Installationsanforderungen zu erfüllen.

## **Layout für direkt mit Videos verbundene Stationen**

- Bei einer Station mit direkt-Video-Verbindung wird der Abstand zwischen den Monitoren und dem Computer durch die Videokabel Länge beschränkt.
- Die Verwendung von zwischen Hubs oder mit der Verwendung von Daisy verketteten Stations Hubs wird zur Erleichterung der Bereitstellung unterstützt, aber die empfohlene Höchstzahl von aufeinander folgenden Hubs ist drei. Dies bedeutet, dass der maximale Abstand zwischen dem Computer und dem stationshub 15 Meter beträgt, da jedes USB 2,0-Kabel über die maximale Länge von fünf Metern verfügt.

### **IMPORTANT**

Es sollte immer mindestens eine direkte Videoverbindung pro Computer vorhanden sein, um als primäre Station fungieren zu können.

## **Layout für USB-Verbindungen mit Client verbundenen Stationen**

- Die Verwendung von zwischen Hubs oder mit der Verwendung von Daisy verketteten Stations Hubs wird zur Erleichterung der Bereitstellung unterstützt, aber die empfohlene Höchstzahl von aufeinander folgenden Hubs ist drei. Dies bedeutet, dass der maximale Abstand zwischen dem Computer und dem stationshub 15 Meter beträgt, da jedes USB 2,0-Kabel über die maximale Länge von fünf Metern verfügt.
- Die maximal empfohlene Anzahl von USB-Clients, die mit einem einzelnen Zwischenhub verbunden sind, ist drei.

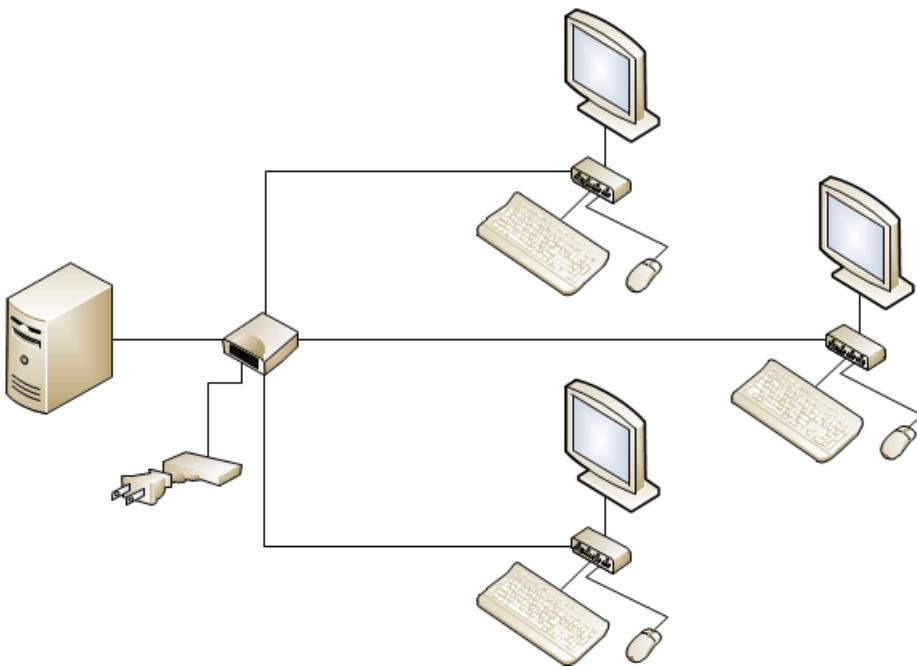
### **NOTE**

Einige Computer verfügen über einen generischen Hub auf der Hauptplatine. Dies hat Auswirkungen auf das Hinzufügen eines zusätzlichen Hubs zwischen dem *stamphub* des Computers und den Stations Hubs.

- Wenn Videos stark verwendet werden, empfiehlt es sich, höchstens zwei USB-Clients mit einem USB-Anschluss auf dem Server zu verbinden. Wenn z. b. ein Zwischenhub verwendet wird, müssen nur zwei USB-Clients verbunden werden. Wenn Sie keine USB-Clients verkettet, sollten nur zwei USB-Clients verkettet werden. Durch das Hinzufügen eines USB-Null-Clients zum USB-Anschluss auf dem Server wird die verfügbare Videobandbreite verringert.
- Wenn Sie beabsichtigen, mehr als drei USB-Clients mit einem einzelnen USB-Anschluss auf dem Server zu verbinden, wird die Verwendung von USB 3,0 zwischen dem Server und dem Zwischenhub empfohlen.

### **NOTE**

Es wird empfohlen, die Leistung mithilfe Ihrer Anwendungen und Hardware zu überprüfen, um zu entscheiden, wie viele USB-Clients Sie mit einem USB-Anschluss auf dem Server verbinden können.



**Abbildung 5** Multipoint Services-System mit drei USB-Clients, die mit einem einzelnen Zwischenhub verbunden sind

#### Layout für verbundene RDP-over-LAN-Stationen

Es gibt keine Einschränkungen hinsichtlich der physischen Entfernung für LAN-Clients. Solange Sie sich im LAN befinden, können Sie eine Verbindung mit dem Multipoint Services-System herstellen.

## Verwenden zusätzlicher Hubs

Zusätzliche Hubs können verwendet werden, um die Installation zu vereinfachen. Es gibt drei Arten von Hubs, die in einem Multipoint Services-System verwendet werden:

- [Stations Hubs](#)
- [Zwischen Hubs](#)
- [Downstream-Hubs](#)

#### Stations Hubs

Ein stationshub ist ein externer Hub, der einer Multipoint Services-Station zugeordnet ist. Der stationshub muss mindestens über eine Tastatur eingebunden werden. Es können auch zusätzliche Peripheriegeräte angefügt werden. Ein stationshub kann ein generischer USB-Hub sein, der der Spezifikation USB 2,0 oder höher entspricht. Stations Hubs sollten extern eingeschaltet werden, wenn hoch betriebene Geräte ein Plug-in für Sie durchführt.

**Stammhub** Ein USB-Hub, der auf dem Host Controller auf der Hauptplatine eines Computers integriert ist, wird als *Stammhub* bezeichnet. Stations Hubs sind in der Regel an den Stammhub auf dem Computer angeschlossen, auf dem Multipoint Services ausgeführt wird.

#### NOTE

Stamm-Hubs sollten nicht als Stations Hubs verwendet werden. Wenn USB-Ports auf einem Computer integriert sind, ist es oft nicht möglich, zu ermitteln, mit welchem USB-Stammhub eine interne Verbindung besteht. Wenn Sie also eine Station-Tastatur und die Maus direkt an die USB-Anschlüsse des Computers angeschlossen haben, können Sie die Tastatur und die Maus an verschiedene USB-Stamm Hubs anpacken. Um sicherzustellen, dass sich die Tastatur und die Maus auf demselben Hub befinden, können Sie einen stationshub in den USB-Anschluss des Computers einbinden und dann die Tastatur und die Maus an den stationshub anschließen.

**Daisy-Verkettung-Stationen** Es ist möglicherweise einfacher, Station Hubs mit einem anderen stationshub zu verbinden, als nicht direkt mit dem Computer. Dies ermöglicht es Ihnen, einen USB-Hub mit einem stationshub zu verbinden, der bereits an den Computer angeschlossen ist, sodass Sie über einen stationshub verfügen, der an einen anderen stationshub angeschlossen ist.

Es dürfen nicht mehr als drei USB-Clients oder stationshub, die in der Zwischenzeit mit einem Punkt verkettet sind. Es muss darauf geachtet werden, dass die USB-Bandbreite nicht überschritten wird, wenn die Station-Hubs für die

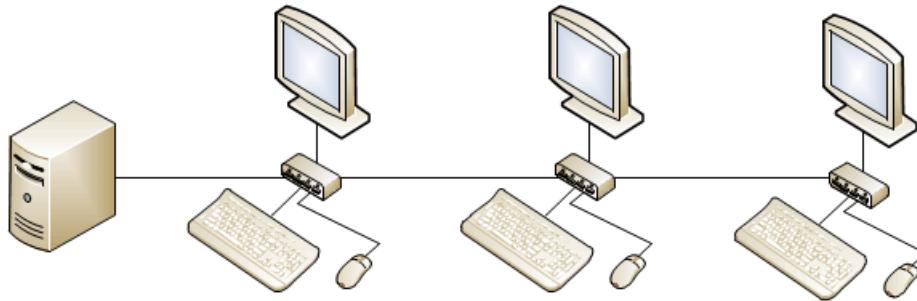


Abbildung 6 Multipoint Services-System mit an sich verketteten Stationen

### Zwischen Hubs

Ein Zwischenhub ist ein Hub zwischen dem Server und einem stationshub. Sie wird in der Regel verwendet, um die Anzahl der Ports zu erhöhen, die für Station Hubs verfügbar sind, oder um die Entfernung der Stationen vom Computer zu verlängern. Es wird empfohlen, zwischen einem stationshub und dem Server höchstens zwei Zwischen Hubs zu verwenden.

Zwischen Hubs müssen USB 2,0 oder höher sein, und Sie müssen extern eingeschaltet werden. USB 3,0 wird zwischen dem Server und dem Zwischenhub empfohlen, wenn Sie mehr als drei USB-Clients mit einem Zwischenhub verbinden.

### Downstreamhubs

Ein downstreamhub ist mit einem stationshub verbunden, um weitere verfügbare Ports für Stations Geräte hinzuzufügen. Abhängig von den Geräten, die mit dem Hub verbunden sind, kann ein downstreamhub extern oder durch Busbetrieb betrieben werden.

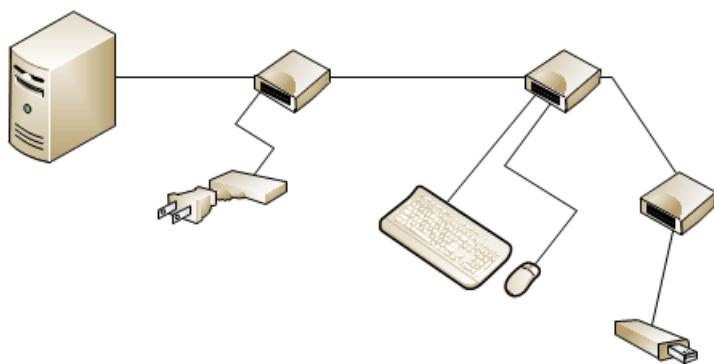


Abbildung 7 Multipoint Services-System mit einem Zwischenhub, einem stationshub und einem Downstream-Hub

## Benutzer, Stationen und Computer

Die Anzahl der benötigten Stationen hängt von der Anzahl der Benutzer ab, die gleichzeitig auf die Computer zugreifen müssen, auf denen Multipoint Services ausgeführt wird. Ebenso hängt die Anzahl der Computer, auf denen Multipoint Services ausgeführt wird, von der Gesamtanzahl der erforderlichen Stationen ab. An Direct-Video-Connected-Stationen, auf USB-Clients angeschlossene Stationen und an RDP-over-LAN-Verbindungen werden als Stationen angesehen. Wenn außerdem die Split-Screen-Funktionalität verwendet wird, wird jede

Hälften als Station betrachtet.

## Überlegungen zur Leistung

Die folgenden Komponenten erfordern Zugriff auf einen Strom oder eine Steckdose:

- Server
- Monitor
- Zwischen Hubs (bei Verwendung)
- Einige USB-Clients
- USB-Geräte, wie z. b. externe Speichergeräte und DVD-Laufwerke

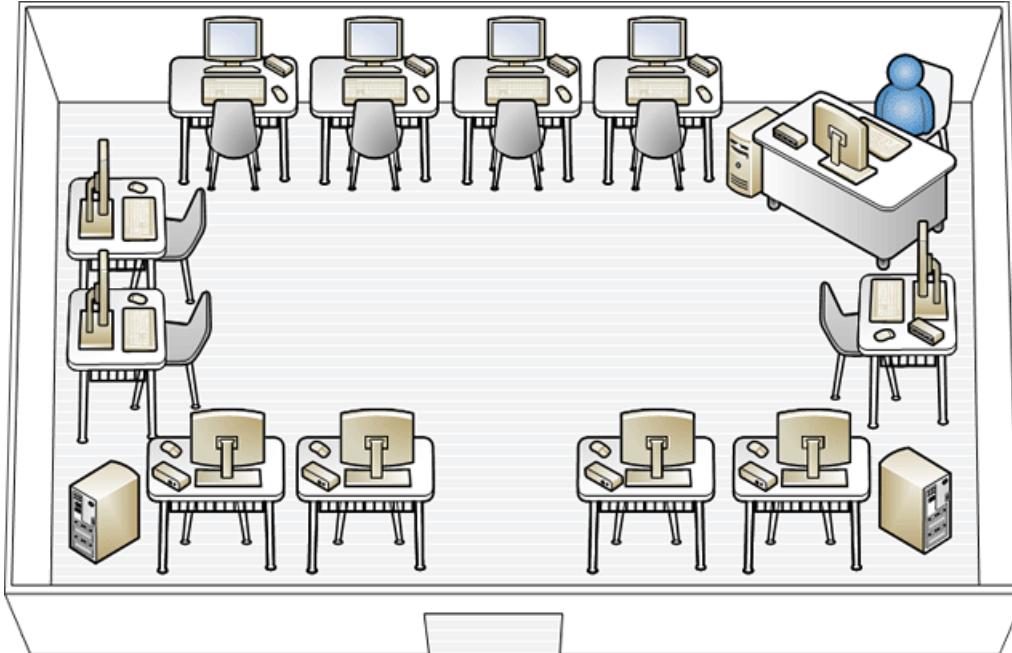
## Beispiel für Multipoint Services-systemlayouts

Abhängig von den verfügbaren Möbeln, der Größe des Raums, der Anzahl der Computer, auf denen Multipoint Services ausgeführt wird, und den Stationen im Raum gibt es eine Vielzahl von Möglichkeiten, wie die physischen Stationen angeordnet werden können. In den folgenden Diagrammen werden fünf mögliche Alternativen veranschaulicht.

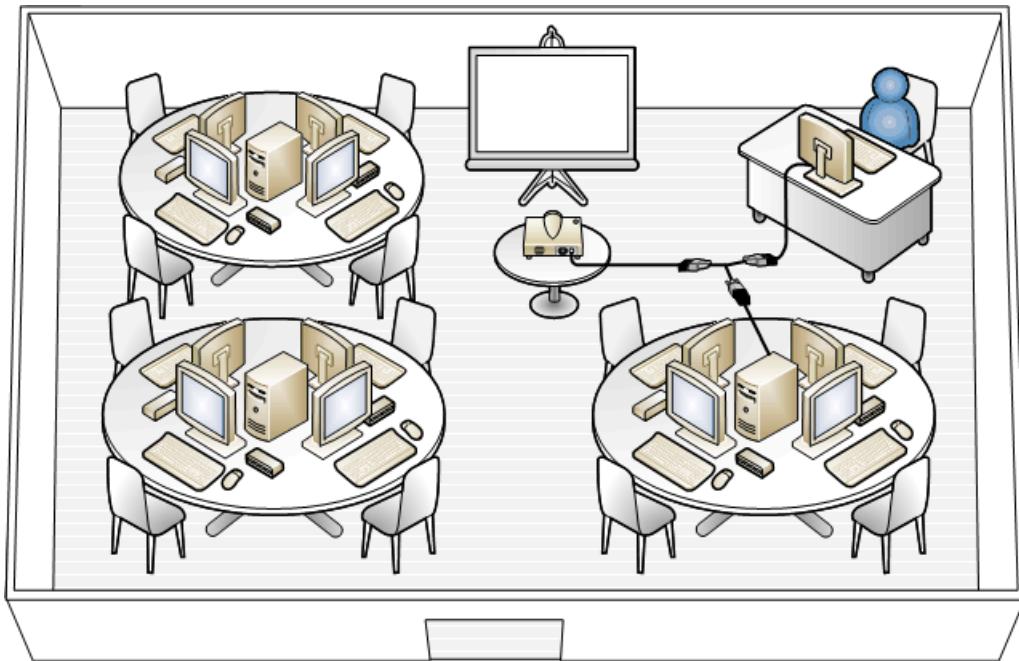
### NOTE

Einige dieser Diagramme zeigen einen Projektor, der mit dem Multipoint Services-System verbunden ist. Dies ist nur ein Beispiel: das Einschließen eines Projektors in ein Multipoint Services-System ist optional.

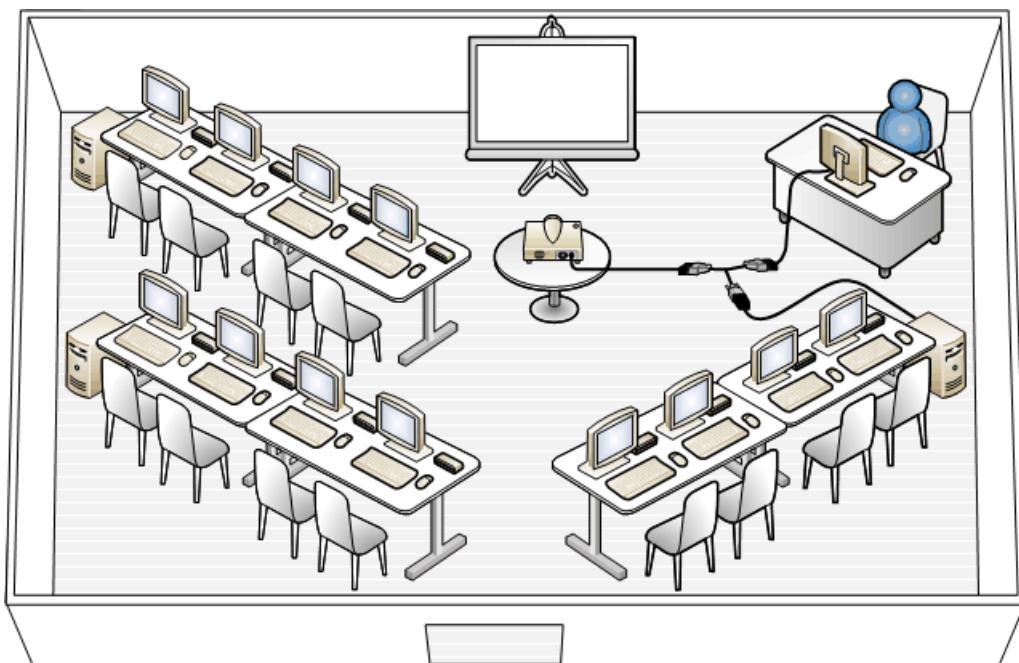
**Computer Labor** In diesem Setup werden die Stationen um die Wände des Raums angeordnet, wobei die Schüler/Studenten die Wände sehen.



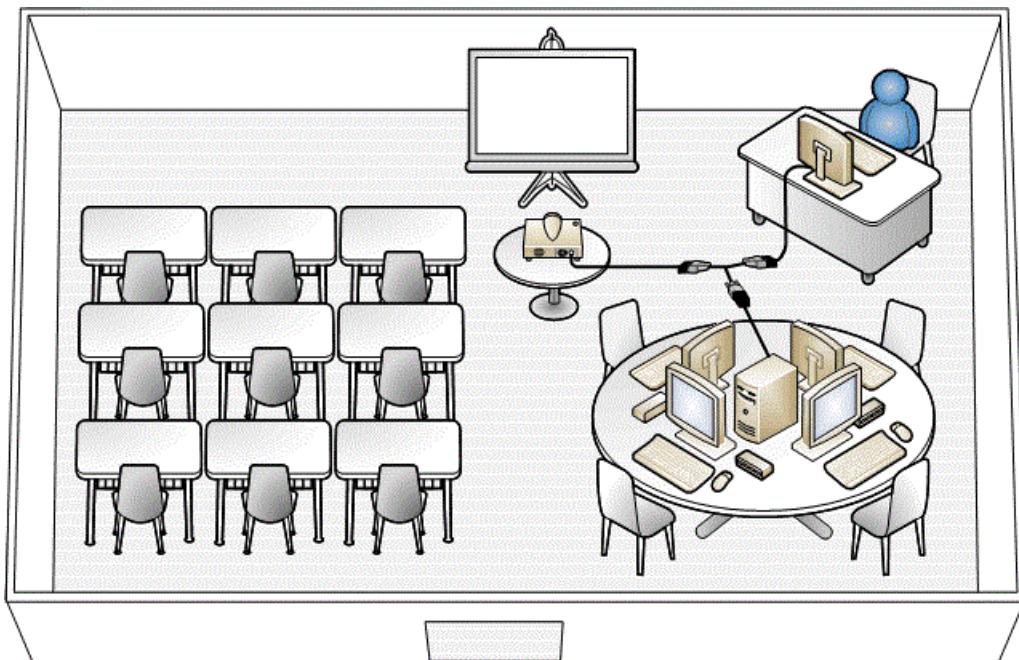
**Gruppen** In diesem Setup sind drei Computer vorhanden, auf denen Multipoint Services ausgeführt wird, wobei Stationen um jeden Computer gruppiert sind.



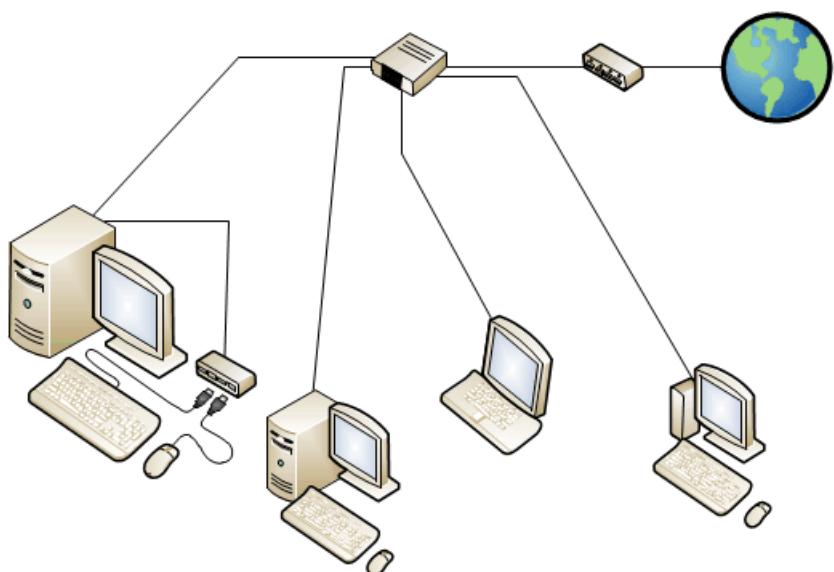
**Vortragsraum** In diesem Setup werden die Stationen in Zeilen eingerichtet. Ein Vorteil dieses Setups besteht darin, dass alle Schüler/Studenten dem Dozenten ausgesetzt sind.



**Aktivitäts Center** Diese Einrichtung besteht aus einem herkömmlichen Vortragsraum Layout für die Schalter und verfügt über einen separaten Bereich mit einem einzelnen Computer, auf dem Multipoint Services mit den zugehörigen Stationen ausgeführt wird.



**Small Business Office** In diesem Setup wird der Computer, auf dem Multipoint Services ausgeführt wird, an einem zentralen Ort platziert, und Benutzer im gesamten Büro stellen eine Verbindung mit dem Computer her, indem Sie ein lokales Netzwerk (LAN-)verwenden.



# Überlegungen zu Netzwerk und Benutzerkonten

09.04.2020 • 10 minutes to read • [Edit Online](#)

Multipoint Services können in einer Vielzahl von Netzwerkumgebungen bereitgestellt werden, und es können lokale Benutzerkonten und Domänen Benutzerkonten unterstützt werden. Im Allgemeinen werden Multipoint Services-Benutzerkonten in einer der folgenden Netzwerkumgebungen verwaltet:

- Einen einzelnen Computer, auf dem Multipoint Services mit lokalen Benutzerkonten ausgeführt wird
- Mehrere Computer, auf denen Multipoint Services ausgeführt wird, jeweils mit einem lokalen Benutzerkonto
- Mehrere Computer, auf denen Multipoint Services ausgeführt wird und die Domänen Benutzerkonten verwenden

Definitionsgemäß können auf *lokale Benutzerkonten* nur von dem Computer aus zugegriffen werden, auf dem Sie erstellt wurden. Lokale Benutzerkonten sind Benutzerkonten, die auf einem bestimmten Computer erstellt werden, auf dem Multipoint Services ausgeführt wird. Im Gegensatz dazu sind *Domänen Benutzerkonten* Benutzerkonten, die sich auf einem Domänen Controller befinden, und auf Sie kann von jedem Computer aus zugegriffen werden, der mit der Domäne verbunden ist. Berücksichtigen Sie Folgendes, wenn Sie entscheiden, welche Art von Netzwerkumgebung Sie verwenden möchten:

- Werden Ressourcen von Servern gemeinsam genutzt?
- Werden Benutzer zwischen Servern wechseln?
- Greifen Benutzer auf Datenbankserver zu, die eine Authentifizierung erfordern?
- Werden Benutzer auf interne Webserver zugreifen, für die eine Authentifizierung erforderlich ist?
- Ist bereits eine Active Directory Domänen Infrastruktur vorhanden?
- Wer verwendet die Multipoint Manager-Konsole zum Verwalten von Benutzer Desktops, zum Anzeigen von Miniaturansichten, zum Hinzufügen von Benutzern, zum Einschränken von Websites usw. Verwaltet diese Person mehr als einen Server? Diese Person muss über Administrator Berechtigungen auf den Servern verfügen.

In den folgenden Abschnitten wird die Benutzerkonten Verwaltung in diesen Netzwerkumgebungen behandelt.

## Einzelner Multipoint-Server mit lokalen Benutzerkonten

In Umgebungen mit einem einzelnen Computer, auf dem Multipoint Services ausgeführt wird, muss kein Netzwerk vorhanden sein. Um Internet Ressourcen zu nutzen, sind die Netzwerk Anforderungen jedoch möglicherweise so einfach wie ein Router und eine Verbindung mit einem Internetdienstanbieter (Internet Service Provider, ISP). Netzwerkverbindungen, die einem Netzwerkkadapter in Multipoint Services zugeordnet sind, werden standardmäßig so konfiguriert, dass automatisch eine IP-Adresse und DNS-Server Adresse über DHCP abgerufen werden. Internet Router werden in der Regel als DHCP-Server konfiguriert und stellen privaten IP-Adressen für Computer bereit, die eine Verbindung mit dem internen Netzwerk herstellen. Daher können von einem einzelnen Computer, auf dem Multipoint Services ausgeführt wird, eine Verbindung mit der internen Schnittstelle des Routers hergestellt, automatische IP-Informationen abgerufen und eine Verbindung mit dem Internet hergestellt werden, ohne dass ein Administrator einen erheblichen Aufwand oder eine andere Konfiguration durchführt.

Eine gängige Methode zum Verwalten von Benutzern in dieser Art von Umgebung ist das Erstellen eines lokalen Benutzerkontos für jede Person, die auf das System zugreift. Jeder Benutzer, der über ein lokales Benutzerkonto auf

diesem Computer verfügt, kann sich von jeder Station, die dem System zugeordnet ist, bei Multipoint Services anmelden. Lokale Benutzerkonten können über den Multipoint-Manager erstellt und verwaltet werden.

## Mehrere Multipoint-Server Systeme mit lokalen Benutzerkonten

Da auf lokale Benutzerkonten nur von dem Computer aus zugegriffen werden kann, auf dem Sie erstellt wurden, können Sie lokale Benutzerkonten auf zwei Arten verwalten, wenn Sie mehrere Multipoint Services-Systeme in einer Umgebung bereitstellen:

- Sie können Benutzerkonten für bestimmte Personen auf bestimmten Computern erstellen, auf denen Multipoint Services ausgeführt wird.
- Mit dem Multipoint-Manager können Sie Konten für jeden Benutzer auf jedem Computer erstellen, auf dem Multipoint Services ausgeführt wird.

Wenn Sie z. B. die Zuweisung von Benutzern zu einem bestimmten Computer planen, auf dem Multipoint Services ausgeführt wird, können Sie auf Computer a (USER01, user02, user03 und user04) und vier lokalen Benutzerkonten auf Computer B (user05, user06, user07 und user08) vier lokale Benutzerkonten erstellen. In diesem Szenario können sich Benutzer 01-04 von jeder Station, die mit ihr verbunden ist, bei Computer A anmelden. Sie können sich jedoch nicht bei Computer B anmelden. Dasselbe gilt für Benutzer 05-08, die sich nur bei Computer B anmelden können, jedoch nicht bei Computer A. je nach der jeweiligen Bereitstellungs Umgebung kann dies akzeptabel oder sogar wünschenswert sein.

Wenn sich allerdings alle Benutzer in der Lage sein müssen, sich bei einem Computer anzumelden, auf dem Multipoint Services ausgeführt wird, muss ein lokales Benutzerkonto für jeden Benutzer auf jedem Computer erstellt werden, auf dem Multipoint Services ausgeführt wird. Wenn Sie die Benutzer auf diese Weise verwalten, werden bestimmte Komplexitäten eingeführt. Wenn sich z. B. USER01 am Montag an Computer a anmeldet und eine Datei im Ordner Dokumente speichert und sich der Benutzer dann am Dienstag an Computer b anmeldet, ist die Datei, die im Ordner Dokumente auf Computer A gespeichert wurde, auf Computer b nicht verfügbar.

Außerdem gibt es keine Möglichkeit, die Kenn Wörter für die Konten automatisch zu synchronisieren, wenn ein Benutzer über Konten auf Computer a und Computer B verfügt. Dies kann dazu führen, dass Benutzer Probleme bei der Anmeldung haben, wenn das Konto Kennwort auf einem Computer geändert wird, nicht jedoch auf dem anderen. Sie können die Benutzerkonten Verwaltung in dieser Art von Netzwerkumgebung vereinfachen, indem Sie jeden Benutzer einem einzelnen Computer zuweisen, auf dem Multipoint Services ausgeführt wird. Auf diese Weise kann sich der Benutzer an allen Stationen anmelden, die diesem Computer zugeordnet sind, und auf die entsprechenden Dateien zugreifen.

## Mehrere Multipoint Services-Systeme mit Domänen Konten

Domänen Umgebungen sind in großen Netzwerkumgebungen üblich, die mehrere Server umfassen. Beispielsweise können Sie einem oder mehreren Computern, auf denen die Multipoint Services-Rolle ausgeführt wird, eine Domäne hinzufügen und dann Microsoft Active Directory zum Verwalten von Benutzerkonten verwenden, auf die von jedem Computer in der Domäne zugegriffen werden kann. Dadurch können einzelne Domänen Benutzerkonten erstellt werden, und der Zugriff erfolgt über eine beliebige Station in jedem Multipoint Services-System, das der Domäne beigetreten ist.

Wenn Sie Multipoint Services in einer Domänen Umgebung bereitstellen, müssen Sie mehrere Faktoren berücksichtigen:

- Wenn Domänen Konten verwendet werden, können Sie nicht über den Multipoint-Manager verwaltet werden.
- Standardmäßig ist Multipoint Services so konfiguriert, dass jeder Benutzer die Berechtigung erhält, sich jeweils nur an einer Station anzumelden. Wenn Sie es Benutzern ermöglichen, sich gleichzeitig mit einem einzelnen Konto bei mehreren Stationen anzumelden, können Sie die Option **Server Einstellungen**

bearbeiten im Multipoint-Manager verwenden.

- Der Speicherort von Domänen Controllern kann sich auf die Geschwindigkeit und Zuverlässigkeit auswirken, mit der sich Benutzer bei der Domäne authentifizieren und Ressourcen suchen können.

## Einzelnes Benutzerkonto für mehrere Stationen

Multipoint Services bietet die Möglichkeit, sich mit einem einzelnen Benutzerkonto gleichzeitig an mehreren Stationen auf demselben Computer anzumelden. Diese Funktion ist nützlich in Umgebungen, in denen Benutzer keine eindeutigen Benutzernamen haben und die Verwendung eines einzelnen Benutzerkontos die Verwaltung des Multipoint Services-Systems vereinfachen kann.

# Speichern von Dateien mit MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Multipoint Services unterstützt das Speichern von Benutzer Dateien auf folgende Weise:

- **In der Betriebssystem Partition des Festplatten Laufwerks.** Standardmäßig speichert Multipoint Services Benutzer Dateien auf der Festplatte mit dem Betriebssystem.
- **In einer separaten Partition des Festplatten Laufwerks.** Wenn das Multipoint Services-System erstmalig eingerichtet wird, können Sie die Festplatte *Partitionieren*. Das heißt, Sie können einen Abschnitt des Laufwerks so konfigurieren, dass er so funktioniert, als ob es sich um ein separates Laufwerk handelt. Dadurch ist es einfacher, das Betriebssystem wiederherzustellen, ohne dass sich dies auf die Benutzer Dateien auswirkt. Weitere Informationen finden Sie unter [Erstellen einer Partition oder eines logischen Laufwerks](#) in der technischen Bibliothek für Windows Server.
- **Auf einem zusätzlichen internen oder externen Festplattenlaufwerk.** Sie können zusätzliche interne oder externe Festplattenlaufwerke an Multipoint Services anfügen, um Daten zu speichern und zu sichern.
- **In einem freigegebenen Netzwerkordner.** Um Benutzer Dateien von einer beliebigen Station aus verfügbar zu machen, können Sie einen freigegebenen Ordner im Netzwerk erstellen. Dies erfordert zusätzlich zum Computer, auf dem Multipoint Services ausgeführt wird, einen anderen Computer oder Server. Dies ist die empfohlene Methode zum Speichern von Dateien, wenn ein Dateiserver verfügbar ist.

Bei kleinen Systemen mit 2-3 Computern, auf denen Multipoint Services ohne verfügbaren Dateiserver ausgeführt wird, kann einer der Multipoint Services-Computer als Dateiserver für alle Multipoint Services-Computer fungieren. Anschließend erstellen Sie Benutzerkonten für alle Benutzer in den Multipoint Services, die als Dateiserver fungieren.

# Schützen des Systemvolumes mit Datenträgerschutz

09.04.2020 • 2 minutes to read • [Edit Online](#)

Multipoint Services bietet die Option, alle Änderungen am System Volume jedes Mal, wenn der Computer gestartet wird, unverzüglich zu löschen. Wenn Sie das Datenträger Schutz Feature aktivieren, werden alle Änderungen am Laufwerk, z. b. eine Beschädigung der Konfiguration oder die Einführung von Schadsoftware, beim nächsten Neustart des Computers rückgängig gemacht. Dies ist ein nützliches Feature für Administratoren, die sicherstellen möchten, dass jedes Mal ein bekanntes "gutes" oder "Golden" Software Image geladen wird. Automatische Updates oder das Patchen von Software kann beispielsweise in der Mitte der Nacht geplant werden. Der Planungs Aspekt ist, ob Endbenutzer in der Lage sein sollen, Änderungen, z. b. das Installieren von Software, über das Internet vorzunehmen. Wenn diese Funktion aktiviert ist und Benutzer in der Lage sein sollen, Dateien zu speichern, muss sich die Dateifreigabe außerhalb des System Volume befinden.

# Unterstützung der Virtualisierung von MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Multipoint Services unterstützt die Hyper-V-Rolle auf zwei Arten:

- Multipoint Services können als Gast Betriebssystem auf einem Server mit Hyper-V bereitgestellt werden.
- Multipoint Services können als Virtualisierungsserver verwendet werden.

Beim Ausführen von Multipoint Services auf einem virtuellen Computer werden die Hyper-V-Tools zum Verwalten von Betriebssystemen verwendet. Zu diesen Tools gehören Checkpoint-und Rollback-Features, die es Ihnen ermöglichen, virtuelle Computer zu exportieren und zu importieren. Bei größeren Installationen können Sie Server konsolidieren, indem Sie mehrere virtuelle Multipoint Services-Computer auf einem einzelnen physischen Server ausführen. Mögliche Szenarien:

- Ein einzelner Classroom oder Lab verfügt über mehr als 20 Arbeitsplätze. Anstatt mehrere physische Computer bereitzustellen, auf denen Multipoint Services ausgeführt wird, können Sie mehrere virtuelle Maschinen auf einem einzelnen physischen Computer bereitstellen.

## NOTE

Sie können mehrere Multipoint-Server, unabhängig davon, ob physisch oder virtuell, über eine einzelne Multipoint Manager-Konsole verwalten.

- Der Multipoint-Server wird auf einem virtuellen Computer mit einer anderen Serverinfrastruktur auf demselben physischen Computer ausgeführt. In diesem Fall zentralisiert diese Serverinfrastruktur die Domäne, die Sicherheit und die Daten für das Netzwerk. Der Multipoint-Server stellt Remotedesktopdienste bereit und zentralisiert die Desktops.

## NOTE

Beim Ausführen von Multipoint Services auf einem virtuellen Computer werden USB-over-Ethernet-und RDP-Client Stationen unterstützt. Direkt Video- und USB-Client verbundene Stationen werden nicht unterstützt.

Weitere Informationen zur Hyper-v-Rolle finden Sie unter [Hyper-v](#).

# Überlegungen zu Anwendungen

09.04.2020 • 2 minutes to read • [Edit Online](#)

## Anwendungskompatibilität

Alle Anwendungen, die Sie in einem Multipoint Services-System ausführen möchten, müssen die folgenden Anforderungen erfüllen:

- Es sollte auf Windows Server 2016 installiert und ausgeführt werden.
- Er muss Sitzungs fähig sein, damit jeder Benutzer eine Instanz der app in einem Multipoint-System ausführen kann.

Wenn die Anwendung diese Anforderung angibt, empfiehlt es sich, zu versuchen, die Anwendung zu installieren und in einer Remote Desktop Sitzung zu verwenden.

## Adressieren von Anwendungs Kompatibilitätsproblemen

Multipoint Services bietet die Option, Stationen vollständigen Instanzen von Windows 10 Enterprise Edition zuzuordnen, die virtuell auf demselben Host Computer ausgeführt werden. Bei kritischen Anwendungen, die nicht mehrere-Instanzen für mehrere Benutzer ausführen oder nicht auf einem 64-Bit-Betriebssystem installiert werden, kann dies eine Lösung sein. Wenn Sie Desktops auf diese Weise bereitstellen, müssen Sie die Registerkarte virtuelle Desktops im Multipoint-Manager für Folgendes

- Virtuelle Desktops aktivieren
- Erstellen einer Desktop Vorlage
- Anpassen der Vorlage mit der Problem Anwendung
- Ordnen Sie Stationen der angepassten Vorlage zu.

Jede Station beginnt mit derselben Vorlage, sodass alle Änderungen bei jedem Start des Computers gelöscht werden.

### NOTE

Es ist wichtig, die Lizenzierungsanforderungen für die Anwendungen zu überprüfen, die Sie auf einem Multipoint ausführen möchten. Obwohl Sie eine Kopier Anwendung installieren, ist möglicherweise eine Lizenzierung pro Benutzer erforderlich.

# Prüfliste vor der Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Verwenden Sie die folgende Checkliste für die Planung der Multipoint Services-Bereitstellung.

SCHRITT	PROBLEM	HILFETHEMA
1.	Überprüfen Sie, ob Ihre Anwendungen mit Multipoint Services kompatibel sind.	<a href="#">Überlegungen zu Anwendungen</a>
2.	Bestimmen Sie die Anzahl der Benutzer, die wahrscheinlich gleichzeitig auf jeden Computer zugreifen, auf dem Multipoint Services ausgeführt wird, damit Sie die Anzahl der erforderlichen Computer einschätzen können, auf denen Multipoint Services ausgeführt werden muss.	<a href="#">Benutzer, Stationen und Computer</a>
3.	Informieren Sie sich über die Softwareanwendungen und den Webinhalt, auf die Benutzer wahrscheinlich zugreifen und die Auswirkungen auf die Systemleistung haben werden.	<a href="#">Hardwareanforderungen und Empfehlungen zur Leistung</a>
4.	Bestimmen Sie die Anzahl und den Typ der Stationen, die mit dem System verbunden werden.	<a href="#">MultiPoint-Stationen</a>
5.	Bestimmen Sie die benötigte Hardware.	<a href="#">Auswählen von Hardware für Ihr Multipoint Services-System und Hardwareanforderungen und Empfehlungen zur Leistung</a>
6.	Legen Sie fest, wo sich das Multipoint Services-System befindet. Wird Sie in einem einzelnen Raum eingerichtet, oder wird Sie so eingerichtet, dass Sie von einem Speicherort zu einem anderen verschoben werden kann?	<a href="#">Planung der Multipoint-Server Site</a>
7.	Bestimmen Sie, wie die Stationen angeordnet werden.	<a href="#">MultiPoint Services-Standortplanung</a>
8.	Überprüfen Sie eine geeignete Strom- und Netzwerkinfrastruktur.	<a href="#">MultiPoint Services-Standortplanung</a>
9.	Bestimmen Sie, wie Benutzerkonten implementiert und verwaltet werden.	<a href="#">Überlegungen zu Netzwerk und Benutzerkonten</a>
10.	Bestimmen Sie, wie Benutzer Dateien freigegeben und gespeichert werden.	<a href="#">Speichern von Dateien mit MultiPoint Services</a>

# Glossar

09.04.2020 • 10 minutes to read • [Edit Online](#)

## Zuordnen einer Station

Zum Angeben des Monitors, der mit der Station und den Peripheriegeräten verwendet wird, z. b. Tastatur und Maus. Bei direkt mit dem Video verbundenen Stationen erfolgt dies durch Drücken eines angegebenen Schlüssels auf der Tastatur der Station, wenn Sie dazu aufgefordert werden. Bei USB-Verbindungen mit Clientverbindungen erfolgt dies in der Regel automatisch.

## Bus-gestützter Hub

Ein Hub, der seine gesamte Leistung von der USB-Schnittstelle des Computers zeichnet. Für Bus gestützte Hubs sind keine separaten Stromverbindungen erforderlich. Viele Geräte funktionieren jedoch nicht mit dieser Art von Hub, da Sie mehr Energie benötigen, als diese Art von Hub bereitstellt.

## Konsolenmodus

In einem der beiden Modi kann Multipoint Services gestartet werden. Wenn sich das System im Konsolenmodus befindet, sind keine Stationen zur Verwendung verfügbar. Stattdessen werden alle Monitore als einzelner erweiterter Desktop für die Konsolen Sitzung des Computer Systems behandelt. Der Konsolenmodus wird normalerweise verwendet, um Software zu installieren, zu aktualisieren oder zu konfigurieren, die nicht ausgeführt werden kann, wenn sich der Computer im Stations Modus befindet. Siehe auch: *Stations Modus*.

## direkt mit Videos verbundene Station

Eine Multipoint-Station, die aus einem Monitor besteht, der direkt mit einer Videoausgabe auf dem Server verbunden ist, und mindestens eine Tastatur und eine Maus enthält, die über einen USB-Hub mit dem Server verbunden sind.

## Domänen Benutzerkonto

Ein Benutzerkonto, das auf einem Domänen Computer gehostet wird. Der Zugriff auf Domänen Benutzerkonten kann von jedem Computer aus erfolgen, der mit der Domäne verbunden ist, und ist nicht an einen bestimmten Computer gebunden.

## Downstream-Hub

Ein Hub, der mit einem stationshub verbunden ist, um weitere verfügbare Ports für Stations Geräte hinzuzufügen. An einen Downstream-Hub darf keine Tastatur angefügt sein.

## extern gestützter Hub

Dieser Hub wird auch als selbst gestützter Hub bezeichnet und nutzt seine Leistungsfähigkeit von einer externen Netzteil Einheit. aus diesem Grund kann ein vollständiger Strom (bis zu 500 mA) für jeden Port bereitgestellt werden. Viele Hubs können als busgestützte oder extern betriebene Hubs betrieben werden.

## HID-consumersteuerunggerät

Ein Eingabegerät (HID) ist ein Computer Gerät, das direkt mit den Menschen interagiert. Es kann Eingaben aus der Eingabe oder Ausgabe an Menschen übermitteln. Beispiele hierfür sind Tastatur, Maus, Trackball, Touchpad, zeige Stick, Grafik Tabelle, Joystick, Fingerabdruckscanner, Gamepad, Webcam, Headset und Fahr simulatorgeräte. Ein geverstecktem consumersteuerunggerät ist eine bestimmte Klasse von verborgenen Geräten, die audiovolumensteuerelemente und Multimedia-und Browser-Steuerelement Tasten umfasst.

## Zwischenhub

Ein Hub zwischen einem *Stammhub* auf dem Server und einem stationshub. Zwischen Hubs werden in der Regel verwendet, um die Anzahl der verfügbaren Ports für Stations Hubs zu erhöhen oder um die Entfernung der Stationen vom Computer zu verlängern.

## **lokales Benutzerkonto**

Ein Benutzerkonto auf einem bestimmten Computer. Ein lokales Benutzerkonto ist nur auf dem Computer verfügbar, auf dem das Konto definiert ist.

## **multifunktionshub**

Siehe *USB-Zero-Client*.

## **Multipoint Services-System**

Eine Sammlung von Hardware und Software, die aus einem Computer besteht, auf dem Windows Server 2016 mit aktivierter Multipoint Services-Rolle und mindestens einer Multipoint-Station installiert ist. Weitere Informationen zu systemlayoutoptionen finden Sie unter [Planen von Multipoint Services-Websites](#).

## **spaltet**

Ein Abschnitt des Speicherplatzes auf einem physischen Datenträger, der so funktioniert, als handele es sich um einen separaten Datenträger.

## **primäre Station**

Die Station, die beim Starten von Multipoint Services zuerst gestartet werden soll. Die primäre Station kann von einem Administrator verwendet werden, um auf Startmenüs und-Einstellungen zuzugreifen. Wenn Sie nicht vom Administrator verwendet wird, kann Sie als normale Station verwendet werden (Sie muss nicht ausschließlich für die Verwaltung reserviert werden). Der Monitor der primären Station muss stets direkt mit einer Videoausgabe auf dem Computer verbunden sein, auf dem Multipoint Services ausgeführt wird. Siehe auch: Station.

## **RDP-über-LAN-verbundene Station**

Eine Station, bei der es sich um einen Thin Client, herkömmlichen Desktop Computer oder Laptop Computer handelt, der mithilfe von Remotedesktopprotokoll (RDP) über das lokale Netzwerk (Local Area Network, LAN) eine Verbindung mit Multipoint Services herstellt.

## **stamphub**

Ein USB-Hub, der auf dem Host Controller auf der Hauptplatine eines Computers integriert ist.

## **Bildschirm teilen**

Eine Station, in der ein einzelner Monitor verwendet werden kann, um zwei unabhängige Benutzer Desktops anzuzeigen. Zwei Gruppen von Hubs, Tastaturen und Mäusen sind einem einzigen Monitor zugeordnet. Der linken Seite des Monitors wird ein Satz zugeordnet, und die andere Gruppe ist der rechten Seite des Monitors zugeordnet.

## **Standard Station**

Im Gegensatz zur *primären Station*, die von einem Administrator verwendet werden kann, um auf Startmenüs zuzugreifen, werden Standard Stationen keine Startmenüs angezeigt, und Sie können erst nach Abschluss des Startvorgangs von Multipoint Services verwendet werden. Siehe auch: Station.

## **Senders**

Benutzer Endpunkt zum Herstellen einer Verbindung mit dem Computer, auf dem Multipoint Services ausgeführt wird. Drei Stations Typen werden unterstützt: Direct-Video-Connected, USB-Zero-Client-Connected und RDP-over-LAN-verbundene Stationen. Weitere Informationen zu Stationen finden Sie unter [Multipoint-Stationen](#).

## **stationshub**

Ein USB-Hub, der einem Monitor zugeordnet ist, um eine Multipoint-Station zu erstellen. Er verbindet Peripheriegerät-USB-Geräte mit Multipoint Services. Siehe auch: *USB-Zero-Client* und *USB-Hub*.

## **Stations Modus**

In einem der beiden Modi kann Multipoint Services gestartet werden. In der Regel befindet sich das Multipoint Services-System im Stations Modus. Im Stations Modus Verhalten sich die Multipoint Services-Stationen so, als ob jede Station ein separater Computer ist, auf dem das Windows-Betriebssystem ausgeführt wird, und mehrere Benutzer können das System gleichzeitig verwenden. Siehe auch: *Konsolenmodus*.

## **USB-Hub**

Ein generischer Multiport-USB-erweiterungshub, der den Spezifikationen für den universellen seriellen Bus (USB) 2,0 oder höher entspricht. Solche Hubs verfügen in der Regel über mehrere USB-Ports, sodass mehrere USB-Geräte mit einem einzelnen USB-Anschluss auf dem Computer verbunden werden können. USB-Hubs sind in der Regel separate Geräte, die *extern* oder im *Bus betrieben* werden können. Einige andere Geräte, z. B. einige Tastaturen und Videomonitore, können einen USB-Hub in Ihren Entwurf integrieren. Siehe auch: *USB-Zero-Client*.

### **USB-over-Ethernet-Client**

Ein USB-Null-Client, der über eine LAN-Verbindung anstelle eines USB-Ports eine Verbindung mit dem Computer herstellt. Dieser Client wird dem Server als USB-Gerät angezeigt, auch wenn die Daten über die Ethernet-Verbindung gesendet werden.

### **USB-Zero-Client**

Ein erweiterungshub, der über einen USB-Anschluss eine Verbindung mit dem Computer herstellt und die Verbindung verschiedener nicht-USB-Geräte mit dem Hub ermöglicht. USB-Clients werden von bestimmten Hardwareherstellern erstellt und erfordern die Installation eines gerätespezifischen Treibers. USB-Null-Clients unterstützen das Verbinden eines Video Monitors (über VGA, DVI usw.) und Peripheriegeräte (über USB, manchmal PS/2 und Analoge Audiodaten). Der USB-Null-Client kann *extern* oder per *busstrom betrieben* werden. Siehe auch *USB-Hubs*.

### **Verbindung zwischen USB-Client und Verbindung**

Eine Multipoint Services-Station, die (mindestens) einen Monitor, eine Tastatur und eine Maus umfasst, die über einen USB-Client mit dem Server verbunden sind.

# Migration von Multipoint Services in Windows Server 2016

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Sie können von einer früheren Version von Windows Server 2016 Multipoint Services zur RTM-Version von Multipoint Services migrieren. Die folgenden Informationen enthalten Informationen zur Vorbereitung sowie zu Migrations- und Überprüfungs Schritten.

Die Migrations Dokumentation und -Tools vereinfachen die Migration von Server Rollen Einstellungen und Daten von einem vorhandenen Server zu einem Zielserver, auf dem Windows Server 2016 ausgeführt wird. Mit dem in diesem Handbuch beschriebenen Prozess können Sie den Migrationsvorgang vereinfachen, die Migration beschleunigen, ihre Genauigkeit verbessern und mögliche Konflikte vermeiden, die andernfalls während der Migration auftreten können.

## Was Sie wissen sollten, bevor Sie beginnen

Beachten Sie Folgendes, bevor Sie mit der Migration beginnen:

- Bei der Migration werden Einstellungen für Anwendungen in der Multipoint Services-Rolle nicht automatisch erfasst oder aufgezeichnet. Sie sollten einen angepassten Migrationsplan für alle Anwendungen erstellen, die Sie migrieren möchten. Dies gilt auch, wenn das Feature für virtuelle Desktops in Multipoint Services verwendet wird.
- Dieses Handbuch enthält keine Anleitungen zum Verschieben von Daten, die in Benutzer- oder freigegebenen Ordner auf dem Multipoint-Server gespeichert sind. Dies gilt für reguläre Stationen und virtuelle Desktop Stationen.
- Dieses Handbuch enthält keine Anweisungen zum Migrieren, wenn auf dem Quell Server mehrere Rollen ausgeführt werden. Wenn auf dem Server mehrere Rollen ausgeführt werden, müssen Sie ein benutzerdefiniertes Migrationsverfahren entwerfen, das für Ihre Serverumgebung spezifisch ist, basierend auf Informationen, die in den Handbüchern für die Rollen Migration bereitgestellt werden.
- Dieses Handbuch enthält keine Informationen zum Migrieren von Remotedesktopdienste CALs. Informationen zu diesen Informationen finden Sie unter [Migrieren von Remotedesktopdienste Client Zugriffs Lizenzen \(RDS-CALs\)](#).

## Unterstützte Migrationsszenarien für Multipoint Services in Windows Server 2016

Die Multipoint Service-Rollen Dienste sind in Windows Server 2016 Standard und Datacenter verfügbar. In diesem Migrations Handbuch wird beschrieben, wie Sie die Multipoint Services-Rollen Dienste von einem Quell Server unter Windows Server 2016 zu einem Zielserver migrieren, auf dem die gleiche Version ausgeführt wird.

## Nicht unterstützte Szenarien

Die folgenden Migrationsszenarien werden nicht unterstützt:

- Migrieren oder Aktualisieren von Windows MultiPoint Server 2012 und 2011.
- Migrieren von einem Quell Server zu einem Zielserver, auf dem unter einem Betriebssystem ausgeführt wird,

auf dem eine andere Benutzeroberflächen Sprache des Systems installiert ist.

- Migrieren des Multipoint Services-Rollen Diensts von physischen Servern zu virtuellen Maschinen.
- Migrieren von Anwendungen oder Anwendungseinstellungen vom Multipoint-Server.

## Auswirkungen der Migration auf Multipoint Services

Beachten Sie, dass die Multipoint Services-Rolle während der Migration nicht verfügbar ist. Planen Sie die Datenmigration für einen Zeitraum mit geringerer Auslastung, um die Ausfallzeit und die Auswirkungen auf Benutzer gering zu halten. Benachrichtigen Sie die Benutzer, dass die Ressourcen während dieser Zeit nicht verfügbar sind.

## Migrations Informationen und-Schritte

Verwenden Sie die folgenden Informationen, um die Multipoint Services-Migration zu planen und auszuführen:

- [Sammeln Sie die Informationen, die Sie für die Migration benötigen.](#)
- [Migrieren Sie den Multipoint Services-Rollen Dienst.](#)
- [Überprüfen der Migration und Ausführen von Bereinigungs Tasks nach der Migration](#)

# Vorbereiten der Migration zu Multipoint Services in Windows Server 2016

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Verwenden Sie die folgenden Informationen, um die Informationen zu sammeln, die Sie benötigen, um den Multipoint Services-Rollen Dienst von einem Quell Server mit einer früheren Version von Windows Server 2016 zu einem Zielserver mit Windows Server 2016 RTM zu migrieren.

Sie müssen mindestens Mitglied der Gruppe "Administratoren" auf dem Quell Server und dem Zielserver sein, um Multipoint Services zu installieren, zu entfernen oder einzurichten.

## NOTE

Die hier beschriebenen Schritte bieten keine Anleitungen zum Migrieren von Daten, die in Benutzer Ordnern oder freigegebenen Ordnern gespeichert sind. Stellen Sie sicher, dass die Benutzer Ihre Daten sichern, bevor Sie mit der Migration beginnen.

Verwenden Sie Multipoint Manager, um die für die Migration erforderlichen Informationen abzurufen. Sie benötigen die Server Administrator Berechtigung, um den Multipoint-Manager zu verwenden.

Notieren Sie den Multipoint-Server, den Benutzer und die Umgebungseinstellungen im [Arbeitsblatt für die Sammlung von Migrationsdaten](#). Verwenden Sie die folgenden Schritte, um diese Informationen zu erfassen.

## Multipoint-Serveereinstellungen für den lokalen Server

1. Starten Sie den Multipoint-Manager.
2. Wählen Sie auf der Registerkarte **Startseite** den lokalen Server aus, und klicken Sie dann auf **Servereinstellungen bearbeiten**.
3. Notieren Sie die Einstellungen im Daten Arbeitsblatt.
4. Schließen Sie das Fenster Einstellungen.

## Verwaltete Server und Computer

Die Namen der verwalteten Server und Computer finden Sie auf der Registerkarte **Start** im Multipoint-Manager.

## Stations Einstellungen

Wenn die automatische Anmeldung oder Anzeige Ausrichtung für die Station konfiguriert ist, verwenden Sie die folgenden Schritte, um diese Informationen abzurufen. Andernfalls können Sie diesen Schritt überspringen.

So rufen Sie die Stations Einstellungen ab:

1. Wechseln Sie im Multipoint-Manager zur Registerkarte **Stationen**.
2. Suchen Sie in der Spalte für die **automatische Anmeldung** eine Station, die "yes" aufweist.
3. Wählen Sie diese Station aus, und klicken Sie dann auf **Station konfigurieren**.
4. Notieren Sie den Benutzer, der für die automatische Anmeldung verwendet wird.

Zum Abrufen der Einstellungen für die Anzeige Ausrichtung zeigen Sie die **Stations Einstellungen** für jede Station an.

## Liste der Benutzer

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Benutzer** .
2. Notieren Sie sich die Benutzer Zugriffsrechte für **Administrator** und **Multipoint-Dashboard** .
3. Notieren Sie die Standardbenutzer.

## Standort der VDI-Vorlage

Wenn Sie zuvor die VDI-Vorlagen Funktion aktiviert haben, notieren Sie den Speicherort der VDI-Vorlage. Solange sich die Quell-und Zielserver im gleichen Netzwerk befinden, können Sie die Vorlage mithilfe von Multipoint Manager importieren.

## Nächster Schritt

Sie sind jetzt bereit für die [Migration zu Multipoint Services](#) in der RTM-Version von Windows Server 2016.

# Planen des Arbeitsblatts für die Multipoint Services-Migration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Verwenden Sie die folgenden Listen und Tabellen, um die Einstellungen zu erfassen, die Sie bei der Multipoint Services-Migration benötigen.

## Quellservereinstellungen

Sie finden die Servereinstellungen auf der Registerkarte **Start** im Multipoint-Manager. Platzieren Sie ein Häkchen neben jeder Einstellung, die auf dem Quell Server verwendet wird.

- Gestatten Sie, dass ein Konto über mehrere Sitzungen verfügt.
- Ermöglicht die Remote Verwaltung dieses Computers.
- Hiermit wird die Überwachung der Desktops dieses Computers ermöglicht.
- Starten Sie immer im Konsolenmodus.
- Datenschutz Benachrichtigung bei der ersten Benutzeranmeldung nicht anzeigen.
- Weisen Sie jeder Station eine eindeutige IP-Adresse zu.
- Lässt zwischen dem Multipoint-Dashboard und den Benutzersitzungen auf diesem Computer zu.
- Ermöglicht die Orchestrierung von Administrator-und Multipoint-dashboardbenutzersitzungen.
- Ermöglicht Stationen die Verwendung des GPU-Hardware Rendering.

## Verwaltete Server und Computer

Notieren Sie die Namen der verwalteten Server und Computer. Diese Informationen finden Sie auf der Registerkarte **Startseite** im Multipoint-Manager.

COMPUTER	COMPUTERNAME
1	
2	
3	
4	
5	
6	
7	
8	

COMPUTER	COMPUTERNAME
9	
10	

## Station

Notieren Sie die lokalen Stationen und deren Einstellungen. Diese Informationen finden Sie auf der Registerkarte **Stationen** im Multipoint-Manager.

#	STATIONSNAME	BENUTZERKONTO FÜR DIE AUTOMATISCHE ANMELDUNG	BILDSCHIRMAUSRICHTUNG
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

## Administratoren und Multipoint-Dashboardbenutzer

Kopieren Sie die Benutzernamen für die Benutzer von Administratoren und Multipoint-Dashboards. Diese Informationen finden Sie auf der Registerkarte **Benutzer** im Multipoint-Manager.

Administratoren:

- Benutzername:

Dashboardbenutzer:

- Benutzername:
- Benutzername:

- Benutzername:
- Benutzername:
- Benutzername:

## VDI-Vorlage und virtuelle Desktops

Notieren Sie die VDI-Vorlagen Informationen und die Namen virtueller Desktops in der Multipoint Services-Bereitstellung. Diese Informationen finden Sie auf der Registerkarte **virtuelle Desktops** im Multipoint-Manager.

Speicherort der VDI-Vorlage:

#	NAME DES VIRTUELLEN DESKTOPS
1	
2	
3	
4	
5	

# Migrieren zu Multipoint Services in Windows Server 2016

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Führen Sie die folgenden Schritte aus, zuzüglich der Informationen, die Sie im Arbeitsblatt zur Migrationsplanung gesammelt haben, um zu Multipoint Services in Windows Server 2016 zu migrieren.

## Servereinstellungen übertragen

Öffnen Sie auf dem Zielserver den Multipoint-Manager. Klicken Sie auf **Servereinstellungen bearbeiten**. Übernehmen Sie die Einstellungen gemäß dem Arbeitsblatt für die Migrationsplanung.

### NOTE

Wenn Sie den Datenträger Schutz auf dem Zielserver aktivieren müssen, warten Sie, bis Sie Multipoint Services konfiguriert haben.

## Übertragungs Stations Einstellungen

Stellen Sie sicher, dass die Stationen mit dem Zielserver verbunden sind und alle zugeordnet sind, bevor Sie die Stations Einstellungen anwenden. Die Stationen werden automatisch erkannt. Befolgen Sie die Anweisungen auf den einzelnen Stations Bildschirm, um die Server Zuordnung von Benutzer Stationen und verbundenen USB-Geräten zu definieren. Wenden Sie die im Arbeitsblatt für die Migrationsplanung aufgeführten bevorzugten Stations Einstellungen an.

## Migrieren der VDI-Vorlage

Bevor Sie die VDI-Vorlage vom Quell Server importieren können, können Sie virtuelle Desktops auf dem Zielserver mithilfe von Multipoint Manager aktivieren:

1. Wechseln Sie im Multipoint-Manager zur Registerkarte **virtuelle Desktops**.
2. Klicken Sie auf **aktivierte virtuelle Desktops**. Der Server installiert die Hyper-V-Rolle und startet dann neu.
3. Öffnen Sie den Multipoint-Manager, und navigieren Sie zurück zu **virtuelle Desktops**.
4. Klicken Sie auf **Vorlage für virtuellen Desktop importieren**. Befolgen Sie die Anweisungen, um die Vorlage vom Quell Server zu importieren.

### NOTE

Wenn Sie eine Vorlage für virtuelle Desktops importieren, werden alle Anpassungen, die auf die Vorlage angewendet werden, zurückgesetzt.

## Nächster Schritt

[Überprüfen Sie die neue Multipoint Services-Bereitstellung.](#)

# Multipoint Services-Aufgaben nach der Migration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Nachdem Sie zu Multipoint Services in Windows Server 2016 migriert haben, verwenden Sie die folgenden Informationen, um die Migration zu überprüfen und um Bereinigungs Schritte auszuführen.

## Überprüfen der Migration durch Ausführen eines Pilotprogramms

Sie können Ihre Multipoint Services-Migration überprüfen, indem Sie in der Produktionsumgebung ein Pilotprojekt erstellen. Führen Sie das Pilotprojekt auf den Servern aus, bevor Sie die migrierten Rollen Dienste in der Produktionsumgebung ablegen, um sicherzustellen, dass die Bereitstellung erwartungsgemäß funktioniert. Beschränken Sie die Anzahl der Verbindungen zunächst, und erhöhen Sie die Anzahl der Benutzer, die auf Multipoint Services zugreifen.

### NOTE

Verwenden Sie immer Testkonten, um die Migration zu testen. Verwenden Sie ein Konto mit Administratorrechten und einem Konto für einen gültigen Benutzer.

## Zurückziehen des Quellservers

Nachdem Sie die Migration überprüft haben, können Sie den Quell Server von Ihrem Netzwerk Herunterfahren oder trennen. Wenn der Server einer Domäne beigetreten ist, entfernen Sie ihn aus der Domäne, bevor Sie die Verbindung trennen.

# Bereitstellen von MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

In diesem Leitfaden wird beschrieben, wie Sie einen Server bereitstellen, auf dem Multipoint Services ausgeführt wird, und Sie können Multipoint-Stationen einrichten, das System installieren und konfigurieren, Benutzerkonten einrichten und einige grundlegende Verwaltungsaufgaben ausführen, wie z. B. das Aktivieren des Datenträger Schutzes und das Einrichten von Sicherungen, bevor Sie das System verwenden

## NOTE

Weitere Unterstützung finden Sie in der Hilfe zu Multipoint Services, die geöffnet werden kann, indem Sie auf einem Multipoint-Manager oder einem Multipoint-dashboardbildschirm auf das Hilfe Symbol oder F1 klicken.

Die Bereitstellungs Informationen sind wie folgt organisiert. Sie müssen mindestens die Aufgaben für die Bereitstellung Ihres Systems durchführen und die Umgebung für Benutzer vorbereiten. Andere Aufgaben können für Ihre Umgebung gelten.

- [Bereitstellen eines neuen MultiPoint Services-Systems](#)

Einrichten des Multipoint Services-Computers und der Stationen. Installieren und Konfigurieren von Multipoint Services Einrichten der Stationen Installieren von Treibern, Updates und Software optional einer Domäne beitreten Fügen Sie Client Lizenzen (CALs) für jede Station hinzu.

- [Optionale Konfigurationsaufgaben für eine MultiPoint Services-Bereitstellung](#)

Führen Sie optionale Konfigurationsaufgaben aus. Einrichten einer unterteilten Bildschirm Station Drucker hinzufügen; Aktivieren des Zugriffs über ein drahtloses LAN Erstellen virtueller Desktops für Stationen mit dem Betriebssystem Windows 10, Windows 8 oder Windows 7 Ändern Sie die Anzeige Sprache für das System oder für einzelne Benutzer.

- [Vorbereiten Ihres Multipoint Services-Systems für Benutzer](#)

Planen und Erstellen von Benutzerkonten beschränken Sie den Benutzer Zugriff auf den Server. Konfigurieren Sie für den offenen Zugriff Stationen für die automatische Anmeldung. mehrere Sitzungen für freigegebene Benutzerkonten zulassen Implementieren Sie die Dateifreigabe für Benutzer.

- [Systemverwaltung in MultiPoint Services](#)

Führen Sie einige grundlegende Server Verwaltungsaufgaben aus, bevor Sie mit der Verwendung des Servers beginnen. Datenträger Schutz aktivieren; Server Sicherung installieren; um Energie zu sparen, konfigurieren Sie die standbyeinstellungen. Konfigurieren Sie Gruppenrichtlinien und die Registrierung für eine Domänen Bereitstellung.

## Siehe auch

- [MultiPoint Services](#)
- [Multipoint Services-Forum](#)

# Bereitstellen eines neuen Windows MultiPoint Services-Systems

09.04.2020 • 2 minutes to read • [Edit Online](#)

In den Themen in diesem Abschnitt wird erläutert, wie Sie Ihr Multipoint Services-System einrichten. Sie installieren und konfigurieren einen Multipoint-Server. Einrichten der Stationen Installieren von Treibern, Updates und Software optional einer Domäne beitreten Multipoint-Server aktivieren; und fügen Client Zugriffs Lizenzen (Client Access Licenses, CALs) für jede Station hinzu.

## IMPORTANT

Wenn Sie Ihre Multipoint Services-Bereitstellung noch nicht geplant haben, finden Sie weitere Informationen unter [Planning a Windows MultiPoint Services Deployment](#).

## Inhalt dieses Abschnitts

Für die Erstinstallation wird empfohlen, die Aufgaben in der Reihenfolge auszuführen, in der Sie angezeigt werden.

1. [Erfassen der für die Installation benötigten Hardware und Gerätetreiber](#)
2. [Einrichten des physischen Computers und der primären Station](#)
3. [Installieren von Windows Server 2016 und Registrieren von Multipoint Services](#)
4. [Aktualisieren und Installieren von Gerätetreibern bei Bedarf](#)
5. [Festlegen des Datums, der Uhrzeit und der Zeitzone](#)
6. [Hinzufügen des Multipoint Services-Systems zu einer Domäne \(optional\)](#)
7. [Updates installieren](#)
8. [Anfügen zusätzlicher Stationen an den Multipoint Services-Computer](#)
9. [Aktivieren von Windows Server 2016 und Hinzufügen von Remotedesktopdienste CALs](#)
10. [Installieren von Software auf Ihrem Multipoint Services-System](#)

# Erfassen von der für die Installation benötigten Hardware und Gerätetreiber

09.04.2020 • 2 minutes to read • [Edit Online](#)

Bevor Sie mit der Bereitstellung Ihres Multipoint Services-Systems beginnen, benötigen Sie Folgendes:

- **Hardware Komponenten für den Server** : Installieren Sie zu diesem Zeitpunkt alle zusätzlichen Grafikkarten oder anderen Systemkomponenten.
- **Hardwarekomponenten für die Stationen** : Informationen zum Planen von Stationen für Ihre Umgebung finden Sie unter [Auswählen von Hardware für Ihr Multipoint Services-System](#).
- **Die neuesten Treiber für ihre Grafikkarten** : Wenn Ihr OEM-oder Gerätehersteller diese nicht bereitgestellt hat, müssen Sie sie von der Website des Geräteherstellers herunterladen.
- **Die neuesten USB Zero-Client Treiber** : Wenn Sie USB-Client Stationen verwenden, müssen Sie die neuesten USB-Client Treiber installieren.

## IMPORTANT

Für eine Multipoint Services-Installation müssen Sie die 64-Bit-Version der Treiber installieren.

## TIP

Wenn Sie Multipoint Services auf einem Computer installieren, auf dem bereits eine andere Version von Windows installiert ist, sollten Sie vor dem Starten der Windows Server-Installation das Videokarten-und-Modell in Geräte-Manager finden und sicherstellen, dass Sie Treiber abrufen können, die für Windows Server 2016 verfügbar sind. Öffnen Sie Geräte-Manager, und öffnen Sie die **Computer Verwaltung** über den **Start** Bildschirm. Klicken Sie dann in der Konsolen Struktur auf **Geräte-Manager**.

# Einrichten des physischen Computers und der primären Station

09.04.2020 • 4 minutes to read • [Edit Online](#)

Vor der Installation von Multipoint Services müssen Sie die primäre Station für Ihr Multipoint Services-System einrichten. Wenn Sie ein LAN (Local Area Network) verwenden, verbinden Sie den Computer mit dem LAN.

Eine *Station* ist ein Endpunkt, über den auf Multipoint Services zugegriffen wird. Die *primäre Station* ist die erste Station, die gestartet wird, wenn Multipoint Services gestartet wird. Administratoren können Sie verwenden, um auf Startmenüs und-Einstellungen zuzugreifen. Die primäre Station ermöglicht den Zugriff auf Systemkonfigurations-und Problem Behandlungsinformationen, die nur während des Starts und vor der Ausführung des Multipoint Services-Systems verfügbar sind. Nach dem Start können Sie die primäre Station wie jede andere Station verwenden.

Bei der primären Station muss es sich um eine Station mit direkt Videoverbindung handeln. Im folgenden Verfahren wird beschrieben, wie Sie die erforderliche Hardware mit Ihrem Multipoint Services-Computer verbinden.

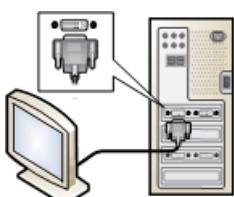
Weitere Informationen zu Stationen finden Sie unter [Multipoint-Stationen](#). Hilfe zum Treffen von Hardware Auswählen finden [Sie unter Auswählen von Hardware für Ihr Multipoint Services-System](#). Informationen zum Verbinden anderer Stations Typen mit Multipoint Services finden Sie unter [Anfügen zusätzlicher Stationen an Ihren Multipoint Services-Computer](#).

## NOTE

Um eine Station mit Videoverbindung zu erstellen, müssen Sie eine lateinische Tastatur verwenden (z. b. eine englische oder spanischsprachige Tastatur).

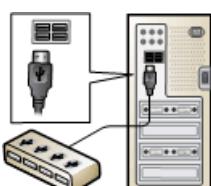
## So richten Sie Ihre primäre Station ein

1. Stellen Sie sicher, dass der Computer, auf dem Multipoint Services ausgeführt wird, ausgeschaltet ist.
2. Verbinden Sie das Netzkabel des Monitors mit einer Stromversorgung, und verbinden Sie das Monitorkabel mit dem Video anschauport auf dem Computer, wie unten gezeigt.



3. Wenn die Station eine USB-Tastatur und-Maus verwendet, führen Sie die folgenden Schritte aus:

- a. Stellen Sie eine Verbindung zwischen einem externen USB-Hub und einem geöffneten USB-Anschluss auf dem Computer her (siehe unten).



- b. Verbinden Sie die USB-Tastatur und die Maus mit dem USB-Hub.



**NOTE**

Wenn Ihr Multipoint Services-Computer über PS/2-Ports verfügt, können Sie bei Bedarf eine PS/2-Tastatur verwenden und die Maus direkt an den Computer angeschlossen. Diese Einrichtung hat jedoch erhebliche Einschränkungen. Benutzer können keine Audiogeräte, Web-Cams und Flash Laufwerke auf PS/2-Stationen verwenden.

- c. Wenn Sie einen extern betriebenen Hub verwenden, verbinden Sie das Netzkabel des Hubs mit einer Stromversorgung.

**IMPORTANT**

Wir empfehlen dringend die Verwendung eines gestützten Hubs. Ein erratisches Systemverhalten kann sich aus unter aktuellen Bedingungen ergeben.

Benutzer dürfen keine Maus und Tastatur direkt an die USB-Anschlüsse des Computers anfügen. Dadurch wird wahrscheinlich die falsche Zuordnung mehrerer Tastaturen und Mäuse zur gleichen Station oder zu keiner Station ausgelöst.

**NOTE**

Das hostaudiogerät auf der Hauptplatine des Systems ist nur verfügbar, wenn sich Multipoint Services im Konsolenmodus befindet. Sie müssen ein USB-Audiogerät verwenden, das mit dem Hub verbunden ist, um das ununterbrochene Audiomaterial für eine Station sicherzustellen, die einen externen USB-Hub verwendet.

## So verbinden Sie den Computer mit dem LAN

- Wenn Sie über ein LAN verfügen, verbinden Sie Ihren Computer mit Ihrem Netzwerk über ein Netzwerkkabel.

# Installieren von MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie einen Server von Grund auf neu installieren, befolgen Sie diese Anweisungen, um Multipoint Services zu installieren.

Nachdem Sie Windows Server 2016 installiert haben, melden Sie sich erfolgreich als Administrator an. Verwenden Sie die Server-Manager, in der Sie Multipoint Services aktivieren können. Der Server-Manager wird beim Start automatisch geöffnet. Wählen Sie auf dem Dashboard **Rollen und Features hinzufügen** aus, um Multipoint Services zu aktivieren, und befolgen Sie die Anweisungen im Assistenten.

Im Abschnitt für den Installationstyp können Sie entweder mit dem

- Rollenbasierte oder featurebasierte Installation oder
- Installation von Remotedesktopdiensten

Für Standard Bereitstellungen von Multipoint Services empfiehlt es sich, die Remotedesktopdienste Installation auszuwählen, mit der Sie die Multipoint Services-Rolle unter Bereitstellungstyp bequem auswählen können. Bei der rollenbasierten Installation müssen Sie in der Liste der Rollen **Multipoint Services** auswählen. Der Server wird nach der erfolgreichen Installation neu gestartet.

## Konfigurieren der primären Station

1. Geben Sie auf der Seite **Multipoint-Server Station erstellen** den angegebenen Buchstaben von der Tastatur für diesen Monitor ein. Mit dem richtigen Schlüssel Eintrag werden die Tastatur und die Maus für diese Station verknüpft.
2. Melden Sie sich als Administrator an.

# Aktualisieren und Installieren von Gerätetreibern bei Bedarf

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie USB-Clients oder Peripheriegeräte verwenden, die Treiber erfordern, sollten Sie die Treiber zu diesem Zeitpunkt installieren. Es empfiehlt sich auch, **Geräte-Manager** auf Treiber Warnungen zu überprüfen und Treiber für diese Geräte zu installieren.

Im Allgemeinen sind die aktuellen Treiber für die folgenden Arten von Geräten erforderlich:

- USB-Clients
- USB-over-Ethernet-Clients (null)
- Datenträger Controller
- Netzwerkadapter
- Sound Controller
- USB-Host Controller
- Grafikkarten

## So überprüfen Sie die Treiber Warnungen in Geräte-Manager

1. Öffnen Sie den Start Bildschirm.
2. Geben Sie **Computer Verwaltung** ein, und klicken Sie dann in den Ergebnissen auf **Computer Verwaltung**.
3. Klicken Sie in der Konsolen Struktur der Computer Verwaltung auf **Geräte-Manager**.
4. Überprüfen Sie in den System Geräten auf der rechten Seite die Treiber Warnungen, die sich auf Multipoint Server auswirken können.

## So installieren Sie Gerätetreiber im Multipoint-Manager

1. Um den Multipoint-Manager zu öffnen, suchen Sie nach "Multipoint-Manager", und klicken Sie dann in den Ergebnissen auf **Multipoint-Manager**.
2. Klicken Sie im Multipoint-Manager auf die Registerkarte **Start**, und klicken Sie dann auf **zum Konsolenmodus wechseln**.
3. Um einen Gerätetreiber zu installieren, doppelklicken Sie auf die Treiberdatei, und befolgen Sie die Anweisungen zum Installieren des Treibers.
4. Wiederholen Sie den vorherigen Schritt, um alle erforderlichen Treiber zu installieren.

**NOTE**

Wenn für eine Installation ein Computer Neustart erforderlich ist, müssen Sie wieder in den Konsolenmodus wechseln, bevor Sie den nächsten Treiber installieren. Der Multipoint-Server wird immer im Stations Modus gestartet. Wechseln Sie in den Konsolenmodus, und klicken Sie im Multipoint-Manager auf die Registerkarte **Home** , und klicken Sie auf **zum Konsolenmodus wechseln**.

# Festlegen des Datums, der Uhrzeit und Zeitzone

09.04.2020 • 2 minutes to read • [Edit Online](#)

Nachdem Sie die Installation von Gerätetreibern abgeschlossen haben, legen Sie das Datum, die Uhrzeit und die Zeitzone auf dem Multipoint-Server fest.

1. Öffnen Sie die **Systemsteuerung** über den **Start** Bildschirm des Multipoint-Servers.
2. Klicken Sie unter **Uhr, Sprache und Region** auf **Uhrzeit und Datum festlegen**.
3. Überprüfen Sie auf der Registerkarte **Datum und Uhrzeit** das Datum und die Uhrzeit. Wenn Sie nicht korrekt sind, klicken Sie auf **Datum und Uhrzeit ändern**, aktualisieren Sie das Datum und die Uhrzeit, und klicken Sie dann auf **OK**.
4. Überprüfen Sie unter **Zeitzonen** die Zeitzone. Wenn dies nicht korrekt ist, klicken Sie auf **Zeitzone ändern**, wählen Sie die richtige Zeitzone aus, und klicken Sie dann auf **OK**.
5. Klicken Sie erneut auf **OK**, um die Einstellungen zu speichern und das Dialogfeld zu schließen.

# Hinzufügen des Multipoint Services-Computers zu einer Domäne (optional)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie über eine Active Directory Domäne auf den Multipoint Services-Computer zugreifen werden, besteht der nächste Schritt darin, den Computer der Domäne hinzuzufügen.

## IMPORTANT

Sie müssen die Zeitzone überprüfen, bevor Sie den Computer einer Domäne hinzufügen. Anweisungen finden Sie unter [Festlegen von Datum, Uhrzeit und Zeitzone](#).

1. Öffnen Sie auf der Startseite die Systemsteuerung. Klicken Sie auf **System und Sicherheit**, und klicken Sie dann auf **System**.
2. Klicken Sie unter **Einstellungen für Computernamen, Domäne und Arbeitsgruppe** auf **Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Computer Name** auf **ändern**.
4. Wählen Sie im Dialogfeld **Computer Name/Domänen Änderungen** die Option **Domäne aus**, geben Sie den Namen der Domäne ein, und klicken Sie dann auf **OK**. Führen Sie dann die Schritte im Assistenten aus, um den Vorgang abzuschließen.
5. Melden Sie sich nach dem Neustart des Computers als Administrator an, und warten Sie, bis der Multipoint-Manager geöffnet wird.

## IMPORTANT

Um sicherzustellen, dass die Bereitstellung der Multipoint Services-Domäne ordnungsgemäß funktioniert, müssen Sie einige Gruppenrichtlinien konfigurieren und die Registrierung aktualisieren. Weitere Informationen finden Sie unter [Konfigurieren von Gruppenrichtlinien für eine Domänen Bereitstellung](#).

# Installieren von Updates

09.04.2020 • 2 minutes to read • [Edit Online](#)

Es wird empfohlen, dass Sie Updates installieren, falls verfügbar. Zum Installieren von Updates ist eine Internet Verbindung erforderlich.

1. Öffnen Sie auf der Startseite die Systemsteuerung.
2. Geben Sie in der Systemsteuerung **Updates** ein, und klicken Sie dann auf **nach Updates suchen**.
3. Wenn die Windows Update-Website alle Updates auflistet, die auf Ihrem Computer erforderlich sind, installieren Sie die Updates.

# Anfügen zusätzlicher Stationen an Multipoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

In ihrer Multipoint Services-Umgebung verwenden die Benutzer Stationen, um eine Verbindung mit Multipoint Services herzustellen und ihre Arbeit zu erledigen. Die Stationen sind die Benutzer Endpunkte zum Herstellen einer Verbindung mit dem Computer, auf dem Multipoint Services ausgeführt wird.

Multipoint Services unterstützt drei Arten von Stationen:

- Direkt mit Videos verbundene Stationen
- USB-Verbindungen mit Clientverbindungen (und USB-über-Ethernet-Verbindungen mit einem Client verbundene Stationen)
- Verbundene RDP-over-LAN-Stationen

Die Klassifizierungen basieren auf der Hardware der Station und der Art der verwendeten Verbindung. Sie können Verbindungstypen für Ihre Stationen kombinieren und abgleichen. Die einzige Voraussetzung ist, dass es sich bei der primären Station (die Sie zuvor installiert haben) um eine Station mit direkt Videoverbindung handeln muss. Weitere Informationen zu Station-Setups finden Sie unter [Multipoint-Stationen](#).

Anweisungen zum Einrichten der einzelnen Stations Stationen finden Sie in den folgenden Abschnitten:

- [Einrichten einer Station mit direkter Videoverbindung](#)
- [Einrichten einer verbundenen USB-Station ohne Clients](#)
- [Einrichten einer mittels RDP über LAN verbundenen Station](#)

Einen ausführlichen Vergleich der Stations Typen finden Sie unter [Stations Typvergleich](#).

## NOTE

- In den Vorgehensweisen zum Anfügen von Stationen wird nicht beschrieben, wie Sie zwischen Hubs oder downstreamhubs einrichten. Informationen dazu, wo Sie diese Hubs installieren, finden Sie unter [Multipoint-Stationen](#).
- In einigen Fällen müssen Sie möglicherweise Station Virtual Desktops erstellen, die auf virtuellen Computern ausgeführt werden. Beispielsweise verwenden Sie Anwendungen, die nicht auf Windows Server oder Anwendungen installiert werden können, auf denen nicht mehrere Instanzen auf demselben Host Computer ausgeführt werden. Weitere Informationen finden Sie unter [Erstellen von virtuellen Windows 10 Enterprise-Desktops für Stationen](#).

## TIP

Es ist hilfreich, die Stationen in der Reihenfolge ihrer physischen Standorte zu erstellen, damit Sie sequenziell in Multipoint Server identifiziert werden. Wenn Sie den Namen einer Station später ändern möchten, können Sie dies in Multipoint Manager tun. Weitere Informationen finden Sie unter Neuzuordnen aller Stationen in Hilfe und Support für Multipoint-Server.

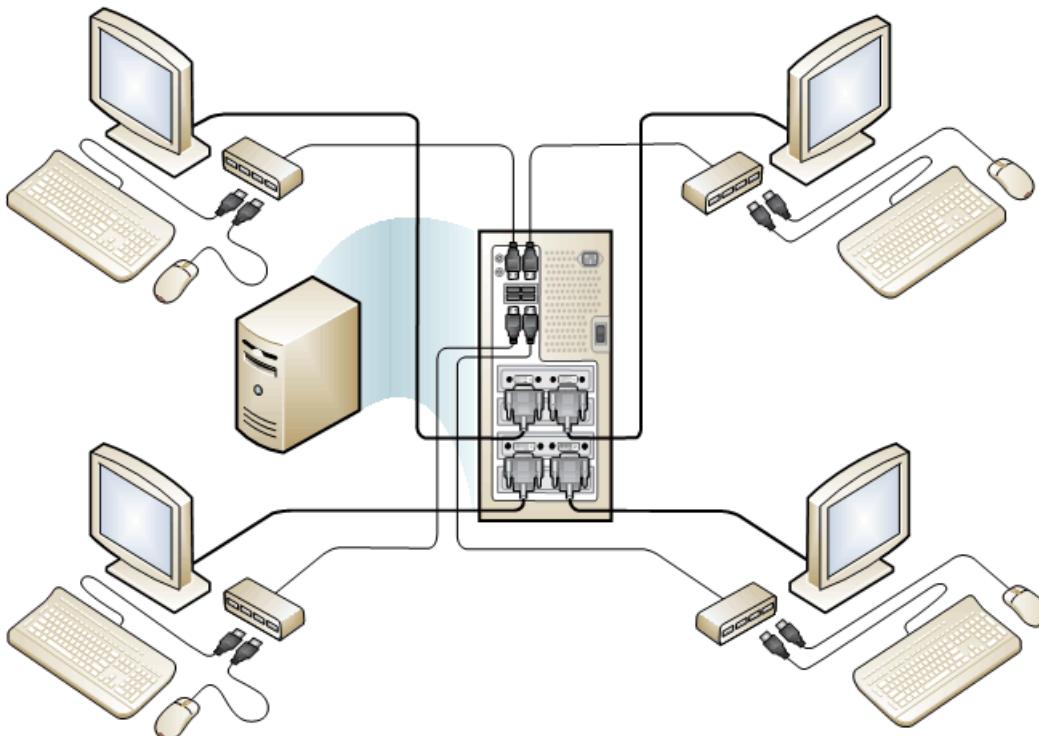
# Einrichten einer Station mit direkt Videoverbindung in Multipoint Services

09.04.2020 • 3 minutes to read • [Edit Online](#)

Auf einer direkt mit dem Video verbundenen Station ist der Monitor direkt mit einem Videoport auf dem Multipoint Server-Computer verbunden. Eine Tastatur und eine Maus werden dann mit einem USB-Hub verbunden und dem Monitor zugeordnet.

Die folgende Abbildung zeigt eine Multipoint-Serverumgebung mit einem einzelnen Multipoint-Server Computer und vier direkt mit einem Video verbundenen Stationen. Weitere Informationen finden Sie unter [Multipoint-Server Stationen](#).

**Multipoint Services-System mit vier direkten Video Verbindungen**

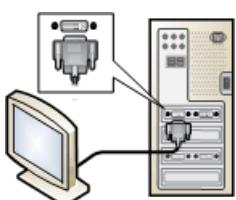


## NOTE

Sie müssen eine lateinische Tastatur (z. B. eine Englisch- oder spanischsprachige Tastatur) verwenden, um eine Station mit einem direkt Video zu konfigurieren.

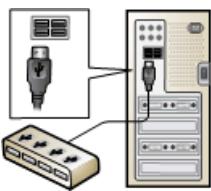
## So richten Sie eine direkte Station mit Videoverbindung ein

1. Verbinden Sie das Monitorkabel mit dem videoanzeigeport auf dem Computer, wie unten gezeigt.



2. Stecken Sie das Stromkabel des Videomonitors in eine Steckdose.

3. Verbinden Sie einen USB-Hub wie unten dargestellt mit einem geöffneten USB-Anschluss auf dem Computer.



4. Verbinden Sie eine Tastatur und eine Maus mit dem USB-stationshub.



5. Verbinden Sie alle zusätzlichen Peripheriegeräte, z. B. Kopfhörer, mit dem USB-Hub.

6. Wenn Sie einen extern betriebenen Hub verwenden, verbinden Sie das Netzkabel des Hubs mit einer Stromversorgung.

**IMPORTANT**

Wir empfehlen dringend die Verwendung eines gestützten Hubs. Ein erratisches Systemverhalten kann sich aus unter aktuellen Bedingungen ergeben.

Benutzer dürfen keine Maus und Tastatur direkt an die USB-Anschlüsse des Computers anfügen. Dadurch wird wahrscheinlich die falsche Zuordnung mehrerer Tastaturen und Mäuse zur gleichen Station oder zu keiner Station ausgelöst.

7. Befolgen Sie die Anweisungen, die auf dem Monitor zum Erstellen der Station angezeigt werden.

Wenn Sie Ihrer Multipoint Services-Umgebung mehr als eine direkte, mit einem Video verbundene Station hinzufügen, kann sich die primäre Station ändern. Sie können mühelos feststellen, welche direkte Videoverbindung Ihre primäre Station ist.

## So ermitteln Sie, welche direkte, mit dem Video verbundene Station die primäre Station ist

1. Schalten Sie alle Monitore ein, die direkt mit den Anzeige Adapters des Computers (Grafikkarten) verbunden sind.
2. Starten (oder Neustarten) des Multipoint Services-Computers, und sehen Sie, welcher Monitor die Startbildschirme anzeigt. Diese Station ist die primäre Station.

**NOTE**

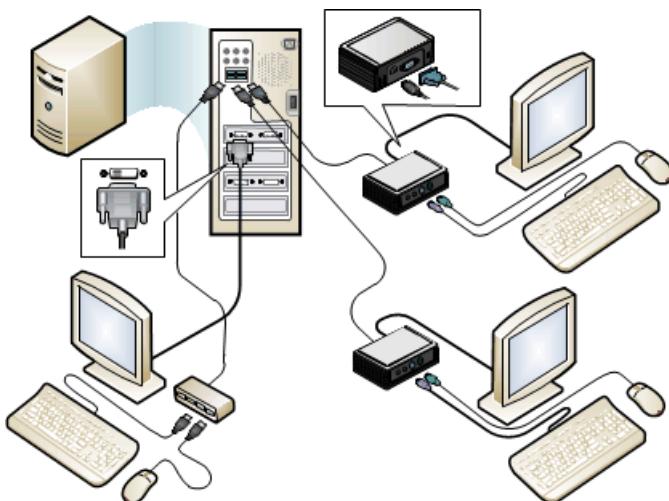
In einigen Fällen werden BIOS-Startinformationen gleichzeitig auf mehreren Monitoren angezeigt. In diesem Fall kann jeder Monitor als "primäre Station" betrachtet werden, um auf das BIOS zuzugreifen.

# Einrichten einer Verbindung zwischen einem USB-Client und einem Client verbundenen Station in Multipoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie Multipoint Services-Stationen mithilfe von USB-Clients erstellen, wird der Monitor für jede Station mit dem Videoport auf dem USB Zero-Client verbunden, wie in der folgenden Abbildung dargestellt. Weitere Informationen zu diesem und anderen Stations Typen finden Sie unter [Multipoint-Stationen](#).

**Multipoint Services-System mit einer direkt mit einem Video verbundenen Station und zwei mit zwei USB-Verbindungen verbundenen Stationen**



## IMPORTANT

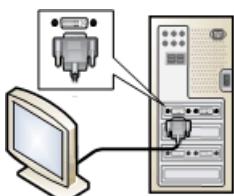
Stellen Sie sicher, dass Sie die neuesten Treiber für die Videokarten und den USB-Zero-Client installieren, bevor Sie die von einem Client verbundenen USB-Verbindungen einrichten. Veraltete Treiber können verhindern, dass die Multipoint Services-Konfiguration erfolgreich abgeschlossen wird. Anweisungen hierzu finden Sie unter [aktualisieren und Installieren von Gerätetreibern bei Bedarf](#).

## IMPORTANT

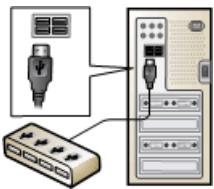
Wenn Sie einen USB-over-Ethernet-Client verwenden, befolgen Sie die Anweisungen Ihres Anbieters, anstatt dieses Verfahrens zu verwenden, um die Ethernet-Verbindung zum Einrichten des Geräts im Netzwerk zu verwenden.

## So richten Sie eine Verbindung mit USB-Client Verbindung ein

1. Verbinden Sie das Videomonitor Kabel mit dem Bildschirm "DVI" oder "VGA Videodisplay Port" auf dem USB-Zero-Client, wie in der folgenden Abbildung dargestellt.



2. Verbinden Sie den USB-Null-Client mit einem geöffneten USB-Anschluss auf dem Computer.



3. Verbinden Sie eine Tastatur und eine Maus mit dem USB-Client.



4. Wenn Sie einen extern betriebenen USB-Zero-Client verwenden, verbinden Sie das Netzkabel des USB Zero-Clients mit einer Stromversorgung.

5. Stecken Sie das Stromkabel des Videomonitors in eine Steckdose.

6. Wenn Sie aufgefordert werden, die Geräte der Station zuzuordnen, befolgen Sie die Anweisungen auf dem Monitor, um das Setup abzuschließen. (Im Allgemeinen werden den Stationen von USB-Clients, die mit dem Client verbunden sind, automatisch Stationen zugeordnet, wenn Sie sie dem Server hinzufügen.)

# Einrichten einer verbundenen RDP-over-LAN-Station in Multipoint Services

09.04.2020 • 3 minutes to read • [Edit Online](#)

Eine RDP-over-LAN-Station ist ein Thin Client, herkömmlicher Desktop oder Laptop Computer, der mithilfe des Remotedesktopprotokoll (RDP) eine Verbindung mit Multipoint Services in einem LAN (Local Area Network) herstellt. Weitere Informationen zu diesem und anderen Stations Typen finden Sie unter [Multipoint-Stationen](#).

## So richten Sie eine Multipoint-Station mit einem Computer oder einem Thin Client auf einem LAN ein

1. Schalten Sie den Computer ein, auf dem Multipoint Services ausgeführt wird.
2. Stellen Sie sicher, dass der Multipoint-Server Computer von einem Switch, einem Router oder einem anderen Netzwerkgerät mit dem LAN verbunden ist und über eine passende IP-Adresse verfügt. (Eine IP-Adresse, die mit 169,254 beginnt (eine APIPA-Adresse), weist möglicherweise darauf hin, dass ein Problem mit der LAN-Verbindung vorliegt oder der DHCP-Server nicht erreicht werden kann oder nicht ordnungsgemäß funktioniert.)
3. Verbinden Sie den Client Computer oder den Thin Client mit dem LAN.
4. Schalten Sie den Client Computer oder den Thin Client ein.
5. Starten Sie auf dem Client Computer oder Thin Client Remotedesktopverbindung oder eine entsprechende Anwendung, und geben Sie den Namen oder die IP-Adresse des Computers ein, auf dem Multipoint Services ausgeführt wird.

## Einrichten eines Windows 10-Geräts für die Remote Verwaltung mithilfe von Connector-Diensten

Alle PCs oder Laptops, auf denen Windows 10 ausgeführt wird, können Remote verwaltet werden:

- die Connector-Dienste wurden aktiviert.
- der Computer wurde den verwalteten Computern auf dem Multipoint-Server hinzugefügt.

Führen Sie auf dem PC mit Windows 10 die folgenden Schritte aus, um den Multipoint-Connector zu aktivieren:

1. Geben Sie im Suchfeld "Windows-Funktionen ein-oder ausschalten" ein, und wählen Sie das richtige Suchergebnis aus.
2. Aktivieren Sie in der Liste der Funktionen den **Multipoint-Connector**. Dadurch werden Multipoint-Connector-Dienste aktiviert, die für die Verwaltung des Geräts erforderlich sind.

Auf dem Multipoint-Server:

1. Öffnen Sie Multipoint-Manager, und wählen Sie entweder **persönliche Computer hinzufügen oder entfernen** oder **Multipoint Services hinzufügen oder entfernen**.
2. Wählen Sie die Remote Computer aus, die Sie verwalten möchten, und klicken Sie auf **OK**. Sie werden auf den Remote Computern zur Eingabe von Administrator Anmelde Informationen aufgefordert. Nachdem dies geschehen ist, werden die Remote Computer auf der Registerkarte "Start" von Multipoint Manager angezeigt.

Wenn der Dashboard-Manager erfolgreich eingerichtet wurde, kann er Benutzer überwachen, die auf dem verwalteten Gerät arbeiten.

**IMPORTANT**

Beim Überwachen verwalteter Windows 10-Geräte administrative können Benutzer nur dann überwacht werden, wenn die Servereinstellungen entsprechend geändert wurden. Siehe [Bearbeiten von Server Einstellungen](#)

# Verwalten der Clientzugriffslizenzen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Jede Station, die eine Verbindung mit einem Multipoint Services-System herstellt, einschließlich des Computers, auf dem Multipoint Services ausgeführt wird und als Station verwendet wird, muss über eine gültige benutzerspezifische Remotedesktop *Client Zugriffslicenz (CAL)* verfügen.

Wenn Sie virtuelle Station-Desktops anstelle physischer Stationen verwenden, müssen Sie für jeden virtuellen Computer der Station eine Client Zugriffslicenz (CAL) installieren.

1. Erwerben Sie eine Client Lizenz für jede Station, die mit Ihrem Multipoint Services-Computer oder-Server verbunden ist. Weitere Informationen zum Erwerb von CALs finden Sie in der Dokumentation zur Remotedesktop Lizenzierung.
2. Öffnen Sie auf dem **Start** Bildschirm den **Multipoint-Manager**.
3. Klicken Sie auf die Registerkarte **Start**, und klicken Sie dann auf **Client Zugriffs Lizenzen hinzufügen**. Dadurch wird das Verwaltungs Tool für die CAL-Lizenzierung geöffnet.

## Manuelles Festlegen des Lizenzierungs Modus

Wenn diese Einstellung nicht ordnungsgemäß konfiguriert ist, wird bei der Einrichtung von Multipoint Services eine Benachrichtigung über den Ablauf der Toleranz Periode angezeigt. Führen Sie diese Schritte aus, um den Lizenzierungs Modus festzulegen:

1. Starten Sie **Editor für lokale Gruppenrichtlinien** (gpeer dit.msc).
2. Navigieren Sie im linken Bereich zu " **lokaler Computer Richtlinien-> Computer Konfiguration-> Administrative Vorlagen-> Windows-Komponenten-> Remotedesktopdienste> Remotedesktop-Sitzungshost >-Lizenzierung**".
3. Klicken Sie im rechten Bereich mit der rechten Maustaste auf **die angegebenen Remotedesktop Lizenzserver verwenden**, und wählen Sie dann **Bearbeiten** aus:
  - Wählen Sie im Dialogfeld Gruppenrichtlinien-Editor die Option **aktiviert** aus.
  - Geben Sie im Feld **zu verwendende Lizenzserver** den Namen des lokalen Computers ein.
  - **OK** auswählen
4. Klicken Sie im rechten Bereich mit der rechten Maustaste auf **Remotedesktop Lizenzierungs Modus festlegen**, und wählen Sie **Bearbeiten** aus.
  - Wählen Sie im Dialogfeld Gruppenrichtlinien-Editor die Option **aktiviert** aus.
  - Legen Sie den **Lizenzierungs Modus** auf pro Gerät/pro Benutzer fest.
  - **OK** auswählen

## Weitere Informationen

[Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)

# Installieren von Software auf Ihrem Multipoint Services-System

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie als Administrator angemeldet sind, können Sie neue Programme entweder im Konsolenmodus oder, von einer Station im Stations Modus installieren. Es wird jedoch empfohlen, Programme im Konsolenmodus zu installieren.

Sie können auf dem Computer, auf dem Multipoint Server ausgeführt wird, neue Software installieren, damit alle Benutzer die Software ausführen können, oder Sie können die Software abhängig von den Installations-und Lizenzierungsoptionen der Software verwenden.

1. Melden Sie sich beim Multipoint Services-Computer als Administrator an.
2. Öffnen Sie den Multipoint-Manager.
3. Klicken Sie auf die Registerkarte **Start**, und klicken Sie dann **auf zum Konsolenmodus wechseln**.
4. Melden Sie sich als Administrator an, und installieren Sie Ihre Anwendungen.
5. Nachdem Sie die Installation von Anwendungen abgeschlossen haben, schalten Sie den Computer wieder in den Stations Modus um. Klicken Sie hierzu auf der Registerkarte **Startseite auf in den Stations Modus wechseln**.

# Optionale Konfigurationsaufgaben für eine MultiPoint Services-Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

In den Themen in diesem Abschnitt wird erläutert, wie optionale Konfigurationsaufgaben auf Ihrem Multipoint Services-System ausgeführt werden.

[Einrichten einer Station mit geteiltem Bildschirm](#)

[Hinzufügen von Druckern](#)

[Erstellen virtueller Windows 10 Enterprise-Desktops für Stationen](#)

# Einrichten einer Station mit geteiltem Bildschirm

09.04.2020 • 5 minutes to read • [Edit Online](#)

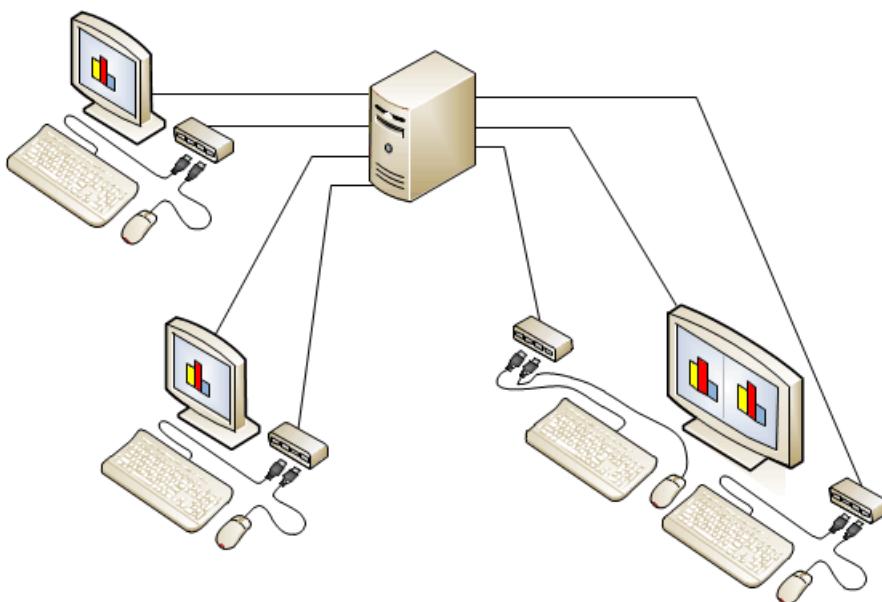
Sie können eine Split-Screen-Station einrichten, sodass zwei Benutzer gleichzeitig das System verwenden können.

Jeder Monitor mit einer Auflösung von mindestens 1200 x720, wenn er mit einer Station verbunden ist, die das Split-Screen-Feature unterstützt, kann in zwei Stationen aufgeteilt werden. Nachdem eine Station aufgeteilt wurde, wechselt der Desktop, der vom Monitor angezeigt wurde, in die linke Hälfte des Bildschirms, und in der rechten Hälfte des Bildschirms wird eine neue Station angezeigt. Um die Erstellung der neuen Station abzuschließen, müssen Sie der Station eine Tastatur, eine Maus und einen USB-Hub zuordnen. Nach dem Teilen einer Station kann sich ein Benutzer auf der linken Station anmelden, während sich ein anderer Benutzer auf der rechten Station anmeldet.

Geteilte Bildschirm Stationen haben mehrere Vorteile:

- Sie können Kosten und Speicherplatz reduzieren, indem Sie mehr Benutzer in einem Multipoint Services-System berücksichtigen.
- Zwei Benutzer können nebeneinander in einem Projekt zusammenarbeiten.
- Ein Multipoint-Dashboardbenutzer kann eine Prozedur auf einer Station veranschaulichen, während ein Student auf der anderen Station dafolgt.

Die folgende Abbildung zeigt ein Multipoint Services-System mit einer unterteilten Bildschirm Station (auf der rechten Seite).



## Anforderungen für eine geteilte Bildschirm Station

Zum Erstellen einer Split-Screen-Station müssen der Monitor und die Station die folgenden Anforderungen erfüllen:

- Der Monitor muss eine Auflösung von 1200 x720 oder höher aufweisen.
- Wenn Sie einen USB-over-Ethernet-Client verwenden, wenden Sie sich an den Hardwarehersteller, um herauszufinden, ob unterstützte Bildschirm Stationen unterstützt werden. Viele USB-over-Ethernet-Client Geräte verfügen über Einschränkungen, die Ihre Konfiguration als getrennte Bildschirm Stationen verhindern.

# Einrichten einer Split-Screen-Station

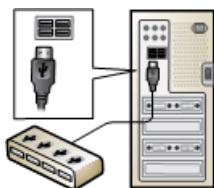
Verwenden Sie die folgenden Verfahren, um einen zweiten Hub für eine Split-Screen-Station hinzuzufügen und die Station dann in Multipoint Services aufzuteilen. Das abschließende Verfahren erläutert, wie Sie eine Split-Screen-Station an eine einzelne Station zurückgeben.

## NOTE

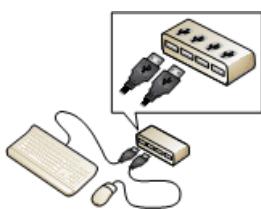
Wenn Sie eine Station teilen, wird die aktive Sitzung auf der Station angehalten. Der Benutzer muss sich erneut bei der Station anmelden, um die Arbeit nach dem aufteilen wieder aufzunehmen.

**So fügen Sie einen zweiten Hub mit Tastatur und Maus hinzu:**

1. Verbinden Sie einen USB-Hub mit einem geöffneten USB-Anschluss auf dem Computer, wie in der folgenden Abbildung dargestellt.



2. Verbinden Sie eine Tastatur und eine Maus mit dem USB-Hub.



3. Verbinden Sie alle zusätzlichen Peripheriegeräte, z. B. Kopfhörer, mit dem USB-Hub.
4. Wenn Sie einen extern betriebenen Hub verwenden, verbinden Sie das Netzkabel des Hubs mit einer Stromversorgung.

**So teilen Sie eine Station:**

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Stationen**.
2. Klicken Sie unter **Station** auf den Namen der Station, die Sie aufteilen möchten.
3. Klicken Sie unter **Aufgaben des ausgewählten Elements** auf **Station aufteilen**.

Der ursprüngliche Bildschirm wird in die linke Hälfte des Monitors verschoben, und auf der rechten Hälfte desselben Monitors wird der Bildschirm einer neuen Station erstellt.

4. Erstellen Sie die neue Station, indem Sie den angegebenen Buchstaben auf der neu hinzugefügten Tastatur entsprechend der Angabe anzeigen, wenn auf der rechten Hälfte des Monitors der Bildschirm zum **Erstellen einer Multipoint-Server Station** angezeigt wird.

Nachdem eine Station aufgeteilt wurde, kann sich ein Benutzer an der linken Station anmelden, während sich ein anderer Benutzer an der rechten Station anmeldet.

**So kehren Sie eine geteilte Station an eine einzelne Station zurück:**

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Stationen**.
2. Klicken Sie unter **Station** auf den Namen der Station, die Sie aufteilen möchten.

3. Klicken Sie unter **Aufgaben des ausgewählten Elements** auf die Option zum **Aufteilen der Station**.

# Hinzufügen von Druckern

09.04.2020 • 2 minutes to read • [Edit Online](#)

Verwenden Sie die Verfahren in diesem Thema, um einen lokalen Drucker für alle Benutzer in einem Multipoint Services-System verfügbar zu machen.

## NOTE

Wenn Sie Domänen Konten mit Multipoint Services verwenden, können Benutzer beliebige Netzwerkdrucker von ihren Stationen verwenden.

1. Verbinden Sie den Drucker mit dem Multipoint-Server.
2. Konfigurieren Sie den Drucker als freigegebenen Drucker:
  - a. Melden Sie sich beim Multipoint-Server Computer als Administrator an.
  - b. Öffnen Sie auf der Startseite die Systemsteuerung.
  - c. Klicken Sie in der Systemsteuerung auf **Hardware**, und klicken Sie dann auf **Geräte und Drucker**.
  - d. Klicken Sie unter **Drucker und Fax** mit der rechten Maustaste auf den Drucker, und klicken Sie dann auf **Druckereigenschaften**.
  - e. Klicken Sie auf die Registerkarte **Freigabe**.
  - f. Klicken Sie auf **diesen Drucker freigeben**, geben Sie einen Freigabe Namen für den Drucker an, und klicken Sie dann auf **OK**.

Benutzer, die sich bei einer Station angemeldet haben, die mit dem Multipoint Services-Computer verbunden ist, können den Drucker sehen und verwenden.

# Erstellen virtueller Windows 10 Enterprise-Desktops für Stationen

09.04.2020 • 15 minutes to read • [Edit Online](#)

Diese optionale Konfiguration in Multipoint Services ist hauptsächlich für Situationen vorgesehen, in denen eine erforderliche Anwendung für jeden Benutzer eine eigene Instanz eines Client Betriebssystems erfordert. Zu den Beispielen zählen Anwendungen, die nicht auf Windows Server installiert werden können, und Anwendungen, die nicht mehrere Instanzen auf demselben Host Computer ausführen.

## NOTE

Diese virtuellen Desktops, auch als VDI bezeichnet, sind viel mehr ressourcenintensiver als die standardmäßigen Multipoint Services-Desktop Sitzungen. Daher empfiehlt es sich, nach Möglichkeit standardmäßige Multipoint Services-Sitzungen zu verwenden.

## Erforderliche Komponenten

Stellen Sie sicher, dass Ihr Multipoint Services-System die folgenden Anforderungen erfüllt, um die Erstellung virtueller Desktops auf der Station vorzubereiten:

HARDWARE	VORAUSSETZUNGEN
CPU (Multimedia)	1 Kern oder Thread pro virtuellem Computer
Solid State Drive (SSD)	Kapazitäts > = 20 GB pro Station + 40 GB für das Multipoint Services-Host Betriebssystem Zufälliger Lese-/Schreib-IOPS-> = 3K pro Station
RAM	2 GB pro Station + 2 GB für das Windows-MultiPoint Server-Host Betriebssystem
Grafik	DX11
BIOS	BIOS-CPU-Einstellung, die für die Aktivierung der Virtualisierung konfiguriert ist – Second Level Address Translation (slat)

- **Stationen** : richten Sie die Stationen für Ihr Multipoint Services-System ein. Weitere Informationen finden Sie unter [Anfügen zusätzlicher Stationen an Multipoint Services](#).
- **Domäne** : der Windows-MultiPoint-Server Computer wurde der Domäne hinzugefügt, und ein Domänen Benutzer wurde der lokalen Administrator Gruppe auf dem Multipoint Services-Host Betriebssystem hinzugefügt.

# Verfahren

Verwenden Sie die folgenden Verfahren für Folgendes:

- [Erstellen einer Vorlage für virtuelle Desktops](#)
- [Erstellen virtueller Desktops aus der Vorlage](#)
- [Kopieren einer vorhandenen Vorlage für virtuelle Desktops](#)

## Erstellen einer Vorlage für virtuelle Desktops

Bevor Sie eine Vorlage für Ihre virtuellen Desktops erstellen können, müssen Sie die Funktion für virtuelle Desktops in Multipoint Server aktivieren.

So aktivieren Sie die Funktion für virtuelle Desktops

1. Melden Sie sich beim Multipoint Server-Host Betriebssystem mit einem lokalen Administrator Konto oder in einer Domäne mit einem Domänen Konto an, das Mitglied der lokalen Administratoren Gruppe ist.
2. Öffnen Sie auf dem **Start** Bildschirm den Multipoint-Manager.
3. Klicken Sie auf die Registerkarte **virtuelle Desktops**, klicken Sie auf **virtuelle Desktops aktivieren** und dann auf **OK**, und warten Sie, bis das System neu gestartet wird.

Der nächste Schritt ist das Erstellen einer Vorlage für virtuelle Desktops. Sie erstellen eine virtuelle Festplatten Datei (VHD), die Sie als Vorlage zum Erstellen von virtuellen Station-Desktops für Multipoint Manager verwenden können. Sie können entweder die physischen Installationsmedien für Windows oder verwenden ISO-Abbild Datei als Quelle für die Vorlage. Sie können auch einen verwenden. VHD der Windows-Installation. Beachten Sie, dass Sie zum Verwenden eines physischen Installations Datenträgers den-CD einfügen müssen, bevor Sie den Assistenten starten.

So erstellen Sie eine Vorlage für virtuelle Desktops

1. Melden Sie sich beim Multipoint Server-Host Betriebssystem mit einem lokalen Administrator Konto oder in der Domäne als Domänen Konto an, das Mitglied der lokalen Administratoren Gruppe ist.
2. Öffnen Sie auf dem **Start** Bildschirm den Multipoint-Manager.
3. Klicken Sie auf die Registerkarte **virtuelle Desktops**.
4. Kopieren Sie eine Windows 10 Enterprise. ISO-Datei auf das lokale SSD.
5. Klicken Sie auf der Registerkarte **virtuelle Desktops** auf **Vorlage für virtuellen Desktop erstellen**.
6. Geben Sie unter **Präfix** ein Präfix ein, das zum Identifizieren der Vorlage und der mit der Vorlage erstellten virtuellen Desktops verwendet werden soll. Das Standard Präfix ist der Name des Host Computers.

Das Präfix wird als Name der Vorlage und der virtuellen Desktopstationen verwendet. Die Vorlage wird <*Präfix*>-t. Die virtuellen Desktop Stationen werden <*Präfix*>-n benannt, wobei n der Stations Bezeichner ist.

7. Geben Sie einen Benutzernamen und ein Kennwort ein, die für das lokale Administrator Konto der Vorlage verwendet werden sollen. Geben Sie in einer Domäne die Anmelde Informationen für ein Domänen Konto ein, das der lokalen Administrator Gruppe hinzugefügt wird. Dieses Konto kann verwendet werden, um sich bei der Vorlage und allen virtuellen Desktop Stationen anzumelden, die mithilfe der Vorlage erstellt wurden.
8. Klicken Sie auf **OK**, und warten Sie, bis die Vorlagen Erstellung beendet ist.
9. Die neue Vorlage wird auf der Registerkarte **virtuelle Desktops** aufgeführt. Die Vorlage wird ausgeschaltet.

Der nächste Schritt besteht darin, die Vorlage mit der Software und den Einstellungen zu konfigurieren, die Sie auf den virtuellen Desktops ausführen möchten. Dies müssen Sie tun, bevor Sie virtuelle Desktops aus der Vorlage erstellen.

So passen Sie eine Vorlage für virtuelle Desktops an

1. Melden Sie sich beim Multipoint Server-Host Betriebssystem mit einem lokalen Administrator Konto oder in einer Domäne mit einem Domänen Konto in der lokalen Gruppe Administratoren an.
2. Öffnen Sie auf dem **Start** Bildschirm den Multipoint-Manager.
3. Klicken Sie auf die Registerkarte **virtuelle Desktops**.
4. Wählen Sie die Vorlage aus, die Sie anpassen möchten, klicken Sie auf **Vorlage anpassen**, und klicken Sie dann auf **OK**.

**NOTE**

Es sind nur die Vorlagen verfügbar, die nicht zum Erstellen virtueller Desktop Stationen verwendet wurden. Wenn Sie eine Vorlage aktualisieren möchten, die bereits verwendet wird, müssen Sie eine Kopie der Vorlage erstellen, indem Sie den Task "Vorlage importieren" verwenden, der später in [Kopieren einer vorhandenen Vorlage für virtuelle Desktops](#) beschrieben wird.

Die Vorlage wird in einem Hyper-V- **VM-Verbindungs** Fenster geöffnet, und die automatische Anmeldung erfolgt über das integrierte Administrator Konto.

5. An diesem Punkt können Sie Anwendungen und Software Updates installieren, Einstellungen ändern und das Administrator Profil aktualisieren. Alle Änderungen, die am integrierten Administrator Profil der Vorlage vorgenommen werden, werden in die virtuellen Desktop Stationen, die mithilfe der Vorlage erstellt werden, in das Standardbenutzer Profil kopiert.

Wenn Sie Ihre Stationen über eine Domäne verbinden, empfiehlt es sich, ein lokales Benutzerkonto zu erstellen und es der lokalen Administrator Gruppe während der Anpassung hinzuzufügen.

**NOTE**

Wenn das System neu gestartet wird, während eine Vorlage angepasst wird, schlägt die automatische Anmeldung mit dem integrierten Administrator Konto möglicherweise fehl, nachdem das System neu gestartet wurde. Um dieses Problem zu umgehen, melden Sie sich manuell mithilfe des lokalen Administrator Kontos an, das Sie erstellt haben, ändern Sie das Kennwort für das integrierte Administrator Konto, melden Sie sich ab, und melden Sie sich dann mit dem integrierten Administrator Konto und dem neuen Kennwort wieder an. (Sie müssen das Profil löschen, das erstellt wurde, als Sie sich mit dem lokalen Administrator Konto angemeldet haben.)

6. Nachdem Sie die Konfiguration des Systems abgeschlossen haben, doppelklicken Sie auf dem Desktop des Administrators auf die Verknüpfung **completemanagement**, um syunp auszuführen, und fahren Sie dann die Vorlage herunter. Während der Anpassung entfernt das sybandp-Tool alle eindeutigen Systeminformationen, um die Windows-Installation für das Abbild vorzubereiten.

### **Erstellen von Desktops virtueller Computer aus der Vorlage**

Wenn die Vorlage für virtuelle Desktops wie Ihre Desktops konfiguriert ist, können Sie mit dem Erstellen virtueller Desktops beginnen. Ein virtueller Desktop wird für jede Station erstellt, die an den Multipoint-Server Computer angeschlossen ist. Wenn sich ein Benutzer das nächste Mal an einer Station anmeldet, wird der virtuelle Desktop anstelle des Sitzungs basierten Desktops angezeigt, der zuvor angezeigt wurde.

**NOTE**

Diese Prozedur funktioniert nur, wenn sich der Multipoint-Server im *Stations Modus* befindet. Wenn sich das System im *Konsolenmodus* befindet, können Sie von Multipoint Manager in den Stations Modus wechseln. Wenn Sie die Standardeinstellungen für Multipoint verwenden, können Sie den Stations Modus auch starten, indem Sie den Computer neu starten. Standardmäßig wird der Multipoint-Server Computer immer im Stations Modus gestartet.

#### So erstellen Sie virtuelle Desktops für Ihre Stationen

1. Melden Sie sich über eine Remote Station (z. b. über einen Windows-Computer mithilfe Remotedesktopverbindung) beim Windows-MultiPoint-Server an, indem Sie ein lokales Administrator Konto oder in einer Domäne ein Domänen Konto in der lokalen Administratoren Gruppe verwenden.

#### NOTE

Alternativ können Sie sich mit einer lokalen Station beim Server anmelden. Wenn Sie jedoch einen virtuellen Desktop für die Station erstellen, müssen Sie sich von der Station abmelden, die Sie zum Erstellen des virtuellen Desktops verwendet haben, um die andere Station mit dem neuen virtuellen Desktop zu verbinden.

2. Öffnen Sie auf dem **Start** Bildschirm den Multipoint-Manager.
3. Wechseln Sie in den Stations Modus, wenn sich der Computer im Konsolenmodus befindet:
  - a. Klicken Sie auf der Registerkarte **Startseite** auf **in den Stations Modus wechseln**.
  - b. Wenn der Computer neu gestartet wird, melden Sie sich als Administrator an.
4. Klicken Sie auf die Registerkarte **virtuelle Desktops**.
5. Wählen Sie die Vorlage für virtuelle Desktops aus, die Sie mit den Stationen verwenden möchten, klicken Sie auf **virtuelle Desktop Stationen erstellen**, und klicken Sie dann auf **OK**.

Wenn die Aufgabe abgeschlossen ist, stellt jede lokale Station eine Verbindung mit einem virtuellen Computer her, auf dem ein virtueller Computer ausgeführt wird.

#### NOTE

Wenn ein Benutzerkonto bei einer der lokalen Stationen angemeldet ist, müssen Sie sich bei der Sitzung abmelden, um die Station zum Herstellen einer Verbindung mit einer der neu erstellten virtuellen Computer für die Station zu erhalten.

### Kopieren einer vorhandenen Vorlage für virtuelle Desktops

Verwenden Sie das folgende Verfahren, um eine Kopie einer vorhandenen virtuellen Desktop Vorlage zu erstellen, die Sie anpassen und verwenden können. Dies kann in den folgenden Situationen nützlich sein:

- Kopieren Sie eine Master Vorlage aus einer Netzwerkfreigabe auf einen Multipoint Server-Host Computer, damit virtuelle Desktop Stationen aus der Master Vorlage erstellt werden können.
- Zum Erstellen einer Kopie einer Vorlage, die derzeit verwendet wird, sodass Sie weitere Anpassungen vornehmen können.

#### So importieren Sie eine Vorlage für virtuelle Desktops

1. Melden Sie sich beim Multipoint-Server als Administrator an.
2. Öffnen Sie auf dem **Start** Bildschirm den Multipoint-Manager.
3. Klicken Sie auf die Registerkarte **virtuelle Desktops**.
4. Klicken Sie auf **virtuelle Desktop Vorlage importieren**, und wählen Sie mit **Durchsuchen** die VHD-Datei (Vorlage) aus, die Sie importieren möchten. Wenn Sie eine Vorlage importieren, wird eine Kopie der ursprünglichen VHD-Datei erstellt. Standardmäßig speichert Multipoint Services VHD-Dateien in den C:\Benutzern\öffentlichen\Dokumenten\Hyper-V\virtuellen Festplatten\ Ordners.
5. Geben Sie ein Präfix für die neue Vorlage ein, und klicken Sie dann auf **OK**.
6. Wenn Sie weitere Anpassungen an einer lokalen Vorlage vornehmen, können Sie den Präfix Namen ändern, indem Sie eine Versionsnummer am Ende des Präfixes erhöhen. Oder wenn Sie eine Master Vorlage

importieren, sollten Sie die Version der Master Vorlage am Ende des Standard Präfix namens hinzufügen.

7. Wenn die Aufgabe abgeschlossen ist, können Sie die Vorlage anpassen oder Sie verwenden, um Stationen zu erstellen.

# Vorbereiten Ihres Multipoint Services-Systems für Benutzer

09.04.2020 • 2 minutes to read • [Edit Online](#)

Nachdem Sie Multipoint Services installiert und konfiguriert und zusätzliche Konfigurations-und Hardware Konfigurationen durchgeführt haben, können Sie Benutzern den Zugriff auf das System bereitstellen. Sie müssen Benutzerkonten planen und erstellen. In einigen Umgebungen müssen Sie auch Stationen für die automatische Anmeldung konfigurieren und mehrere Sitzungen für Ihre freigegebenen Benutzerkonten zulassen. Und Sie müssen entscheiden, wie Sie die Dateifreigabe für Ihre Benutzer einrichten möchten. Diese Themen werden in diesem Abschnitt behandelt.

## NOTE

Nachdem Sie Ihre Benutzerkonten erstellt und die anderen Konfigurations Aktualisierungen für die Benutzer Vorbereitung vorgenommen haben, empfiehlt es sich, den Datenträger Schutz zu aktivieren, damit kein Benutzer versehentlich Änderungen an den Systemdateien und-Einstellungen vornehmen kann. Weitere Informationen finden Sie unter [Konfigurieren des Datenträger Schutzes](#).

Bereiten Sie Ihr System anhand der folgenden Informationen vor:

[Planen von Benutzerkonten für Ihre Multipoint Services-Umgebung](#)

[Beispieldaten für die Erstellung von Benutzerkonten](#)

[Erstellen von lokalen Benutzerkonten in Multipoint Services](#)

[Einschränken des Benutzer Zugriffs auf den Server](#)

[Konfigurieren von Stationen für die automatische Anmeldung](#)

[Zulassen mehrerer Sitzungen für ein Konto](#)

[Aktivieren der Dateifreigabe](#)

# Planen von Benutzerkonten für eine MultiPoint Services-Umgebung

09.04.2020 • 10 minutes to read • [Edit Online](#)

Die beste Methode zum Implementieren von Benutzerkonten in Multipoint Services hängt von der Größe und Komplexität Ihrer Bereitstellung ab:

- **Lokale Benutzerkonten** : für eine kleine Bereitstellung mit nur wenigen Computern, auf denen multipoint-Dienste und wenige Benutzer ausgeführt werden, ist es möglicherweise am einfachsten, *lokale Benutzerkonten* zu verwenden, die in Multipoint Services erstellt werden. Sie können für jede Person, die das System verwendet, ein einzelnes Konto erstellen oder ein allgemeines Konto für jede Station erstellen, das jeder zum Anmelden verwenden kann. Multipoint Services-Administratoren erstellen und verwalten lokale Benutzerkonten mithilfe von Multipoint-Manager. Bei den lokalen Konten kann es sich um Administratoren mit eingeschränkten Administratorrechten oder um reguläre Benutzer ohne Zugriff auf den Multipoint Services-Desktop oder den Multipoint-Manager handeln.
- **Domänen Konten** : Wenn in Ihrer Umgebung viele Computer mit Multipoint Services und vielen Benutzern vorhanden sind, ist es wahrscheinlich sinnvoller, eine Active Directory Domain Services (AD DS) Domäne einzurichten und *Domänen Benutzerkonten* zu verwenden, die es Benutzern ermöglichen, von einer beliebigen Station in der Domäne aus auf Ihr eigenes Benutzerprofil und ihre eigenen Einstellungen zuzugreifen. Domänen Benutzerkonten müssen von einem Domänen Administrator auf dem Domänen Controller erstellt werden.

## NOTE

In den folgenden Abschnitten werden Szenarien erörtert, die Sie möglicherweise für lokale Benutzerkonten in Multipoint Services implementieren. Wenn Sie Domänen Benutzerkonten verwenden, finden Sie weitere Informationen im Szenario "mindestens ein Multipoint-Server in einer Domänen Netzwerkumgebung" in [Beispieldaten: Multipoint Services-Benutzerkonten](#).

## Planen von lokalen Benutzerkonten

In den folgenden Abschnitten werden die vor- und Nachteile sowie die Anforderungen für verschiedene Methoden zum Implementieren einzelner oder gemeinsam genutzter lokaler Benutzerkonten in Ihrer Windows-MultiPoint Services-Umgebung berücksichtigt.

### Einzelne lokale Benutzerkonten verwenden

Wenn Sie lokale Benutzerkonten erstellen, haben Sie die Option zwei Ansätze. Weisen Sie jeden Benutzer einem bestimmten Server zu, auf dem Multipoint Services ausgeführt wird, und erstellen Sie ein einzelnes Konto für jeden Benutzer. Oder erstellen Sie lokale Benutzerkonten für alle Benutzer auf jedem Computer, auf dem Multipoint Services ausgeführt wird. Ein wichtiger Vorteil der Implementierung einzelner Benutzerkonten besteht darin, dass jeder Benutzer über seine eigene Windows-Desktop Darstellung verfügt, die private Ordner zum Speichern von Daten umfasst.

Aus Sicht der Systemverwaltung ist es möglicherweise bequemer, Benutzer einem bestimmten Multipoint Services-Computer zuzuweisen. Wenn Sie z. B. über zwei Multipoint-Server mit jeweils fünf Stationen verfügen, können Sie lokale Benutzerkonten erstellen, wie in der folgenden Tabelle veranschaulicht.

Tabelle 1: Zuweisen von lokalen Benutzerkonten zu bestimmten Computern, auf denen Multipoint

## **Services ausgeführt wird**

COMPUTER A	COMPUTER B
UserAccount_01	UserAccount_06
UserAccount_02	UserAccount_07
UserAccount_03	UserAccount_08
UserAccount_04	UserAccount_09
UserAccount_05	UserAccount_10

In diesem Szenario hat jeder Benutzer ein einzelnes Konto auf einem bestimmten Computer. Daher können sich alle Benutzer, die über ein lokales Konto auf Computer a verfügen, bei Ihrem Konto von einer beliebigen Station anmelden, die mit Computer a verknüpft ist. Diese Benutzer können jedoch nicht auf Ihre Konten zugreifen, wenn Sie eine Station verwenden, die Computer B zugeordnet ist, und umgekehrt. Ein Vorteil dieses Ansatzes besteht darin, dass Benutzer immer Ihre Dateien finden und darauf zugreifen können, indem Sie immer eine Verbindung mit dem gleichen Computer herstellen.

Im Gegensatz dazu ist es auch möglich, einzelne Benutzerkonten auf allen Computern zu replizieren, auf denen Multipoint Services ausgeführt wird, wie in der folgenden Tabelle veranschaulicht.

**Tabelle 2: Replizieren von Benutzerkonten auf allen Computern, auf denen Multipoint Services ausgeführt wird**

COMPUTER A	COMPUTER B
UserAccount_01	UserAccount_01
UserAccount_02	UserAccount_02
UserAccount_03	UserAccount_03
UserAccount_04	UserAccount_04
UserAccount_05	UserAccount_05

Ein Vorteil dieses Ansatzes besteht darin, dass Benutzer über ein lokales Benutzerkonto für alle verfügbaren Multipoint Services verfügen. Dieser Vorteil kann jedoch durch die Nachteile aufwiegen. Wenn z. b. der Benutzername und das Kennwort für eine bestimmte Person auf beiden Computern identisch sind, sind die Konten nicht miteinander verknüpft. Wenn sich ein Benutzer am Montag bei seinem Konto auf Computer a anmeldet, speichert eine Datei und meldet sich dann bei seinem Konto auf Computer B am Dienstag an, und er kann nicht auf die Datei zugreifen, die zuvor auf Computer a gespeichert wurde. Darüber hinaus erhöht die Replikation von Benutzerkonten auf mehreren Computern den Verwaltungsaufwand und die Speicheranforderungen.

## **Generische lokale Benutzerkonten verwenden**

Wenn Ihr Multipoint Services-System nicht mit einer Domäne verbunden ist und Sie kein einzelnes Konto für jeden Benutzer erstellen möchten, können Sie für jede Station generische Konten erstellen. Wenn Sie beispielsweise über zwei Computer verfügen, auf denen Multipoint Services ausgeführt wird, und jedem Computer fünf Stationen zugeordnet sind, können Sie Benutzerkonten erstellen, die den in der folgenden Tabelle aufgeführten ähneln.

**Tabelle 3: Erstellen von generischen Benutzerkonten, einem Konto pro Station**

COMPUTER A	COMPUTER B
Computer_A Station_01	Computer_B Station_01
Computer_A Station_02	Computer_B Station_02
Computer_A Station_03	Computer_B Station_03
Computer_A Station_04	Computer_B Station_04
Computer_A Station_05	Computer_B Station_05

In diesem Szenario hat jedes Stationskonto das gleiche Kennwort, und sowohl die Kenn Wörter als auch die Namen der generischen Benutzerkonten sind für alle Benutzer verfügbar. Ein Vorteil dieses Ansatzes besteht darin, dass der Aufwand für die Verwaltung von Benutzerkonten wahrscheinlich weniger als bei der Verwendung einzelner Konten ist, weil es in der Regel weniger Stationen als Benutzer gibt. Außerdem wird der Aufwand, der durch das Replizieren von Benutzerkonten auf jedem Server verursacht wird, beseitigt.

Eine andere Möglichkeit ist das Erstellen von generischen Konten auf jedem Server. Jeder Benutzer meldet sich als dasselbe Konto bei einem Server an. Um dies zuzulassen, müssen Sie mehrere Sitzungen pro Konto aktivieren. Sie können weitere vereinfachen, indem Sie den gleichen Kontonamen und das gleiche Kennwort auf allen Servern verwenden. Dies vereinfacht die Anmeldung für die Benutzer, die nur einen Kontonamen und ein Kennwort kennen müssen, damit eine beliebige Station auf einem beliebigen Server verwendet werden kann. Beachten Sie, dass in diesem Szenario alle Benutzer jede beliebige Änderung sehen können. Wenn eine Datei z. B. auf dem Desktop gespeichert wird, können alle Benutzer die Datei sehen.

#### **IMPORTANT**

Es ist wichtig zu wissen, dass Benutzer, die auf dem Server gespeichert sind (entweder eine pro Server oder eine pro Station), auf dem Server gespeicherte Dateien – auch in eigenen Dokumenten gespeicherte Dateien nicht privat sind. Jeder Benutzer, der sich mit dem Konto anmeldet, hat Zugriff auf diese Dateien. Wenn Sie ein Konto pro Station verwenden und ein Benutzer auf einer Station Dateien in meinen Dokumenten speichert, hat der Benutzer keinen Zugriff auf diese Dateien auf einer anderen Station. Dasselbe Problem tritt auf, wenn Sie sich bei verschiedenen Multipoint Services-Computern anmelden.

Damit Benutzer von einer beliebigen Station aus auf Ihre Dateien zugreifen können, können Sie einen Dateiserver verwenden, eine Dateifreigabe für jedes Benutzerkonto erstellen oder Benutzern gestatten, Ihre persönlichen Dokumente auf einem USB-Speicherstick oder einem anderen privaten Speichergerät zu speichern. Einzelne USB-Speicherstick ermöglichen einzelnen Benutzern das Speichern privater Dokumente, auch wenn Sie ein Benutzerkonto in einem Multipoint Services-Dienst freigeben.

# Beispielszenarien: MultiPoint Services-Benutzerkonten

09.04.2020 • 8 minutes to read • [Edit Online](#)

Was müssen Sie tun, um das Benutzerkonto Szenario zu implementieren, das Sie für Ihre Multipoint Services-Umgebung ausgewählt haben? In den folgenden Tabellen werden die einzelnen Aufgaben beschrieben, die zum Konfigurieren von Benutzerkonten und zum Vorbereiten von Stationen für freigegebene oder einzelne Benutzerkonten auf einem eigenständigen Multipoint-Computer oder auf Netzwerkservern in einer Arbeitsgruppe oder einer Active Directory Domäne durchgeführt werden. Wählen Sie das Szenario aus, das für Ihre Umgebung gilt. Folgen Sie dann den Links in der Tabelle, um die einzelnen erforderlichen Konfigurationsaufgaben abzuschließen.

## NOTE

Wenn Sie noch nicht entschieden haben, wie Sie Ihre Benutzerkonten einrichten, finden Sie unter [Planen von Benutzerkonten für Ihre Multipoint Services-Umgebung](#) Weitere Informationen dazu, wie sich die einzelnen Auswahl auf die Benutzer auswirken.

## Einzelner Multipoint Services-Computer in einer eigenständigen Umgebung (kein Netzwerk)

<p><b>Meine Benutzer müssen sich nicht anmelden.</b> Die Stationen können allen Benutzern zur Verfügung stehen. Sie benötigen keine individuelle Windows-Desktop Darstellung, die private Ordner zum Speichern von Daten oder personalisierten Desktops umfasst.</p>	<ol style="list-style-type: none"><li>1. Erstellen Sie ein einzelnes lokales Benutzerkonto (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>).</li><li>2. <a href="#">zulassen, dass ein Konto über mehrere Sitzungen verfügt</a></li><li>3. <a href="#">Konfigurieren von Stationen für die automatische Anmeldung</a></li></ol>
<p><b>Meine Benutzer können die gleiche Benutzeranmeldung verwenden.</b> Sie benötigen keine individuelle Windows-Desktop Darstellung, die private Ordner zum Speichern von Daten oder personalisierten Desktops umfasst.</p>	<ol style="list-style-type: none"><li>1. Erstellen Sie ein einzelnes lokales Benutzerkonto (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>).</li><li>2. <a href="#">zulassen, dass ein Konto über mehrere Sitzungen verfügt</a></li></ol>
<p><b>Meine Benutzer müssen über eine eigene Windows-Desktop Darstellung verfügen.</b></p>	<p>Erstellen Sie ein lokales Benutzerkonto für jeden Benutzer (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>).</p>

## Mehrere Multipoint Services-Computer in einem Netzwerk, aber ohne Domäne

<p><b>Meine Benutzer müssen sich nicht anmelden.</b> Die Stationen können allen Benutzern zur Verfügung stehen. Sie benötigen keine individuelle Windows-Desktop Darstellung, die private Ordner zum Speichern von Daten oder personalisierten Desktops umfasst.</p>	<ol style="list-style-type: none"><li>1. Erstellen Sie ein einzelnes lokales Benutzerkonto auf jedem Server: (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>.)</li><li>2. <a href="#">zulassen, dass ein Konto über mehrere Sitzungen auf jedem Server verfügt</a></li><li>3. <a href="#">Konfigurieren von Stationen für die automatische Anmeldung auf jedem Server</a></li></ol>
--	---

<p><b>Meine Benutzer können die gleiche Benutzeranmeldung verwenden.</b> Sie benötigen keine individuelle Windows-Desktop Darstellung, die private Ordner zum Speichern von Daten oder personalisierten Desktops umfasst.</p>	<ol style="list-style-type: none"> <li>1. Erstellen Sie ein einzelnes lokales Benutzerkonto auf jedem Server. (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>.)</li> <li>2. <a href="#">gewähren Sie einem Konto mehrere Sitzungen</a> auf jedem Server.</li> </ol>
<p><b>Meine Benutzer müssen über eine eigene Windows-Desktop Darstellung verfügen.</b></p> <ul style="list-style-type: none"> <li>- <b>Option A</b> -meine Benutzer verwenden immer lokale Stationen, die mit demselben Multipoint Services-Computer verbunden sind.</li> <li>- <b>Option B</b> -"meine Benutzer" verwenden lokale Stationen auf mehr als einem Multipoint Services-Computer.</li> <li>- <b>Option C</b> -meine Benutzer werden Remote Clients im LAN verwenden.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>Option a</b> : Erstellen Sie auf jedem Server ein einzelnes lokales Benutzerkonto für die Benutzer dieses Servers. (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>.)</li> <li>- <b>Option B</b> -lokale Benutzerkonten für jeden Benutzer auf jedem Server erstellen. <b>Hinweis:</b> Dies bedeutet, dass jeder Benutzer über ein Profil auf jedem Server verfügt. Anders ausgedrückt: Wenn eine Datei in "eigene Dokumente" gespeichert wird, während Sie bei der Station von Server a angemeldet ist, wird die Datei bei der Anmeldung bei Server B nicht angezeigt. (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>.)</li> <li>- <b>Option C</b> : weisen Sie jeden Benutzer einem bestimmten Multipoint Services-Computer zu. Erstellen Sie lokale Benutzerkonten für die zugewiesenen Benutzer auf jedem Server. (Anweisungen hierzu finden Sie unter <a href="#">Erstellen von lokalen Benutzerkonten</a>.)</li> </ul>

## Mindestens ein Multipoint Services-Computer in einer Domänen Netzwerkumgebung

<p><b>Meine Benutzer müssen sich nicht anmelden.</b> Die Stationen können allen Benutzern zur Verfügung stehen. Sie benötigen keine individuelle Windows-Desktop Darstellung, die private Ordner zum Speichern von Daten oder personalisierten Desktops umfasst.</p>	<ol style="list-style-type: none"> <li>1. Erstellen Sie ein Domänen Konto, um sich bei den Servern anzumelden.</li> <li>2. <a href="#">gewähren Sie einem Konto mehrere Sitzungen</a> auf jedem Server.</li> <li>3. <a href="#">Konfigurieren Sie Stationen für die automatische Anmeldung</a> auf den einzelnen Servern.</li> </ol>
<p><b>Meine Benutzer können die gleiche Benutzeranmeldung verwenden.</b> Sie benötigen keine individuelle Windows-Desktop Darstellung, die private Ordner zum Speichern von Daten oder personalisierten Desktops umfasst.</p>	<ol style="list-style-type: none"> <li>1. Erstellen Sie ein Domänen Konto für eine Gruppe oder für jeden Benutzer.</li> <li>2. <a href="#">gewähren Sie einem Konto mehrere Sitzungen</a> auf jedem Server.</li> </ol>
<p><b>Meine Benutzer müssen über eine eigene Windows-Desktop Darstellung verfügen.</b></p> <ul style="list-style-type: none"> <li>- <b>Option A</b> : jeder Benutzer mit einem Domänen Konto kann den Multipoint Services-Computer verwenden.</li> <li>- <b>Option B</b> -ich möchte einschränken, welche Domänen Konten auf den Server zugreifen können.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>Option A</b> -kein Setup ist erforderlich. Standardmäßig haben alle Domänen Benutzer Zugriff auf alle Multipoint Services-Computer im Netzwerk.</li> <li>- <b>Option B</b> : schränken Sie den Zugriff von Domänen Benutzerkonten auf den Multipoint Services-Computer ein. Anweisungen hierzu finden <a href="#">Sie unter Einschränken des Benutzer Zugriffs auf den Server</a>.</li> </ul>

**Ich möchte lokale Benutzerkonten verwenden und diese separat von meinen Domänen Konten verwalten.** Angenommen, Sie möchten, dass eine Person Multipoint Services, aber nicht die Domäne verwaltet, oder Sie möchten Domänen Konten nicht allen Multipoint Services-Benutzern zur Verfügung stellen.

Erstellen Sie ein oder mehrere lokale Benutzerkonten auf jedem Server. (Anweisungen hierzu finden Sie unter [Erstellen von lokalen Benutzerkonten](#).)

**Hinweis:** Dies bedeutet, dass jedes Benutzerkonto ein Profil auf jedem Server hat. Anders ausgedrückt: Wenn eine Datei in "eigene Dokumente" gespeichert wird, während Sie bei der Station von Server a angemeldet ist, wird die Datei bei der Anmeldung bei Server B nicht angezeigt.

# Erstellen lokaler Benutzerkonten

09.04.2020 • 2 minutes to read • [Edit Online](#)

Drei Ebenen lokaler Benutzerkonten können in mithilfe des Multipoint-Managers erstellt werden: Standard Benutzerkonten; Multipoint-Dashboardbenutzer mit eingeschränkten Administratorrechten und vollständige Administrator Benutzerkonten.

Verwenden Sie das folgende Verfahren, um ein lokales Benutzerkonto auf einem Multipoint-Server zu erstellen. Wenn Ihre Umgebung mehrere Multipoint-Server umfasst und Sie möchten, dass sich der Benutzer in einer beliebigen Station auf einem beliebigen Server anmelden kann, müssen Sie auf jedem Server ein lokales Benutzerkonto erstellen. Das Setup weist einige Einschränkungen auf. In einer Domänen Umgebung können Sie Benutzern auch die Verwendung ihrer Domänen Konten erlauben. Eine Übersicht über die Optionen finden Sie unter [Planen von Benutzerkonten für Ihre Windows-MultiPoint Services-Umgebung](#).

1. Melden Sie sich als Administrator beim Server an, und öffnen Sie den Multipoint-Manager.
2. Klicken Sie auf die Registerkarte **Benutzer**, und klicken Sie dann auf **Benutzerkonto hinzufügen**.

Der Assistent zum Hinzufügen eines Benutzerkontos wird geöffnet.

3. Geben Sie einen Kontonamen und ein Kennwort für das neue Benutzerkonto ein, und klicken Sie dann auf **weiter**.
4. Wählen Sie den Typ des Benutzerkontos aus, das Sie erstellen möchten:

- **Standard Benutzer** : kann sich bei einer Station anmelden und Benutzer Aufgaben durchführen, aber keinen Zugriff auf Multipoint Manager oder das Multipoint Server-Dashboard haben. das System kann nicht heruntergefahren werden.
- **Multipoint-Dashboardbenutzer** : verfügt über eingeschränkte Administratorrechte. Ein Dashboardbenutzer kann das Dashboard öffnen und Aufgaben ausführen, wie z. b. das Anmelden von Benutzern vom System oder das Herunterfahren des Multipoint-Server Computers, aber der Benutzer hat keinen Zugriff auf den Multipoint-Manager.
- **Administrative User** Administrator Verfügt über vollständige Administratorrechte in Multipoint Server. Beispielsweise kann ein Administrator den Multipoint-Manager ausführen, Benutzer hinzufügen und löschen, Systemeinstellungen ändern und Treiber aktualisieren.

5. Klicken Sie auf **weiter** und dann auf **Fertig** stellen, um das Benutzerkonto zu erstellen.

# Einschränken des Zugriffs von Benutzern auf den Multipoint-Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Unabhängig davon, ob Sie einen Multipoint-Server einer Active Directory Domäne hinzufügen oder lokale Benutzerkonten verwenden, haben alle Benutzer standardmäßig Zugriff auf Multipoint Server. Bevor Sie es Benutzern ermöglichen, sich an Stationen in ihrer Multipoint Services-Umgebung anzumelden, sollten Sie den Zugriff auf den Server einschränken.

Alle Benutzer in der Gruppe Remotedesktop Benutzer können sich bei Multipoint Server anmelden. Standardmäßig ist die Benutzergruppe "jeder" Mitglied der Gruppe "Remotedesktop Users". Daher können sich alle lokalen Benutzer und Domänen Benutzer am Multipoint-Server anmelden. Entfernen Sie zum Einschränken des Zugriffs auf Multipoint Server die Gruppe Jeder Benutzer aus der Gruppe Remotedesktop Benutzer, und fügen Sie dann der Gruppe Remotedesktop Benutzer bestimmte Benutzer oder Gruppen hinzu.

## Hinzufügen oder Entfernen von Benutzern oder Gruppen zur Gruppe "Remotedesktop Benutzer"

1. Öffnen Sie auf dem **Start** Bildschirm die **Computer Verwaltung**.
2. Klicken Sie in der Konsolen Struktur unter **lokale Benutzer und Gruppen** auf **Gruppen**.
3. Doppelklicken Sie auf **Remotedesktop Benutzer**, und befolgen Sie die Anweisungen zum Hinzufügen oder Entfernen von Benutzern.
  - Entfernen Sie die Gruppe Jeder, um den allgemeinen Zugriff auf den Server einzuschränken.
  - Fügen Sie der Gruppe Remotedesktop Benutzer jedes lokale Konto oder jedes Domänen Benutzer- oder Gruppenkonto hinzu, um den Multipoint Server-Benutzern Zugriff auf Stationen zu geben.

# Konfigurieren von Stationen für die automatische Anmeldung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie möchten, dass Ihre Stationen allen Benutzern zur Verfügung stehen – und die Benutzer keine privaten Ordner zum Speichern Ihrer persönlichen Daten oder personalisierten Desktops benötigen – können Sie die Stationen für die automatische Anmeldung konfigurieren. Bei der automatischen Anmeldung wird automatisch ein Benutzerkonto protokolliert, das beim Start der Multipoint-Dienste in den Einstellungen für die automatische Anmeldung angegeben wurde.

1. Öffnen Sie auf dem **Start** Bildschirm den **Multipoint-Manager**.
  2. Klicken Sie auf die Registerkarte **Stationen**, und klicken Sie dann auf den Namen der Station, die Sie für die automatische Anmeldung konfigurieren möchten.
  3. Klicken Sie im rechten Bereich auf **automatische Anmeldung konfigurieren**.
- Die Seite Automatische Anmeldung konfigurieren wird geöffnet.
4. Aktivieren Sie das Kontrollkästchen **automatische Anmeldung mit den folgenden Informationen**, und geben Sie dann das Benutzerkonto und das Kennwort ein, die für die automatische Anmeldung verwendet werden sollen. Klicken Sie auf **OK**.

## NOTE

Das Benutzerkonto, das Sie für die automatische Anmeldung verwenden, muss über ein Kennwort verfügen.

## NOTE

Wenn Sie sich vorübergehend bei einer Station anmelden möchten, die für die automatische Anmeldung mit einem anderen Benutzerkonto eingerichtet ist, zeigen Sie auf die obere rechte Ecke des Bildschirms, um ein vertikales Menü anzuzeigen, klicken Sie auf den Charm "Einstellungen", klicken Sie auf das Symbol "Power", und **halten Sie die UMSCHALTTASTE gedrückt**. Halten Sie die UMSCHALTTASTE gedrückt, bis eine Anmeldeaufforderung angezeigt wird.

# Zulassen mehrerer Sitzungen für ein Konto

09.04.2020 • 2 minutes to read • [Edit Online](#)

Um eine Gruppe von Benutzern zu aktivieren, verwenden Sie ein gemeinsam genutztes Konto gleichzeitig auf mehreren Stationen. Konfigurieren Sie den Multipoint-Server so, dass ein Konto gleichzeitig an mehreren Stationen angemeldet ist. Wenn sich ein Benutzer bei einer zweiten Station mit einem freigegebenen Benutzerkonto anmeldet, wird das Benutzerkonto standardmäßig von der ersten Station abgemeldet.

1. Öffnen Sie auf dem **Start** Bildschirm den **Multipoint-Manager**.
2. Klicken Sie auf die Registerkarte **Start**.
3. Klicken Sie in der Spalte **Computer** auf den Namen des Multipoint-Server Computers, und klicken Sie dann im rechten Bereich auf **Server Einstellungen bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen einem Konto das Kontrollkästchen **mehrere Sitzungen gestatten**, und klicken Sie dann auf **OK**.

# Aktivieren der Dateifreigabe in MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Sie können zulassen, dass Benutzer auf den Multipoint-Stationen Dateien auf zwei Arten freigeben:

- **Wenn Sie über einen Dateiserver im Netzwerk verfügen**, empfiehlt es sich, einen freigegebenen Ordner auf dem Dateiserver zu erstellen.
- **Wenn Sie ein kleines Netzwerk mit 2-3 Multipoint-Servern ohne dedizierten Dateiserver haben**, kann einer der Multipoint-Server als Dateiserver für alle verbleibenden Computer fungieren, auf denen Multipoint Services ausgeführt wird. Erstellen Sie einen freigegebenen Ordner auf diesem Server, und erstellen Sie dann lokale Benutzerkonten für alle Benutzer auf diesem Server. Der freigegebene Ordner kann sich auf dem ursprünglichen internen Laufwerk befinden, oder Sie können zusätzliche interne oder externe Laufwerke an den Computer anfügen.

# Systemverwaltung in MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Bevor Sie mit der Verwendung Ihres Multipoint Services-Systems beginnen, empfiehlt es sich, eine grundlegende Systemverwaltung durchzuführen.

Verwenden Sie die folgenden Informationen:

[Konfigurieren des Datenträger Schutzes](#)

[Installieren der Server Sicherung auf dem Multipoint Services-Computer](#)

# Konfigurieren des Datenträger Schutzes

09.04.2020 • 9 minutes to read • [Edit Online](#)

Sie können den Datenträger Schutz in Multipoint Services verwenden, um Ihr System Volume vor unbeabsichtigten Updates zu schützen, die Beibehaltung von Windows-Updates zu planen, während der Datenträger Schutz aktiv ist, den Datenträger Schutz vorübergehend zu deaktivieren und den Datenträger Schutz zu deinstallieren.

Wenn Sie den Datenträger Schutz in Multipoint Services aktivieren, können Sie das System Volume (das Laufwerk, auf dem Windows installiert ist, normalerweise C:), schützen, aus unerwünschten Änderungen. Wenn der Datenträger Schutz aktiviert ist, werden an dem System Volume vorgenommene Änderungen an einem temporären Speicherort gespeichert, sodass der Computer durch einfaches Neustarten des Computers verworfen wird und das System automatisch wieder in den vorherigen bekannten Zustand zurückgesetzt wird.

Der Administrator kann auf einfache Weise Software installieren oder Konfigurationsänderungen vornehmen, indem der Datenträger Schutz vorübergehend deaktiviert wird. Um das System mit Windows-Updates und Antimalwaredefinitionen auf dem aktuellen Stand zu halten, plant der Datenträger Schutz ein Wartungsfenster, um Updates herunterzuladen und zu installieren. Der Administrator kann auch ein benutzerdefiniertes Skript bereitstellen, das während des Wartungsfensters ausgeführt werden soll, um die Wartungsanforderungen über Windows Update hinaus zu erfüllen.

## Aktivieren des Datenträger Schutzes

Bevor Sie den Datenträger Schutz aktivieren, stellen Sie sicher, dass alle Anwendungen und Treiber installiert und auf dem neuesten Stand sind, und verschieben Sie die Benutzerprofile auf ein Volume, das nicht geschützt wird. Wenn Sie manuelle Updates vornehmen müssen, nachdem Sie den Datenträger Schutz aktiviert haben, können Sie den Datenträger Schutz temporär deaktivieren. Es ist jedoch am einfachsten, das System in einen idealen Zustand zu bringen, bevor der Datenträger Schutz aktiviert ist.

1. Melden Sie sich bei dem Server, auf dem Multipoint Services ausgeführt wird, als Administrator an.
2. Vor dem Aktivieren des Datenträger Schutzes:
  - Stellen Sie sicher, dass sich das Multipoint Services-System genau in dem Zustand befindet, in dem er bleiben soll. Stellen Sie beispielsweise sicher, dass installierte Software, Systemeinstellungen und Updates korrekt sind.
  - Verschieben Sie Benutzerprofile auf ein nicht geschütztes Volume, oder richten Sie einen freigegebenen Datei Speicherort vom System Volume ein, wie unter [Aktivieren der Dateifreigabe in Multipoint Services](#) beschrieben.
3. Öffnen Sie auf dem **Start** Bildschirm den **Multipoint-Manager**.
4. Klicken Sie auf die Registerkarte **Startseite**, klicken Sie auf **Datenträger Schutz aktivieren** und dann auf **OK**.

Wenn der Datenträger Schutz zum ersten Mal aktiviert wird, wird das System durch Installieren eines Treibers und Erstellen einer Cachedatei auf dem System Volume vorbereitet. Die Cachedatei speichert temporär alle Änderungen, die am System Volume vorgenommen werden, während der Datenträger Schutz aktiv ist. Da Systemupdates in der Cachedatei gespeichert werden, ändern Sie nicht den geschützten Inhalt des Volumes außerhalb der Cachedatei. Jedes Mal, wenn das System gestartet wird, wird die Cachedatei zurückgesetzt. Dadurch werden alle Änderungen verworfen, die seit dem vorherigen Systemstart gespeichert wurden. Folglich startet das

System immer denselben Zustand wie bei Aktivierung des Datenträger Schutzes.

Windows muss einige Systemdateien aktualisieren – einschließlich der System Page File, dem Speicherort des Absturz Abbilds und der Ereignisprotokolle. Diese Dateien werden nicht verworfen, wenn der Datenträger Schutz aktiviert ist. Um dies zu erreichen, wird ein neues Volume mit dem Namen "dkonservig" erstellt, wenn der Datenträger Schutz zum ersten Mal aktiviert wird, und diese Dateien werden auf dieses Volume verschoben. Die beibehaltene Partition ist nicht geschützt, sodass Schreibvorgänge in diese Dateien durch Neustarts beibehalten werden, auch wenn der Datenträger Schutz aktiviert ist.

## Planen von Software Updates

Wenn Windows für die automatische Installation von Windows-Updates konfiguriert ist, werden diese Updates vom Datenträger Schutz zum konfigurierten Zeitpunkt zugelassen, und die Updates werden nicht verworfen.

Wenn Windows Updates beispielsweise 3:00 Uhr geplant sind, prüft der Datenträger Schutz jeden Tag um 3:00 Uhr nach Updates. Wenn Updates gefunden werden, wird der Datenträger Schutz von Multipoint Services vorübergehend deaktiviert, die Updates werden angewendet, und der Datenträger Schutz wird erneut aktiviert.

1. Zeigen Sie im Multipoint-Manager die Registerkarte **Start** an, und klicken Sie dann auf **Software Updates planen**.
2. Klicken Sie im Dialogfeld Software Updates planen auf **Aktualisieren unter**, und wählen Sie eine Uhrzeit für Updates aus, z. B. **3:00 Uhr**.
3. Aktivieren Sie das Kontrollkästchen **Windows Update ausführen**.
4. Wenn Ihre Organisation ein eigenes Update Skript ausführt, aktivieren Sie das Kontrollkästchen **das folgende Programm ausführen**, und geben Sie den Speicherort des Aktualisierungs Skripts Ihrer Organisation an.
5. Wählen Sie eine maximale Zeit für das Ausführen von Updates aus.
6. Wenn Sie fertig sind, wählen Sie aus, ob das System auf den vorherigen Energiezustand zurückkehren oder nach dem Anwenden von Updates heruntergefahren werden soll.
7. Klicken Sie auf **OK**.

## Temporäres Deaktivieren des Datenträger Schutzes

Wenn ein Administrator Software installieren, Systemeinstellungen ändern oder andere Wartungs Tasks ausführen muss, die Systemupdates umfassen, können Sie den Datenträger Schutz temporär deaktivieren. Nachdem die Änderungen vorgenommen wurden, aktivieren Sie den Datenträger Schutz erneut. Während des Systemneustarts behält das System seinen Status bei Aktivierung des Datenträger Schutzes bei.

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Start**.
2. Klicken Sie auf der Registerkarte Startseite auf **Datenträger Schutz deaktivieren**, und klicken Sie dann auf **OK**.

### NOTE

Denken Sie daran, den Datenträger Schutz nach Abschluss der Wartung erneut zu aktivieren. Das System wird erst dann wieder geschützt, wenn der Administrator den Datenträger Schutz explizit erneut aktiviert.

## Datenträger Schutz deinstallieren

Wenn Sie den Datenträger Schutz deinstallieren, werden der Treiber und die Cachedatei entfernt. Daher sollten Sie diesen Vorgang nur ausführen, wenn Sie den Datenträger Schutz langfristig nicht mehr verwenden möchten.

Wenn Sie einfach Wartungsarbeiten durchführen oder den Schutz vorübergehend verhindern möchten, verwenden Sie stattdessen den Task "Datenträger Schutz deaktivieren".

Sie können den Datenträger Schutz unabhängig davon deinstallieren, ob er aktiviert oder deaktiviert ist.

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Start**.
2. Klicken Sie auf der Registerkarte Startseite auf **Datenträger Schutz deinstallieren**, und klicken Sie dann auf **OK**.

Nachdem Sie auf **OK** geklickt haben, wird der Computer neu gestartet. Der Vorgang zur Deinstallation erfordert mehrere Neustarts, in denen der Treiber und die Cachedatei entfernt werden. Die dbeibehaltene Partition bleibt, und die pagefile, der Speicherort des Absturz Abbilds und die Ereignisprotokoll Dateien bleiben für die Verwendung der dbeibehaltenen Partition konfiguriert.

# Installieren der Server Sicherung auf dem Multipoint-Server

09.04.2020 • 4 minutes to read • [Edit Online](#)

Es wird empfohlen, dass Sie einen Sicherungs-und Wiederherstellungs Plan für Ihre Multipoint-Server in Erwägung gezogen.

Ein guter Sicherungs-und Wiederherstellungs Plan ist für jede Größen Umgebung wichtig. Windows Server-Sicherung ist ein Feature in Windows Server 2016, das eine Reihe von Assistenten und anderen Tools bereitstellt, mit denen Sie grundlegende Sicherungs-und Wiederherstellungs Aufgaben für den Server ausführen können, auf dem es installiert ist. Sie können Windows Server-Sicherung verwenden, um einen vollständigen Server (alle Volumes), ausgewählte Volumes, den Systemstatus oder bestimmte Dateien oder Ordner zu sichern und eine Sicherung zu erstellen, die Sie zum Neuerstellen des Systems verwenden können.

Sie können Volumes, Ordner, Dateien, bestimmte Apps und den Systemstatus wiederherstellen. Und bei Notfällen wie Festplattenfehlern können Sie ein System entweder von Grund auf neu oder mithilfe alternativer Hardware neu erstellen. Zu diesem Zweck müssen Sie über eine Sicherung des vollständigen Servers oder nur der Volumes verfügen, die Betriebssystemdateien und die Windows-Wiederherstellungs Umgebung enthalten. Dadurch wird das gesamte System auf dem alten System oder auf einer neuen Festplatte wieder hergestellt.

Ein wichtiges Feature von Windows Server-Sicherung ist die Möglichkeit, Sicherungen für die automatische Ausführung zu planen.

Verwenden Sie die folgenden Verfahren, um den erforderlichen Sicherungstyp einzurichten.

## Installieren von Sicherungs-und Wiederherstellungs Tools

1. Öffnen Sie auf dem **Start Bildschirm Server-Manager**.
2. Klicken Sie zum Starten des Assistenten zum Hinzufügen von Rollen auf **Rollen und Features hinzufügen**. Klicken Sie dann auf **weiter**, nachdem Sie die Anmerkungen zu **Beginn** überprüft haben.
3. Wählen Sie die Option **rollenbasierte oder featurebasierte Installation** aus, und klicken Sie dann auf **weiter**.
4. Wählen Sie den lokalen Computer aus, den Sie verwalten möchten, und klicken Sie auf **weiter**.  
Daraufhin wird der Assistent zum Hinzufügen von Funktionen geöffnet.
5. Erweitern Sie auf der Seite **Features auswählen** die Option Windows Server-Sicherung Features, aktivieren Sie die Kontrollkästchen für **Windows Server-Sicherung** und **Befehlszeilen Tools**, und klicken Sie dann auf **weiter**.

### NOTE

Wenn Sie nur das Snap-in und das Befehlszeilen Tool Wbadmin installieren möchten, erweitern Sie **Windows Server-Sicherung Features**, und aktivieren Sie dann nur das Kontrollkästchen **Windows Server-Sicherung** – Vergewissern Sie sich, dass das Kontrollkästchen **Befehlszeilen Tools** deaktiviert ist.

6. Überprüfen Sie Ihre Auswahl auf der Seite **Installations Auswahl bestätigen**, und klicken Sie dann auf **Installieren**.

Wenn während der Installation Fehler auftreten, werden die Fehler auf der Seite **Installations Ergebnisse** angezeigt.

7. Nachdem die Installation erfolgreich abgeschlossen wurde, sollten Sie in der Lage sein, auf diese Sicherungs-und Wiederherstellungs Tools zuzugreifen:

- Um das Windows Server-Sicherung Snap-in zu öffnen, geben Sie auf dem **Start** Bildschirm **Backup** ein, und klicken Sie dann in den Ergebnissen auf **Windows Server-Sicherung**.
- Zum Starten des Wbadmin-Tools und Anzeigen der Syntax für die zugehörigen Befehle: Geben Sie auf dem **Start** Bildschirm **Command** ein. Klicken Sie in den Ergebnissen mit der rechten Maustaste auf **Eingabeaufforderung**, klicken Sie unten auf der Seite auf **als Administrator ausführen**, und klicken Sie dann an der Bestätigungsaufforderung auf **Ja**. Geben Sie an der Eingabeaufforderung **Wbadmin/?** ein. und drücken Sie die EINGABETASTE. Es sollten Befehlssyntax und Beschreibungen für das Tool angezeigt werden.

## Konfigurieren von Sicherungen mithilfe von Windows Server-Sicherung

- Befolgen Sie die Anweisungen unter [Sichern des Servers](#).

# Konfigurieren von Gruppenrichtlinien für eine Domänenbereitstellung

09.04.2020 • 4 minutes to read • [Edit Online](#)

Um sicherzustellen, dass Ihre Domänen Bereitstellung von Multipoint Services ordnungsgemäß funktioniert, wenden Sie die folgenden Gruppenrichtlinien Einstellungen auf das wmsshell-Benutzerkonto in einem Multipoint Services-System an.

## IMPORTANT

Einige Gruppenrichtlinien Einstellungen können verhindern, dass erforderliche Konfigurationseinstellungen auf Multipoint Services angewendet werden. Stellen Sie sicher, dass Sie Ihre Gruppenrichtlinien Einstellungen verstehen und definieren, damit Sie in Multipoint Services ordnungsgemäß funktionieren. Beispielsweise kann eine Gruppenrichtlinie Einstellung, die die automatische Anmeldung verhindert, Probleme mit dem Multipoint Services-Anmeldeverhalten darstellen.

## Aktualisieren von Gruppenrichtlinien für das wmsshell-Benutzerkonto

Beim wmsshell-Benutzerkonto handelt es sich um ein Systemkonto, das von Multipoint Services zum Anmelden in der-Konsole verwendet wird, in der die eigentlichen Stationen erstellt werden. Dieses Konto soll nicht von Multipoint Manager verwaltet werden.

## NOTE

Informationen zum Aktualisieren von Gruppenrichtlinien finden Sie unter [Editor für lokale Gruppenrichtlinien](#).

**Richtlinie:** Benutzerkonfiguration > Administrative Vorlagen > Systemsteuerung > **Personalisierung**

Weisen Sie die folgenden Werte zu:

EINSTELLUNG	WERTE
Bildschirmschoner aktivieren	Deaktiviert
Zeitlimit für Bildschirmschoner	Deaktiviert Sekunden: xxx
Kennwortschutz für den Bildschirmschoner verwenden	Deaktiviert

**Richtlinie:** Computer Konfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten > **Lokal anmelden zulassen**

EINSTELLUNG	WERTE
-------------	-------

EINSTELLUNG	WERTE
Lokal anmelden zulassen	<p>Stellen Sie sicher, dass die Liste der Konten das wmsshell-Konto enthält.</p> <p><b>Hinweis:</b> Standardmäßig ist das wmsshell-Konto Mitglied der Gruppe "Benutzer". Wenn die Gruppe "Benutzer" in der Liste enthalten ist und wmsshell Mitglied der Gruppe "Benutzer" ist, müssen Sie das wmsshell-Konto nicht zur Liste hinzufügen.</p>

#### IMPORTANT

Wenn Sie Gruppenrichtlinien festlegen, stellen Sie sicher, dass die Richtlinien die automatischen Updates und die Fehlerberichterstattung für Fehlerberichte auf dem Multipoint-Server nicht beeinträchtigen. Diese werden von den Einstellungen **Updates automatisch installieren** und automatisch **Windows-Fehlerberichterstattung** festgelegt, die bei der Installation von Windows MultiPoint Server ausgewählt, in Multipoint Manager mithilfe von **Server Einstellungen bearbeiten** oder in geplanten Updates für den Datenträger Schutz konfiguriert wurden.

## Aktualisieren der Registrierung

Für eine Domänen Bereitstellung von Multipoint Services sollten Sie die folgenden Registrierungs Unterschlüssel aktualisieren.

#### IMPORTANT

Eine fehlerhafte Bearbeitung der Registrierung kann Ihr System schwer beschädigen. Bevor Sie Änderungen an der Registrierung vornehmen, sollten Sie alle wichtigen Computerdaten sichern.

#### So aktualisieren Sie Registrierungs Unterschlüssel für eine Domänen Bereitstellung von Multipoint Services

- Öffnen Sie den Registrierungs-Editor. (Geben Sie an einer Eingabeaufforderung **Regedit. exeein**, und drücken Sie die **EINGABETASTE**.)
- Suchen Sie im linken Bereich den folgenden Registrierungs Unterschlüssel, und wählen Sie ihn aus:

HKEY\_USERS<sidoswmshell > \software\policies\microsoft\windows\control Panel\Desktop

Dabei ist "" die Sicherheits-ID (SID) für das wmsshell-Konto. Informationen dazu, wie Sie die SID identifizieren, finden Sie unter [Zuordnen eines Benutzernamens zu einer Sicherheits-ID \(SID\)](#).

- Aktualisieren Sie in der Liste auf der rechten Seite die folgenden Unterschlüssel.

UNTERSCHLÜSSEL	WERTNAME	WERTDATEN
Screensaveactive	REG_SZ	0 (null)
SCREENSAVETIMEOUT	REG_SZ	120
ScreenSaverIsSecure	REG_SZ	0 (null)

So aktualisieren Sie einen Registrierungs Unterschlüssel:

- Wenn der Registrierungsschlüssel im linken Bereich ausgewählt ist, klicken Sie im rechten Bereich mit der rechten Maustaste auf den Unterschlüssel, und klicken Sie dann auf ändern.
- Geben Sie im Dialogfeld Zeichenfolge bearbeiten einen neuen Wert in **Wertdatenein**, und klicken Sie

dann auf OK.

4. Nachdem Sie die Aktualisierung der Registrierungs Unterschlüssel abgeschlossen haben, starten Sie den Computer neu, um die Änderungen zu aktivieren.

# Verwalten von MultiPoint Services

09.04.2020 • 2 minutes to read • [Edit Online](#)

Multipoint™ Services ermöglicht es mehreren Benutzern, die jeweils über eine eigene unabhängige Windows-Benutzeroberflächen Funktion verfügen, die gleichzeitige Freigabe eines Computers. Benutzerstationen bestehen aus einem Monitor, einer Tastatur und einer Maus und sind direkt über USB, Videokabel oder das Netzwerk mit dem Hostcomputer verbunden.

Verwenden Sie die folgenden Informationen, um zu erfahren, welche Aufgaben Sie in Multipoint Manager und Multipoint-Dashboard ausführen können, wie z. b. die Verwaltung von Multipoint Services-Stationen mithilfe von Multipoint Manager und die tägliche Verwendung des Multipoint-Dashboards.

- [Verwalten des MultiPoint Services-Systems](#)
- [Verwalten der Stationshardware](#)
- [Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)
- [Verwalten von Benutzerstationen](#)
- [Verwalten von Benutzerkonten](#)
- [Verwalten von virtuellen Desktops](#)
- [Verwalten von Benutzerdateien](#)
- [Verwalten von Benutzerdesktops mit dem MultiPoint-Dashboard](#)
- [Verwalten von MultiPoint-Systemen mit dem MultiPoint-Dashboard](#)

## Siehe auch

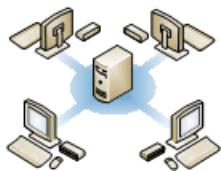
- [Multipoint Services-Forum](#)

# Verwalten des MultiPoint Services-Systems

09.04.2020 • 2 minutes to read • [Edit Online](#)

Mithilfe von MultiPoint Services können mehrere Stationen mit einem einzigen Computer verbunden werden. Eine herkömmliche Station besteht aus einem *Stationshub* oder Zero Client, einem Monitor, einer Tastatur und einer Maus. RDP-Clients (Network-Connected Remotedesktopprotokoll) werden ebenfalls unterstützt.

Die folgende Abbildung zeigt ein Beispieldesign für ein MultiPoint Services-System, das vier *Stationen* umfasst. Eine solche Einrichtung ermöglicht es mehreren Benutzern, den Computer gleichzeitig zu verwenden und unabhängig voneinander zu arbeiten oder Gruppenaktivitäten auszuführen.



Multipoint Services umfasst den Multipoint-Manager, der Ihnen als Administrator bei der Überwachung und Verwaltung Ihres Multipoint-Systems sowie des Multipoint-Dashboards hilft, das eine alltägliche Verwaltungs Funktionalität bietet. Die Themen in diesem Hilfe Handbuch beschreiben viele der Aufgaben, die Sie in Multipoint Manager und Multipoint-Dashboard ausführen können.

## Weitere Informationen

[Verwalten von Benutzerdesktops mit dem MultiPoint-Dashboard](#)

[Überlegungen zu Datenschutz und Sicherheit](#)

# Überlegungen zu Datenschutz und Sicherheit

09.04.2020 • 2 minutes to read • [Edit Online](#)

Da es sich bei Ihrem MultiPoint Services-System entwurfsbedingt um eine freigegebene Computerumgebung handelt, sollten Sie folgende Aspekte des Datenschutzes und der Computersicherheit beachten.

## Datenschutz in einem MultiPoint Services-System

Die Funktionen von MultiPoint Services für das Freigeben oder Schützen von Benutzerdokumenten können für Sie, andere *Administratoren*, *MultiPoint-Dashboardbenutzer* oder *Standardbenutzer* in Ihrem MultiPoint Services-System neu sein. Im Multipoint-Manager können Sie Bildschirmaktivitäten auf allen aktiven Desktops von Standard Benutzern sehen. Standardbenutzer werden benachrichtigt, wenn sie sich beim MultiPoint Services-System anmelden, und müssen diese Überwachung akzeptieren, um fortfahren zu können. Weitere Informationen zum Freigeben oder Schützen von Inhalten finden Sie unter [Verwalten von Benutzerdateien](#).

## Sicherheit in einem MultiPoint Services-System

Machen Sie sich als Administrator Ihres MultiPoint Services-System mit den Windows-Funktionen für Schutz und Sicherheit vertraut. Diese umfassen automatische Windows-Updates sowie Unterstützung für Firewalls, Virenschutz und Schutz vor Spyware und anderer Schadsoftware.

Freigegebene Computerressourcen wie ein MultiPoint Services-System können aufgrund der potenziell großen Anzahl von Systembenutzern und des einfachen Zugangs zu Stationshardwaregeräten und -kabeln für Sicherheitsrisiken anfällig sein. Ein böswilliger Benutzer kann versuchen, eine Vorrichtung zur Protokollierung von Tastatureingaben oder ein ähnliches Gerät an einem MultiPoint Services-Stationshub zu installieren. Wenn Sie unbekannte Geräte feststellen, die mit den Anschläßen Ihres MultiPoint Service-Systems verbunden sind, sollten Sie diese als verdächtig einstufen und die Sicherheitsescalationsrichtlinien Ihrer Organisation befolgen.

## Weitere Informationen

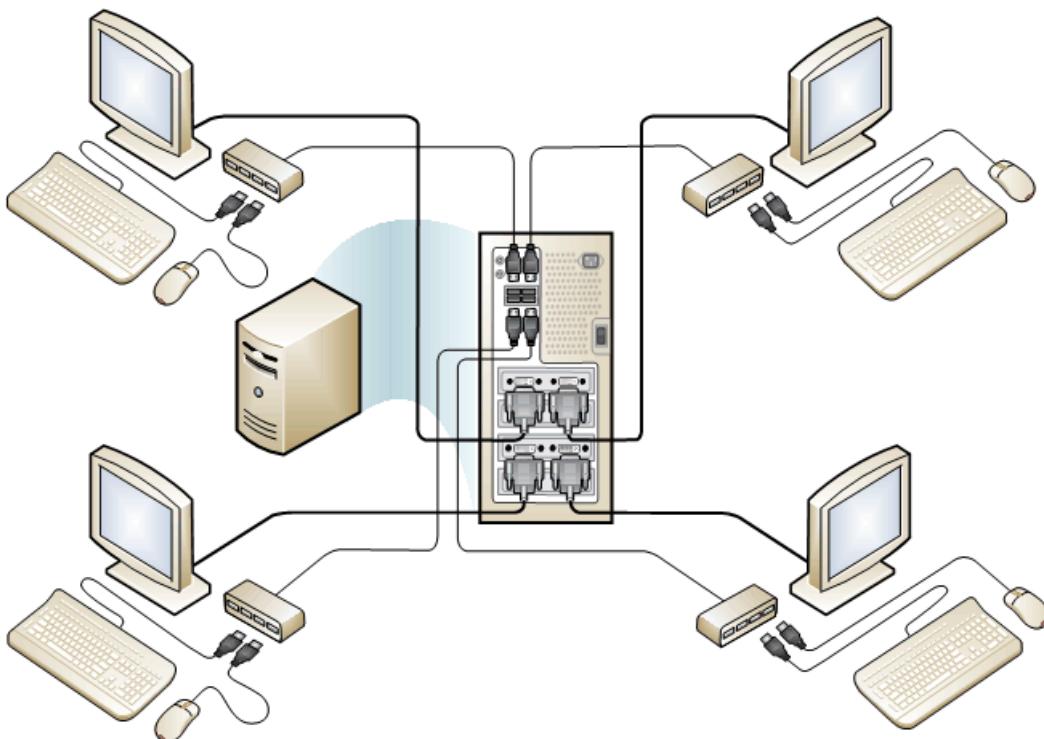
[Verwalten von Benutzerdateien](#)  
[Verwalten des MultiPoint Services-Systems](#)

# Verwalten der Stationshardware

09.04.2020 • 4 minutes to read • [Edit Online](#)

Ein MultiPoint Services-System besteht aus einem einzelnen Computer und mindestens einer Station. Bei der Stationshardware handelt es sich normalerweise um einem Stationshub, eine Maus, eine Tastatur und einen Videomonitor. Stationen sind üblicherweise physisch mit dem Computer verbunden.

Die folgende Abbildung zeigt ein Beispiellayout für ein MultiPoint Services-System mit vier Stationen. Jede Station ist mit dem Multipoint Services-Computer verbunden, indem ein USB-Hub und Multi-Monitor-Grafikkarten verwendet werden. Diese Abbildung zeigt keine Stationen, die mithilfe von Multifunktionshubs angeschlossen sind.



In den Themen dieses Abschnitts wird beschrieben, wie Sie den Status der an das MultiPoint Services-System angeschlossenen Hardware anzeigen können. Ferner erhalten Sie detaillierte Informationen zu den Arten von USB-Geräten und anderen Hardwareperipheriegeräten, mit denen eine MultiPoint Services-Station eingerichtet werden kann. Im Folgenden finden Sie eine kurze Beschreibung der in diesem Abschnitt enthaltenen Themen, mit deren Hilfe Sie Hardware auswählen und Ihre MultiPoint Services-Station einrichten können.

## Anzeigen des Hardwarestatus

Im Multipoint-Manager können Sie die Registerkarte **Stationen** verwenden, um den Status der Stationen und Hardware Geräte anzuzeigen, die mit dem Multipoint Services-Computer verbunden sind. Weitere Informationen zum Anzeigen des Status Ihres MultiPoint Services-Computers und der daran angeschlossenen Hardwaregeräte finden Sie im Thema [Anzeigen des Hardwarestatus](#).

## Arbeiten mit USB-Geräten

USB-Geräte und andere Hardwareperipheriegeräte im MultiPoint Services-System funktionieren unterschiedlich, je nachdem, ob sie an den MultiPoint Services-Computer oder eine MultiPoint Services-Station angeschlossen sind. Im Thema [Arbeiten mit USB-Geräten](#) wird beschrieben, wie unterschiedliche Hardwaregeräte in diesen Szenarios funktionieren können. Zudem bietet das Thema ausführliche Informationen für die Arbeit mit

Stationshubs.

## Arbeiten mit Videogeräten

Im Thema [Arbeiten mit Videogeräten](#) wird erläutert, wie Videogeräte, z.B. Monitore oder Projektoren, funktionieren, wenn sie an einen Computer in Ihrem MultiPoint Services-System oder an eine MultiPoint Services-Station angeschlossen werden.

## Einrichten einer Station

Im Thema [Einrichten einer Station](#) wird beschrieben, wie die Hardwareperipheriegeräte an einen MultiPoint Services-Stationshub angeschlossen werden, um eine MultiPoint Services-Station zu erstellen. MultiPoint Services unterstützt zwei Typen von Stationshubs:

- Einen extern betriebenen oder Bus gestützten *USB-Hub* mit mehreren Ports, mit dem eine Maus, Tastatur und andere USB-Peripheriegeräte unterstützt werden können
- *Multifunktionshubs*, die mit einer integrierten Grafikkarte und Anschlüssen für Maus, Tastatur und Audioperipheriegeräte ausgestattet sein können.

Beide Arten von Stationshubs werden über ein USB-Kabel an den Computer angeschlossen. Mit den Verfahren im Thema [Einrichten einer Station](#) wird beschrieben, wie Hardwaregeräte an die unterschiedlichen Stationshubs angeschlossen werden.

## Weitere Informationen

[Anzeigen des Hardwarestatus](#)

[Arbeiten mit USB-Geräten](#)

[Arbeiten mit Videogeräten](#)

[Einrichten einer Station](#)

# Anzeigen des Hardwarestatus

09.04.2020 • 2 minutes to read • [Edit Online](#)

Verwenden Sie im Multipoint-Manager die Registerkarte **Stationen**, um *Stations* Informationen anzuzeigen, wie z. b.:

- Stationsname
- Erforderliche Hardware, damit jede Station verwendbar ist (in der Regel enthält die Hardware einen Videomonitor, einen *Stations-Hub*, eine Tastatur und eine Maus)
- Zusätzliche, einer Station zugeordnete Hardwareperipheriegeräte
- Benachrichtigungen über fehlende oder nicht funktionierende erforderliche Hardware an einer Station werden in der entsprechenden Spalte angezeigt
- Namen von aktuell mit dem MultiPoint Services-System verbundenen Benutzern

## TIP

Wenn die Stationen in Ihrem Multipoint Services-System physisch auf eine Art und Weise angeordnet sind, die Sie beibehalten möchten (z. B. um eine zirkuläre Tabelle), ist es möglicherweise hilfreich, Stationsnamen oder Zahlen Bezeichnungen wie Aufkleber oder Karten einzuhalten, um den Videomonitor oder den Hub der einzelnen Stationen zu identifizieren. Auf diese Weise können Sie und andere Benutzer der Stationen anhand der eindeutigen Identifizierungsnamen oder -nummern einfacher auf Stationen verweisen und diese unterscheiden.

## NOTE

Wenn sich das System im Konsolenmodus befindet, ist die Registerkarte **Stationen** nicht verfügbar.

## Weitere Informationen

[Verwalten der Stationshardware](#)

[Wechseln zwischen Modi](#)

# Arbeiten mit USB-Geräten

09.04.2020 • 8 minutes to read • [Edit Online](#)

Sie können Geräte entweder an den Computer in Ihrem MultiPoint Services-System oder an einen MultiPoint-Stationshub anschließen. Der Standort, an dem ein Gerät angeschlossen wird, und die Art des Geräts wirken sich darauf aus, ob ein Gerät für alle Benutzer im System, nur für einzelne Benutzer oder für keinen Benutzer verfügbar ist. Nachfolgend finden Sie Beispiele für die verschiedenen Arten der Verbindung:

- Wenn Sie ein Gerät, wie z.B. einen Drucker oder ein USB-Massenspeichergerät, direkt an den Computer anschließen, können alle Sitzungsbenuutzer im MultiPoint Services-System auf das Gerät zugreifen. Benutzer von virtuellen Desktopstationen können nicht auf direkt an den Computer angeschlossene Geräte zugreifen.
- Wenn Sie ein Gerät an einen Stationshub anschließen, z.B. eine Tastatur, eine Maus, ein *Audiogerät* oder ein Massenspeichergerät, ist das Gerät nur für den Benutzer verfügbar, der an dieser MultiPoint Services-Station angemeldet ist.
- Wenn Sie bestimmte Arten von Geräten an den Computer anschließen, z.B. eine Tastatur oder eine Maus, sind diese Geräte für keinen Benutzer im System verfügbar.

Die folgende Tabelle zeigt, welche Liste von Geräten mit ihrem jeweiligen Verhalten in Abhängigkeit vom Anschlussort im System. Informationen zum Verbinden von Stations Hubs finden Sie unter [Arbeiten mit Station Hubs](#). Weitere Informationen zum Verbinden von Videomonitoren mit einer Station finden Sie unter [Arbeiten mit Videogeräten](#).

Schutz	Verhalten, wenn es direkt mit dem Computer verbunden ist	Verhalten bei der Verbindung mit einer Station	Hinweise
Tastatur	Das direkte Anschließen einer Tastatur an den Computer wird nicht empfohlen.	Nur für den Stationsbenutzer verfügbar.	Wenn die Tastatur einen USB-Anschluss aufweist, wird der USB-Hub in der Tastatur möglicherweise als Stationshub verwendet. Andere mit diesem Anschluss verbundene USB-Geräte sind nur für den Benutzer verfügbar, der diese Tastatur verwendet. Einige Stationshubs sind mit einem PS/2-Mausanschluss ausgestattet, der im Hub in eine USB-Verbindung konvertiert wird.
Maus	Das direkte Anschließen einer Maus an den Computer wird nicht empfohlen.	Nur für den Stationsbenutzer verfügbar.	Einige Stationshubs sind mit einem PS/2-Mausanschluss ausgestattet, der im Hub in eine USB-Verbindung konvertiert wird.

USB-Hub	Weitere Informationen finden Sie unter <a href="#">Arbeiten mit Stations Hubs</a> .	Weitere Informationen finden Sie unter <a href="#">Arbeiten mit Stations Hubs</a> .	
Videomonitor	Weitere Informationen finden Sie unter <a href="#">Multipoint Services-Video Geräte</a> .	Weitere Informationen finden Sie unter <a href="#">Multipoint Services-Video Geräte</a> .	
Audioausgabegeräte (z.B. Kopfhörer)	Das direkte Anschließen eines Audioausgabegeräts an den Computer wird nicht empfohlen.	Nur für den Stationsbenutzer verfügbar.	Einige Stationshubs sind mit einem analogen Audioanschluss ausgestattet, der im Hub in eine USB-Audioverbindung konvertiert wird.
Audioeingabegeräte (z.B. Mikrofone)	Das direkte Anschließen eines Audioeingabegeräts an den Computer wird nicht empfohlen.	Nur für den Stationsbenutzer verfügbar.	Einige Stationshubs sind mit einem analogen Audioanschluss ausgestattet, der im Hub in eine USB-Audioverbindung konvertiert wird.
Drucker	Für alle Benutzer im System verfügbar.*	Nur für den Stationsbenutzer verfügbar.	
USB-Massenspeichergerät	Für alle Benutzer im System verfügbar.*	Nur für den Stationsbenutzer verfügbar.	Zu diesen Geräten gehören beispielsweise USB-Flashlaufwerke, externe Festplattenlaufwerke und Digitalkameras.
Webkameras	Für alle Benutzer im System verfügbar.*	Nur für den Stationsbenutzer verfügbar.	Es kann immer nur ein Benutzer gleichzeitig eine Verbindung mit der Kamera herstellen.

\* Geräte, die mit dem Host Computer verbunden sind, sind für die Benutzer, die bei virtuellen Desktop Stationen angemeldet sind, nicht sichtbar.

Weitere Informationen zum Einrichten einer Station finden Sie unter [Einrichten einer Station](#).

## Arbeiten mit Stationshubs

Es gibt vier Szenarien für die Verwendung eines USB-Hubs, wenn er an ein MultiPoint Services-System angeschlossen ist. Jedes der folgenden Szenarien bietet einen unterschiedlichen Zugriff auf die angeschlossenen Geräte, je nach Art des Hubs sowie des Verbindungsports im System.

- Ein Stationshub, der mit dem Computer in Ihrem MultiPoint Services-System mit angeschlossener Tastatur verbunden ist, kann zum Erstellen einer MultiPoint Services-Station verwendet werden. Tastatur und Maus werden über die am Hub verfügbaren Anschlüsse mit dem Stationshub verbunden. Ein Videomonitor wird mit dem Videoanschluss des Computers oder, falls verfügbar, mit dem Videoadapter des Stationshubs verbunden. Tastatur, Maus und Monitor werden dann einer MultiPoint Services-Station *zugeordnet*.
- Ein USB-Hub, der mit dem Computer in Ihrem MultiPoint Services-System ohne angeschlossene Tastatur verbunden ist, kann verwendet werden, um zusätzliche Geräte an den Computer anzuschließen, wenn der Computer nicht über ausreichende Anschlüsse für die erforderlichen Geräte verfügt. Alle an diesen USB-Hub angeschlossenen Geräte sind für alle Benutzer des MultiPoint Services-Systems verfügbar. Hierbei handelt es sich nicht um einen MultiPoint Services-Stationshub.

- Über einen USB-Hub mit eigener Stromversorgung, der mit dem Computer in Ihrem MultiPoint Services-System verbunden ist – auch als Zwischenhub bezeichnet –, können zusätzliche USB-Hubs angeschlossen werden, die zum Erstellen von MultiPoint-Stationen verwendet werden.
- Über einen mit einem Stationshub verbundenen USB-Hub können zusätzliche Geräte an den Stationshub angeschlossen werden. Tastaturen müssen direkt an den Stationshub angeschlossen werden.

Weitere Informationen zum Einrichten einer MultiPoint Services-Station finden Sie unter [Einrichten einer Station](#).

## Weitere Informationen

[Arbeiten mit Videogeräten](#)

[Verwalten der Stationshardware](#)

[Einrichten einer Station](#)

# Arbeiten mit Videogeräten

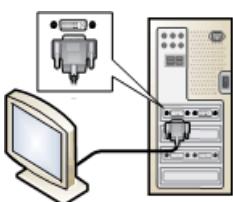
09.04.2020 • 3 minutes to read • [Edit Online](#)

Erfahren Sie, wie Videogeräte, z.B. Monitore oder Projektoren, funktionieren, wenn sie an einen Computer in Ihrem MultiPoint Services-System oder an eine MultiPoint Services-Station angeschlossen werden.

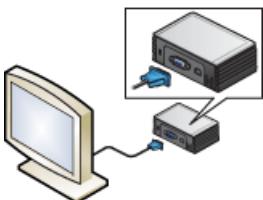
## Arbeiten mit Videomonitoren

In Abhängigkeit von Ihrer MultiPoint Services-Systemhardware gibt es zwei Möglichkeiten, um einen Videomonitor anzuschließen:

- Verbinden Sie bei *USB-Hub-basierten Systemen* das Videomonitor Kabel mit einem geöffneten Videoport auf dem Computer, wie in der folgenden Abbildung dargestellt:



- Verbinden Sie das Videomonitor Kabel für *multifunktionshub-basierte Systeme* mit integrierter Videounterstützung mit dem Videoport auf dem multifunktionshub:

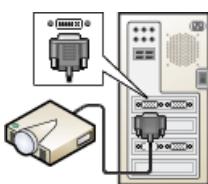


Weitere Informationen finden Sie im Thema [Einrichten einer Station](#).

## Arbeiten mit Videoprojektoren

Wenn ein großes Bild zur Anzeige für andere Benutzer projiziert werden soll – beispielsweise in einer Laborumgebung –, können Sie einen Videoprojektor an Ihr MultiPoint Services-System anschließen. Sowohl für USB Hub-basierte als auch für auf mehreren Funktionen basierende Hub-basierte Stationen haben Sie zwei Möglichkeiten, einen Projektor mit einer Station zu verbinden:

- Ersetzen Sie einen Monitor durch einen Projektor, und verwenden Sie den Projektor als Anzeigegerät für diese Station, wie in der folgenden Abbildung gezeigt:



- Erwerben Sie ein Video Splitter Gerät, um sowohl einen Projektor als auch einen Monitor mit dem Videoport der Station zu verbinden.

In MultiPoint Services wird auf beiden Anzeigegeräten dasselbe Bild angezeigt. Wenn keine Projektion ausgeführt wird, können Sie den Projektor ausschalten und nur den Videomonitor verwenden.

Bei beiden Optionen müssen Sie Folgendes beachten:

- Das Anschließen eines Videoanzeigegeräts kann erfordern, dass *die Station erneut zugeordnet* wird, damit das neue Anzeigegerät von MultiPoint Services richtig erkannt werden kann. Befolgen Sie die Anweisungen, die auf dem Videoanzeige Gerät der Station angezeigt werden.
- Eventuell müssen Sie sich Adapter oder Konverter zur Signalamwandlung zwischen DVI- und VGA-Steckern besorgen.
- Die Verwendung eines "Y"-Splitter Kabels kann die Videoqualität auf beiden Videogeräten verringern.
- Wenn Sie einen Projektor und einen Monitor über ein "Y"-Splitter Kabel verwenden, passt Multipoint Services die Bildschirmauflösung beider Geräte an die niedrigste maximale Auflösung der beiden Geräte an – in der Regel den Projektor.
- Multipoint Services unterstützt nicht die Erweiterung der Anzeige einer einzelnen Station über mehrere Monitore hinweg.

## Weitere Informationen

[Verwalten der Stationshardware](#)

[Einrichten einer Station](#)

# Einrichten einer Station

09.04.2020 • 5 minutes to read • [Edit Online](#)

Eine MultiPoint Server-*Station* besteht normalerweise aus einem *Stationshub*, einer Maus, einer Tastatur und einem Videomonitor. In diesem Thema wird beschrieben, wie die Hardwaregeräte mit dem Stationshub verbunden werden, um eine MultiPoint Services-Station zu erstellen.

Der Stationshub ist ein Hardwaregerät, über das Peripheriegeräte an einen Computer in einem MultiPoint Services-System angeschlossen werden. MultiPoint Services unterstützt zwei Typen von Stationshubs:

- **USB-Hub:** Ein generischer USB-Erweiterungshub mit mehreren Anschlüssen, der die USB 2.0-Spezifikationen (Universal Serial Bus) oder höher erfüllt. Solche Hubs verfügen typischerweise über zwei, vier oder mehr USB-Anschlüsse, die das Verbinden mehrerer USB-Geräte mit einem einzelnen USB-Anschluss des Computers ermöglichen. USB-Hubs sind üblicherweise separate Geräte, die extern oder im Bus betrieben werden können. Bei der Verwendung als Stationshub mit MultiPoint Services wird empfohlen, einen Hub mit vier oder mehr Anschlüssen zu verwenden.

## IMPORTANT

Wenn Sie beabsichtigen, andere USB-Geräte als eine Tastatur und eine Maus am Hub anzuschließen, sollten Sie einen Hub mit externer Stromversorgung verwenden, um die Leistung zu verbessern.

- **Multifunktionshub:** Ein erweiterungshub, der über einen USB-Anschluss eine Verbindung mit dem Computer herstellt und die Verbindung verschiedener nicht-USB-Geräte mit dem Hub, einschließlich eines Video Monitors, ermöglicht. Multifunktionshubs werden von bestimmten Hardwareherstellern erstellt und erfordern möglicherweise die Installation eines gerätespezifischen Treibers.

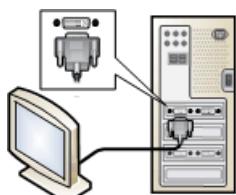
Wenn Sie Ihrem MultiPoint Services-System eine Station hinzufügen möchten, müssen Sie zuerst sicherstellen, dass genügend Anschlüsse für die zu verwendende Stationshardware verfügbar sind. Außerdem müssen Sie die entsprechende Anzahl von *Client Zugriffs Lizenzen* (*Client Access Licenses, CALs*) für Ihr Multipoint Services-System sichern.

## Einrichten der Stationshardware

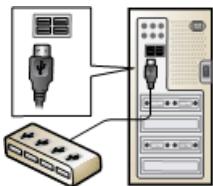
Die Verfahren in diesem Abschnitt beschreiben, wie MultiPoint Services-Stationshardware an die verschiedenen Typen von Stationshubs angeschlossen wird.

### So richten Sie eine Station mit einem USB-Hub ein

1. Bevor eine neue Station angeschlossen werden kann, *beenden Sie alle Benutzersitzungen*, und fahren Sie dann den Computer sowie alle anderen eingeschalteten Geräte in Ihrem MultiPoint Services-System herunter.
2. Schließen Sie das Kabel des neuen Videomonitors wie in der folgenden Abbildung gezeigt am Videoanzeigenschluss des Computers an:



3. Schließen Sie den neuen USB-Hub an einem freien USB-Anschluss des Computers an:



4. Schließen Sie eine Tastatur und eine Maus an den USB-Hub an:



5. Stecken Sie das Stromkabel des Videomonitors in eine Steckdose.

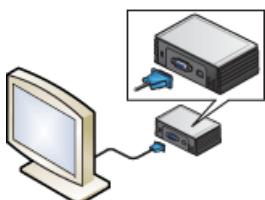
6. Schalten Sie den Computer ein.

7. MultiPoint Services wird gestartet. Befolgen Sie die Anweisungen, die auf dem Videomonitor der neuen Station angezeigt werden, um die Geräte der neuen Station zuzuordnen.

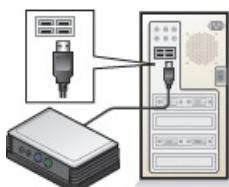
#### **So richten Sie eine Station mit einem Multifunktionshub ein**

1. Bevor eine neue Station angeschlossen werden kann, beenden Sie alle Benutzersitzungen, und fahren Sie dann den Computer sowie alle anderen eingeschalteten Geräte in Ihrem MultiPoint Services-System herunter.

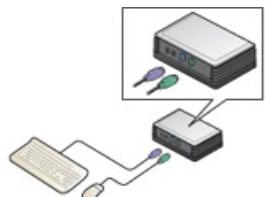
2. Schließen Sie das Kabel des neuen Videomonitors wie in der folgenden Abbildung gezeigt am DVI- oder VGA-Videoanzeigenschluss des Multifunktionshubs an:



3. Schließen Sie den neuen Multifunktionshub an einem freien USB-Anschluss des Computers an:



4. Schließen Sie eine Tastatur und eine Maus an den PS2- oder USB-Anschluss des Multifunktionshubs an:



5. Stecken Sie das Stromkabel des Videomonitors in eine Steckdose.

6. Schalten Sie den Computer ein.

7. MultiPoint Services wird gestartet. Wenn Sie dazu aufgefordert werden, befolgen Sie die Anweisungen, die auf dem Videomonitor der neuen Station angezeigt werden, um die Geräte der neuen Station

*zuzuordnen.*

## Weitere Informationen

- [Beenden einer Benutzersitzung](#)
- [Neustarten oder Herunterfahren](#)
- [Verwalten der Stationshardware](#)
- [Arbeiten mit USB-Geräten](#)

# Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers

09.04.2020 • 2 minutes to read • [Edit Online](#)

Im Multipoint-Manager können Sie die Registerkarte **Start** verwenden, um Multipoint Services-Tasks auszuführen und den Status des Systems zu überprüfen. Zu den Aufgaben, die Sie auf der Registerkarte **Start** ausführen können, gehören unter anderem:

- Bearbeiten der bei der MultiPoint Services-Installation ausgewählten Einstellungen, wie im Thema [Bearbeiten von Servereinstellungen](#) beschrieben.
- Neustarten oder Herunterfahren des Computers, einschließlich der *Benutzersitzungen*, wie im Thema [Neustart oder Herunterfahren](#) beschrieben.
- Wechseln der Modi, um verschiedene Verwaltungsaufgaben auszuführen, wie im Thema [Wechseln zwischen Modi](#) beschrieben.
- Aktivieren oder Deaktivieren des Datenträgerschutzes, wie im Thema [Aktivieren oder Deaktivieren des Datenträgerschutzes](#) beschrieben.
- Neuzuordnen aller Stationen, wie im Thema [Neuzuordnen aller Stationen](#) beschrieben.
- Hinzufügen oder Entfernen von Computern, wie im Thema [Hinzufügen oder Entfernen von Computern](#) beschrieben.

## Weitere Informationen

[Bearbeiten von Servereinstellungen](#)

[Neustarten oder Herunterfahren](#)

[Wechseln zwischen Modi](#)

[Aktivieren oder Deaktivieren des Datenträgerschutzes](#)

[Neuzuordnen aller Stationen](#)

[Computer hinzufügen oder entfernen](#)

# Bearbeiten von Servereinstellungen

09.04.2020 • 6 minutes to read • [Edit Online](#)

Während der Installation von MultiPoint Services haben Sie Einstellungen für das System konfiguriert, einschließlich Einstellungen für die Teilnahme an bestimmten Programmen. In diesem Thema werden die Einstellungen, die Sie für das MultiPoint Services-System festlegen können, und die Möglichkeiten zu ihrer Bearbeitung beschrieben.

## Informationen zu MultiPoint Services-Einstellungen

In der folgenden Tabelle werden die verschiedenen Einstellungen für das MultiPoint Services-System beschrieben, die Sie ändern können.

MULTIPOINT SERVICES-EINSTELLUNG	BESCHREIBUNG
Zulassen mehrerer Sitzungen für ein Konto	Erlaubt einem einzelnen Benutzerkonto, gleichzeitig an mehreren Stationen angemeldet zu sein. Dies kann z.B. in Situationen wie Schulungen nützlich sein, in denen alle Teilnehmer gemeinsam ein einziges Konto verwenden. Mithilfe dieser Einstellung stehen alle Änderungen an den Kontoressourcen, wie Dokumentordner oder der Desktop, allen mit dem gleichen Konto angemeldeten Benutzern zur Verfügung.
Eine Remoteverwaltung dieses Computers erlauben	Ermöglicht die Verwaltung des Computers, auf dem Multipoint Services ausgeführt wird, von anderen Multipoint-Systemen im Netzwerk. Wenn diese Option ausgewählt ist und sich der verwaltende Computer auf dem gleichen Subnetz befindet, erscheint dieser Computer in der Liste der verfügbaren zu verwaltenden Server. Wenn diese Option ausgewählt ist und sich der verwaltende Computer auf einem anderen Subnetz befindet, kann der verwaltende Computer diesen Computer trotzdem verwalten, Sie müssen jedoch die IP-Adresse des Computers angeben.
Überwachung der Desktops dieses Computers zulassen	Ermöglicht Ihnen, festzulegen, ob Desktops auf dem MultiPoint Services-System überwacht werden können. Wenn diese Einstellung deaktiviert (nicht ausgewählt) ist, werden Desktops von Stationen (sowohl lokal als auch Remote), die mit dem Computer verbunden sind, auf dem Multipoint Services ausgeführt wird, nicht auf der Registerkarte Start von Multipoint Manager angezeigt (auch auf einem anderen Computer, wenn der Computer remote verwaltet wird).
Immer im Konsolenmodus starten	Aktiviert die RemoteFX-Technologie, die darauf ausgelegt ist, durch das Auslagern von Prozessen auf die CPU und die GPU schnellere und effizientere Remotedesktopsitzungen zu ermöglichen. Wenn Sie mithilfe eines remotefx-fähigen Clients eine Verbindung mit Multipoint Services herstellen, können Sie mit dieser Option möglicherweise eine bessere Leistung erzielen. Die Vorteile richten sich nach den Fähigkeiten Ihres Servers und Netzwerks. Ein Aspekt beispielsweise ist, ob für die zusätzliche Verarbeitung zum Komprimieren des Datenstroms weniger Zeit erforderlich ist, als durch das Übertragen einer kleineren Datenmenge eingespart wird.

MULTIPOINT SERVICES-EINSTELLUNG	BESCHREIBUNG
Datenschutzerklärung nicht bei der ersten Anmeldung des Benutzers anzeigen	Wenn ein Benutzer sich zum ersten Mal an einer MultiPoint-Station anmeldet, wird eine Benachrichtigung angezeigt, die den Benutzer darüber informiert, dass die auf der Station ausgeführten Aktivitäten möglicherweise überwacht werden.
Zuweisen einer eindeutigen IP zu jeder Station	Weist jeder Station eine eindeutige IP-Station zu. Standardmäßig verfügt MultiPoint Services über eine IP-Adresse, die von allen auf dem System ausgeführten Sitzungen gemeinsam verwendet wird. Diese Konfiguration kann jedoch einige Probleme mit der Anwendungskompatibilität verursachen. Wenn eine Anwendung z.B. eine eindeutige IP-Adresse benötigt, wird die Anwendung in MultiPoint Services möglicherweise nicht ordnungsgemäß ausgeführt. Durch das Aktivieren dieser Option, auch als IP-Virtualisierung bezeichnet, kann dieses Problem behoben werden.  Die IP-Virtualisierung ist auch für das Überwachen von aktiven Sitzungen in MultiPoint Services nützlich. Einige Überwachungstools melden Nutzungsinformationen anhand der IP-Adresse. Zum Aktivieren der Sitzungsüberwachung können Sie in diesen Fällen die IP-Virtualisierung verwenden, um jeder Sitzung eine eindeutige IP-Adresse zuzuweisen. Hinweis: Wenn Sie diese Option aktivieren, erhält jede neue Sitzung eine eindeutige IP-Adresse. Alle vorhandenen Sitzungen verwenden weiterhin die gemeinsam genutzte IP-Adresse, bis sie abgemeldet und erneut angemeldet werden.
Chatunterhaltungen zwischen dem MultiPoint-Dashboard und einer Benutzersitzung auf diesem Computer zulassen	Ermöglicht Chats zwischen einem Benutzer im MultiPoint-Manager und einem Benutzer in einer Benutzersitzung auf diesem Computer. Weitere Informationen finden Sie unter <a href="#">Kommunizieren mit Chat</a> .
Orchestrierung von Administrator- und MultiPoint- Dashboard-Benutzersitzungen zulassen	Ermöglicht bei Aktivierung Administratoren die Verwendung des MultiPoint-Dashboards für die Orchestrierung von Sitzungen. Diese Sitzungen werden als Miniaturansichten angezeigt.
Stationen die Verwendung von GPU-Hardwarerendering ermöglichen	Steuert, ob Stationen die GPU des Systems verwenden können.

## Bearbeiten der Computereinstellungen

- Öffnen Sie den Multipoint-Manager im [Stations Modus](#), und klicken Sie dann auf die Registerkarte **Start**.
- Klicken Sie in der Spalte **Computer** auf den Computernamen, und klicken Sie dann unter *Computername* **Tasks auf Computereinstellungen bearbeiten**.
- Aktivieren oder löschen Sie die Elemente, die Sie ändern möchten, und klicken Sie dann auf **OK**.

## Weitere Informationen

[Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)

# Neustart oder Herunterfahren von MultiPoint-Systemen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Sie können ein Multipoint Services-System oder mehrere Multipoint Services-Systeme im Multipoint-Dashboard neu starten oder Herunterfahren.

## Neustarten eines Multipoint Services-Systems oder mehrerer Systeme

1. Klicken Sie auf **Systeme**.
2. Klicken Sie auf das Miniaturbild des Servers, den Sie neu starten möchten, und klicken Sie dann auf der Registerkarte **Hardware** auf **neu starten**.

## So fahren Sie ein oder mehrere MultiPoint Service-System herunter

1. Klicken Sie auf die Registerkarte **Systeme**.
2. Klicken Sie auf das Miniaturbild des Servers, den Sie neu starten möchten, und klicken Sie dann auf der Registerkarte **Hardware** auf **herunterfahren**.

# Wechseln zwischen Modi

09.04.2020 • 2 minutes to read • [Edit Online](#)

Der Multipoint-Manager umfasst die folgenden Modi, die Ihnen bei der Ausführung verschiedener Typen der Multipoint Services-Systemverwaltung helfen:

- *Stationsmodus*: Das MultiPoint Server-System wird standardmäßig im Stationsmodus gestartet. Im Stationsmodus weisen die MultiPoint Server-Stationen folgendes Verhalten auf: Jede Station wird als separater Computer mit Windows ausgeführt, und das System kann von mehreren Benutzern gleichzeitig verwendet werden. Sie und Ihre Benutzer können Dateien freigeben und die erforderlichen Aufgaben erledigen.
- *Konsolenmodus*: Wenn sich das MultiPoint Server-System im Konsolenmodus befindet, können Sie Software und Treiber installieren und aktualisieren oder andere Wartungsaufgaben ausführen. Im Konsolenmodus sind keine anderen *Stationen* zur Verwendung durch andere Computerbenutzer verfügbar. Solche Stationen werden nicht im Multipoint-Manager angezeigt. Alle Monitore, die direkt mit dem Server verbunden sind, werden als Anzeige dieses Computer Systems behandelt.

## NOTE

Um den Start des Systems im Konsolenmodus zu erzwingen, ändern Sie die Standardeinstellung in den Einstellungen für den Server.

## So wechseln Sie aus dem Stationsmodus in den Konsolenmodus

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Start**.
2. Klicken Sie in der Spalte **Computer** auf den Computer, für den Sie den Modus ändern möchten.
3. Klicken Sie unter *Computernamen Tasks* auf **zum Konsolenmodus wechseln**. Der Computer wird neu gestartet, und keine Station ist mehr verfügbar.

## So wechseln Sie aus dem Konsolenmodus in den Stationsmodus

1. Öffnen Sie den Multipoint-Manager im Konsolenmodus, und klicken Sie dann auf die Registerkarte **Start**.
2. Klicken Sie in der Spalte **Computer** auf den Computer, für den Sie den Modus ändern möchten.
3. Klicken Sie unter *Computernamen Tasks* auf **in den Stations Modus wechseln**. Der Computer wird neu gestartet, und alle Stationen sind verfügbar.

## Weitere Informationen

[Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)

# Aktivieren oder Deaktivieren des Datenträgerschutzes

09.04.2020 • 2 minutes to read • [Edit Online](#)

Mit der Datenträgerschutz-Funktion können Sie das MultiPoint Services-System bei jedem Neustart des Systems auf einen bestimmten Status zurücksetzen. Mithilfe des Datenträgerschutzes können Benutzer temporär Änderungen am MultiPoint Services-System vornehmen. Die Änderungen werden dann bei einem Neustart des Servers verworfen. Beispiele für Änderungen, die bei einem Neustart des Servers verworfen werden, sind das Personalisieren des Profils eines Benutzers, das Speichern von Dateien, das Ändern von Einstellungen oder das Installieren von Anwendungen.

## Aktivieren des Datenträger Schutzes

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Start**, und klicken Sie dann unter \* Computername **\*Tasksauf Datenträger Schutz aktivieren**.
2. Überprüfen Sie die Informationen, und klicken Sie dann auf **OK**.

Nach dem Systemneustart werden alle am System vorgenommenen Änderungen, u.a. neu installierte Anwendungen, bei jedem nachfolgenden Neustart verworfen.

## Datenträger Schutz deaktivieren

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Start**, und klicken Sie dann unter \* Computername **\*Tasksauf Datenträger Schutz deaktivieren**.
2. Überprüfen Sie die Informationen, und klicken Sie dann auf **OK**.

Nach dem Systemneustart sind alle am System vorgenommenen Änderungen, u.a. auf dem Server installierte Anwendungen, dauerhaft und werden beim nächsten Systemneustart nicht verworfen.

# Verwalten der Clientzugriffslizenzen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Jede Station, die eine Verbindung mit einem Multipoint Services-System herstellt, einschließlich des Computers, auf dem Multipoint Services ausgeführt wird und als Station verwendet wird, muss über eine gültige benutzerspezifische Remotedesktop *Client Zugriffslicenz (CAL)* verfügen.

Wenn Sie virtuelle Station-Desktops anstelle physischer Stationen verwenden, müssen Sie für jeden virtuellen Computer der Station eine Client Zugriffslicenz (CAL) installieren.

1. Erwerben Sie eine Client Lizenz für jede Station, die mit Ihrem Multipoint Services-Computer oder-Server verbunden ist. Weitere Informationen zum Erwerb von CALs finden Sie in der Dokumentation zur Remotedesktop Lizenzierung.
2. Öffnen Sie auf dem **Start** Bildschirm den **Multipoint-Manager**.
3. Klicken Sie auf die Registerkarte **Start**, und klicken Sie dann auf **Client Zugriffs Lizenzen hinzufügen**. Dadurch wird das Verwaltungs Tool für die CAL-Lizenzierung geöffnet.

## Manuelles Festlegen des Lizenzierungs Modus

Wenn diese Einstellung nicht ordnungsgemäß konfiguriert ist, wird bei der Einrichtung von Multipoint Services eine Benachrichtigung über den Ablauf der Toleranz Periode angezeigt. Führen Sie diese Schritte aus, um den Lizenzierungs Modus festzulegen:

1. Starten Sie **Editor für lokale Gruppenrichtlinien** (gpeer dit.msc).
2. Navigieren Sie im linken Bereich zu " **lokaler Computer Richtlinien-> Computer Konfiguration-> Administrative Vorlagen-> Windows-Komponenten-> Remotedesktopdienste> Remotedesktop-Sitzungshost >-Lizenzierung**".
3. Klicken Sie im rechten Bereich mit der rechten Maustaste auf **die angegebenen Remotedesktop Lizenzserver verwenden**, und wählen Sie dann **Bearbeiten** aus:
  - Wählen Sie im Dialogfeld Gruppenrichtlinien-Editor die Option **aktiviert** aus.
  - Geben Sie im Feld **zu verwendende Lizenzserver** den Namen des lokalen Computers ein.
  - **OK** auswählen
4. Klicken Sie im rechten Bereich mit der rechten Maustaste auf **Remotedesktop Lizenzierungs Modus festlegen**, und wählen Sie **Bearbeiten** aus.
  - Wählen Sie im Dialogfeld Gruppenrichtlinien-Editor die Option **aktiviert** aus.
  - Legen Sie den **Lizenzierungs Modus** auf pro Gerät/pro Benutzer fest.
  - **OK** auswählen

## Weitere Informationen

[Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)

# Neuzuordnen aller Stationen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Das Neuzuordnen von Stationen ermöglicht das Zuweisen von Tastaturen und Mäusen zu Monitoren. Wenn Sie alle Stationen neu zuordnen, werden die ursprünglichen Einstellungen, wie z. B. Name und Informationen zur automatischen Anmeldung, gelöscht. Während der Neuzuordnung werden alle lokalen Benutzerstationen angehalten.

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Start**.
2. Klicken Sie unter **Aufgaben** auf **Alle Stationen neu zuordnen**.
3. Befolgen Sie die Anweisungen auf den Stationsbildschirmen, um die Tastaturen den Stationen innerhalb Ihres Systems zuzuordnen.

# Speichern der Verbindungseinstellungen in einer Datei

09.04.2020 • 2 minutes to read • [Edit Online](#)

Mithilfe von Remotedesktop können Sie von einem anderen Computer eine Verbindung mit einem MultiPoint Services-System herstellen. Wenn der Remotecomputer das Remotedesktopprotokoll unterstützt, kann die Verbindung mit dem Computer automatisch hergestellt werden.

Sie können drei Arten von Verbindungsdateien erstellen:

- **Multipoint-Manager-Verbindungs Datei:** ermöglicht das Ausführen von Multipoint Manager auf einem anderen Computer als Remote Anwendung.
- **Multipoint-dashboardverbindungsdatei:** ermöglicht das Ausführen eines Multipoint-Dashboards auf einem anderen Computer als Remote Anwendung.
- **Remotestation-Verbindungsdatei:** Ermöglicht es einem anderen Computer, als Remotestation eine Verbindung mit dem MultiPoint Services-System herzustellen.

## So speichern Sie Systemverbindungeinstellungen in einer Datei

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Start**.
2. Klicken Sie in der Spalte **Computer** auf den Namen des Computers, für den Sie die Verbindungeinstellungen in einer Datei speichern möchten.
3. Klicken Sie unter \* ComputerTasksName \* Tasks auf **Verbindungen in Datei speichern**. Die Seite **Verbindungeinstellungen in einer Datei speichern** wird angezeigt.
4. Wählen Sie die Art der Verbindungsdatei aus, die Sie erstellen möchten, und klicken Sie dann auf **OK**.
5. Wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll, bearbeiten Sie ggf. den Namen im Feld **Dateiname**, und klicken Sie dann auf **Speichern**.

# Hinzufügen oder Entfernen von Computern

09.04.2020 • 3 minutes to read • [Edit Online](#)

Mithilfe des Multipoint-Managers können Sie weitere Computer hinzufügen oder Computer aus dem Multipoint Services-System entfernen. Indem Sie andere PCs zum MultiPoint-Manager hinzufügen, können Sie die Sitzungen von Benutzern über das MultiPoint-Dashboard orchestrieren, wenn Sie an diesem PC angemeldet sind – auf die gleiche Weise wie für MultiPoint-Stationen.

## So fügen Sie Server in MultiPoint hinzu oder entfernen diese

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Start**.
2. Klicken Sie unter *Computernamen* Tasks auf **Multipoint-Server hinzufügen oder entfernen**. Der Bildschirm zum **Hinzufügen oder Entfernen von Multipoint-Servern** wird gestartet und beginnt mit der Ermittlung anderer Server im Subnetz des lokalen Netzwerks, die mit Multipoint Manager verwaltet werden können.
3. Führen Sie eine der folgenden Aktionen aus:
  - **So fügen Sie einen Server hinzu:** Klicken Sie in der Liste **verfügbar** auf einen Server, den Sie mit Multipoint Manager verwalten möchten, und klicken Sie dann auf **Hinzufügen**. Wenn sich das Administratorbenutzerkonto und -kennwort für den Server von dem Konto unterscheiden, mit dem Sie aktuell angemeldet sind, werden Sie aufgefordert, die entsprechenden Kontoinformationen anzugeben.
  - **Hinzufügen eines Servers, der nicht zum Subnetz gehört:** Geben Sie in das Feld **MultiPoint Server-Name** den Namen des Servers ein, den Sie hinzufügen möchten, und klicken Sie dann auf **Manuell hinzufügen**.
  - **Entfernen eines Servers:** Klicken Sie in der Liste **Verwaltet** auf einen Server, den Sie aus der Verwaltung entfernen möchten, und klicken Sie dann auf **Entfernen**.

## So fügen Sie weitere Computer hinzu oder entfernen diese

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Start**.
2. Klicken Sie unter **Startaufgaben** auf **PCs hinzufügen oder entfernen**. Der Bildschirm zum **Hinzufügen oder Entfernen persönlicher Computer** wird gestartet und beginnt mit der Ermittlung anderer Computer im Subnetz des lokalen Netzwerks, die mit Multipoint Services verwaltet werden können.
3. Führen Sie eine der folgenden Aktionen aus:
  - **So fügen Sie einen Computer hinzu:** Klicken Sie in der Liste **verfügbar** auf einen Computer, den Sie mit Multipoint Services verwalten möchten, und klicken Sie dann auf **Hinzufügen**. Wenn Sie einen Computer hinzufügen, werden Sie aufgefordert, die Kontoinformationen bereitzustellen.
  - **Hinzufügen eines Computers, der nicht zum Subnetz gehört:** Geben Sie in das Feld **PC-Name** den Namen des Computers ein, den Sie hinzufügen möchten, und klicken Sie dann auf **Manuell hinzufügen**.
  - **Entfernen eines Computers:** Klicken Sie in der Liste **Verwaltet** auf einen Computer, den Sie aus der Verwaltung entfernen möchten, und klicken Sie dann auf **Entfernen**.

## Weitere Informationen

[Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)

[Bearbeiten von Servereinstellungen](#)

# Verwalten von Benutzerstationen

09.04.2020 • 4 minutes to read • [Edit Online](#)

Dieser Abschnitt behandelt die Verwaltung der *Stationen*, aus denen das MultiPoint Services-System besteht. Die Verwaltung eines Multipoint Services-Systems umfasst die Verwaltung der Hardware- und Softwarekomponenten von Multipoint Manager. In einem Multipoint Services-System ist ein Desktop die Software Benutzeroberfläche, die auf dem Monitor für jede Benutzer Station angezeigt wird.

## Stationsstatus

Sie können die folgenden Arten von Status für jeden Desktop auf der Registerkarte **Stationen** anzeigen. der Status umfasst Folgendes:

- Angemeldete Benutzer
- Benutzersitzungen, die angehalten, aber auf dem Computer noch aktiv sind
- Verwendete Stationen mit Benutzern

Weitere Informationen zur Anzeige des Desktopstatus finden Sie im Thema [Anzeigen des Benutzerverbindungsstatus](#).

### TIP

Sie können jeder Station Anzeigenamen zuweisen, wodurch Sie die Stationen leichter identifizieren können. Verwenden Sie **Identify station** (Station identifizieren), um den Stationsname auf dem zugewiesenen Bildschirm anzuzeigen.

## Unterschiedliche Arten zum Abmelden von Standardbenutzern vom MultiPoint Services-System

Als *Administrator* können Sie Windows jederzeit abmelden, ohne dass dies Auswirkungen auf aktive Benutzer in Ihrem MultiPoint Services-Systems hat. *Standardbenutzer* können ihre Sitzung *trennen* oder das MultiPoint Services-System ebenfalls *abmelden*. Wenn ein Benutzer seine Arbeit beendet und den Computer verlässt, sollte er seine Arbeit auf dem Computer oder einem externen Speichergerät speichern, damit er nach dem Herunterfahren des MultiPoint Services-Systems seine gespeicherte Arbeit an einem anderen Tag wieder abrufen kann.

Als Administrator müssen Sie möglicherweise die *Sitzung* eines Standard Benutzers beenden, anstatt den Benutzer abzumelden. Eine Standardbenutzer Sitzung kann auf zwei Arten beendet werden:

- Beenden Sie die Sitzung, und melden Sie den Benutzer ab. Weitere Informationen zum Beenden der Sitzung eines Benutzers finden Sie im Thema [Beenden einer Benutzersitzung](#) .
- Sperren Sie den Benutzer, um die Sitzung des Benutzers vorübergehend zu beenden, behalten Sie jedoch die aktive Sitzung im Computerspeicher des Multipoint Services-Systems bei. Der angehaltene Benutzer kann dann von derselben oder einer anderen Station aus wieder eine Verbindung mit der Sitzung herstellen und seine Arbeit fortsetzen. Weitere Informationen zum Anhalten der Sitzung eines Benutzers finden Sie im Thema [anhalten und verlassen der Benutzersitzung](#) .

## Festlegen der automatischen Anmeldung für eine Station

Als Administrator können Sie für eine oder mehrere Station(en) die automatische Anmeldung beim Starten des Computers festlegen, auf dem MultiPoint Services ausgeführt werden. Weitere Informationen zur automatischen Anmeldung finden Sie im Thema [Einrichten einer Station für die automatische Anmeldung](#).

## Teilen einer Station

Jeder Stationsmonitor mit einer Auflösung von mehr als 1024x768 kann in zwei Stationen geteilt werden. Weitere Informationen zum Teilen einer Station finden Sie im Thema [Teilen einer Benutzerstation](#).

## Weitere Informationen

[Anzeigen des Benutzerverbindungsstatus](#)

[Abmelden oder Trennen von Benutzersitzungen](#)

[Aussetzen und Benutzersitzung aktiv lassen](#)

[Einrichten einer Station für die automatische Anmeldung](#)

[Beenden einer Benutzersitzung](#)

[Teilen einer Benutzerstation](#)

# Anzeigen des Benutzerverbindungsstatus

09.04.2020 • 2 minutes to read • [Edit Online](#)

Verwenden Sie die Registerkarte **Stationen**, um den Status einer Verbindung zwischen einem Standard-oder einem anderen Administrator und einer Multipoint Services-Station zu ermitteln.

Der Status kann folgende Werte aufweisen:

- **Angemeldet:** Eine Benutzersitzung ist auf einer Station aktiv.
- **Angehalten:** Eine Benutzersitzung ist angehalten, auf dem Computer aber noch aktiv. Die Desktop Sitzung des Benutzers bleibt erhalten, bis der Benutzer sich erneut anmeldet.
- **Abgemeldet:** Ein abgemeldeter Benutzer wird auf der Registerkarte **Stationen** nicht angezeigt.

Öffnen Sie zum Anzeigen des Stations Status den Multipoint-Manager im Stations Modus, und klicken Sie dann auf **Stationen**.

## Weitere Informationen

[Verwalten von Benutzer Desktops](#)

[Wechseln zwischen Modi](#)

# Abmelden oder Trennen von Benutzersitzungen

09.04.2020 • 3 minutes to read • [Edit Online](#)

MultiPoint Services-Benutzer können sich an ihren Desktopsitzungen anmelden und davon abmelden wie bei jeder anderen Windows-Sitzung auch. Benutzer können Ihre Sitzung auch trennen oder aussetzen, sodass die Multipoint Services-Station nicht verwendet wird, aber Ihre Sitzung bleibt im Arbeitsspeicher des Multipoint Services-Systems aktiv.

Darüber hinaus können Administratoren die Sitzung eines Benutzers beenden, wenn der Benutzer von der Multipoint Services-Sitzung entfernt wurde oder vergessen hat, sich vom System abzumelden.

## Abmelden oder Trennen einer Sitzung

In der folgenden Tabelle werden verschiedene Möglichkeiten beschrieben, mit deren Hilfe Sie bzw. andere Benutzer eine Sitzung abmelden, anhalten oder beenden können.

Aktion	Entsprechende
Klicken Sie auf <b>Start</b> , klicken Sie auf Einstellungen, klicken Sie auf den Benutzernamen (obere rechte Ecke), und klicken Sie dann auf <b>Abmelden</b> .	Die Sitzung wird beendet, und die Station steht für alle Benutzer zur Anmeldung zur Verfügung.
Klicken Sie auf <b>Start</b> , auf <b>Einstellungen</b> , auf „Ein/Aus“ und dann auf <b>Trennen</b> .	Ihre Sitzung wird getrennt und bleibt im Arbeitsspeicher des Computers erhalten. Die Station steht für denselben sowie andere Benutzer zur Anmeldung zur Verfügung.
Klicken Sie auf <b>Start</b> , klicken Sie auf Einstellungen, klicken Sie auf den Benutzernamen (obere rechte Ecke), und klicken Sie dann auf <b>Sperren</b> .	Die Station ist gesperrt, und Ihre Sitzung bleibt im Arbeitsspeicher des Computers erhalten.

## Anhalten oder Beenden der Sitzung eines Benutzers

In der folgenden Tabelle werden die verschiedenen Optionen beschrieben, die Sie als Administrator zum Trennen oder Beenden der Sitzung eines Benutzers verwenden können.

Aktion	Entsprechende
<b>Aussetzen:</b> Verwenden Sie im Multipoint-Manager die Registerkarte <b>Stationen</b> , um die Sitzung des Benutzers anzuhalten. Weitere Informationen finden Sie im Thema <a href="#">Anhalten von Benutzersitzungen im aktiven Zustand</a> .	Die Sitzung des Benutzers wird beendet und im Arbeitsspeicher des Computers beibehalten. Die Station steht für denselben sowie andere Benutzer zur Anmeldung zur Verfügung. Der Benutzer kann sich an derselben oder einer anderen Station anmelden und seine Arbeit fortsetzen.
<b>Ende:</b> Verwenden Sie im Multipoint-Manager die Registerkarte <b>Stationen</b> , um die Benutzersitzung zu beenden. Sie können auch alle Benutzersitzungen auf der Registerkarte <b>Stationen</b> beenden. Weitere Informationen finden Sie im Thema <a href="#">Beenden einer Benutzersitzung</a> .	Die Sitzung des Benutzers wird beendet, und die Station steht für alle Benutzer zur Verfügung. Die Sitzung des Benutzers wird nicht mehr auf der Registerkarte <b>Stationen</b> angezeigt, und Sie befindet sich nicht im Arbeitsspeicher des Computers.

## Weitere Informationen

[Aussetzen und Benutzersitzung aktiv lassen](#)

[Beenden einer Benutzersitzung](#)

[Verwalten von Benutzer Desktops](#)

[Abmelden von Benutzersitzungen](#)

# Anhalten von Benutzersitzungen im aktiven Zustand

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie die Sitzungen der Benutzer nicht beenden möchten, können Sie die Verbindung zwischen Benutzern und dem Multipoint Services-System trennen oder aussetzen. Ein Benutzer kann eine Sitzung auch selbst trennen. Während eine Benutzersitzung angehalten wird, bleibt die Sitzung im Arbeitsspeicher des Multipoint Services-Systems aktiv, bis der Computer heruntergefahren oder neu gestartet wird. Zu diesem Zeitpunkt werden alle angehaltenen Sitzungen beendet, und sämtliche nicht gespeicherte Arbeit geht verloren.

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Stationen**.
2. Klicken Sie in der Spalte **Computer** auf den Namen des Computers, dessen Sitzungen Sie anhalten möchten.
3. Klicken Sie unter **Stationsaufgaben** auf **Alle Stationen anhalten**.

Nachdem eine Benutzersitzung angehalten wurde, kann sich der Benutzer an derselben oder einer anderen Station anmelden und seine Arbeit in der ursprünglichen Sitzung fortsetzen.

## Weitere Informationen

[Verwalten von Benutzer Desktops](#)

[Abmelden oder Trennen von Benutzersitzungen](#)

# Beenden einer Benutzersitzung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Sie sollten die Sitzung eines Benutzers beenden, wenn Sie den Benutzer aus dem MultiPoint Services-System abmelden müssen, um den Desktop auf seine Standardeinstellungen zurückzusetzen. Dem Benutzer wird eine Warnung angezeigt, dass die Verbindung beendet wird. Sie sollten die Verbindung eines Benutzers beenden, wenn Sie Folgendes tun möchten:

- Neustart des MultiPoint Services-Systemcomputers
- Herunterfahren des MultiPoint Services-Systemcomputers
- Moduswechsel
- Abmelden eines Benutzers, der vergessen hat, sich abzumelden

Endbenutzer Sitzungen:

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Stationen**.
2. Führen Sie eine der folgenden Aktionen aus:
  - Wählen Sie zum Beenden einer einzelnen Benutzersitzung in der Spalte **Benutzer** die zu beendende Sitzung aus, und klicken Sie dann unter **Aufgaben** auf **Abmelden**.
  - Klicken Sie zum Beenden aller Benutzersitzungen unter **Stationsaufgaben** auf **Alle Stationen abmelden**.

## Weitere Informationen

[Verwalten von Benutzer Desktops](#)

[Abmelden oder Trennen von Benutzersitzungen](#)

# Einrichten einer Station für das automatische Anmelden

09.04.2020 • 2 minutes to read • [Edit Online](#)

Bei der automatischen Anmeldung kann jede Station automatisch angemeldet werden, wenn der Computer, auf dem Multipoint Services ausgeführt wird, gestartet wird und der Desktop angezeigt wird. Administratoren können dieses Feature für einzelne oder für alle Stationen festlegen.

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Stationen**.
2. Klicken Sie auf den Namen der Station, für die das automatische Anmelden festgelegt werden soll.
3. Klicken Sie unter **Aufgaben** auf **Station konfigurieren**. Die Seite **Stationen konfigurieren** wird geöffnet.
4. Wählen Sie **mit den folgenden Informationen die Option automatische Anmeldung aus**, und geben Sie dann einen **Benutzerkonto** Namen ein.
5. Geben Sie das Kennwort für das Benutzerkonto ein, und geben Sie das Kennwort erneut ein, um es zu bestätigen.
6. Klicken Sie auf **OK**. Die Seite wird geschlossen. Der Kontoname wird in der Spalte für die **automatische Anmeldung** angezeigt.

## Weitere Informationen

[Verwalten von Benutzerstationen](#)

# Teilen einer Benutzerstation

09.04.2020 • 2 minutes to read • [Edit Online](#)

Jeder Multipoint Services-Stations Monitor mit einer Auflösung von mehr als 1024 x 768 kann mithilfe der Aufgabe **Split Station** auf der Registerkarte **Stationen** in zwei Stationen aufgeteilt werden. Der Desktop, der zum Zeitpunkt der Aufteilung auf dem Monitor vorhanden ist, wechselt zur linken Hälfte des Monitors, und auf der rechten Hälfte desselben Monitors wird eine neue Station erstellt. Der neuen Station müssen eine Tastatur, eine Maus und ein USB-Hub zugeordnet werden, um die Erstellung abzuschließen. Nach dem Teilen einer Station kann sich ein Benutzer auf der linken Station anmelden, während sich ein anderer Benutzer auf der rechten Station anmeldet.

Die Verwendung einer Split-Screen-Station kann Folgendes umfassen:

- Verringerung von Kosten und Raumbedarf durch Unterbringung einer größeren Studentenzahl auf einem MultiPoint Server-System
- Gleichzeitige Zusammenarbeit zwischen zwei Studenten und einem Projekt
- Möglichkeit für einen Lehrer, ein Verfahren auf einer Station vorzuführen, während ein Student die Aktionen auf der anderen Station nachvollzieht

## NOTE

Wenn Sie eine Station teilen, wird die aktive Sitzung auf der Station angehalten. Der Benutzer muss sich erneut bei der Station anmelden, um die Arbeit wieder aufzunehmen, nachdem die Teilung erfolgt ist.

## So teilen Sie eine Station:

1. Klicken Sie im Multipoint-Manager im Stations Modus auf die Registerkarte **Stationen**.
2. Klicken Sie in der Spalte **Station** auf den Namen der Station, die Sie teilen möchten.
3. Klicken Sie unter **Stationsaufgaben** auf **Station teilen**.

## So kehren Sie eine geteilte Station an eine einzelne Station zurück:

1. Klicken Sie im Multipoint-Manager im Stations Modus auf die Registerkarte **Stationen**.
2. Klicken Sie in der Spalte **Station** auf den Namen der Station, deren Teilung Sie aufheben möchten.
3. Klicken Sie unter **Stationsaufgaben** auf **Stationsteilung aufheben**.

## Weitere Informationen

[Verwalten von Benutzerstationen](#)

# Verwalten von Benutzerkonten

09.04.2020 • 2 minutes to read • [Edit Online](#)

In diesem Abschnitt werden die verschiedenen Typen von Benutzerkonten sowie das Erstellen und Verwalten von Benutzerkonten beschrieben. In einem Multipoint Services-System gibt es zwei Arten von Benutzerkonten: *Standardbenutzer Konten* und *Administrator Konten*, wie unten beschrieben.

## TIP

Das Thema [Überlegungen zu Benutzerkonten](#) enthält Richtlinien, die Sie beim Erstellen und Verwalten von Benutzerkonten berücksichtigen sollten.

# Überlegungen zu Benutzerkonten

09.04.2020 • 4 minutes to read • [Edit Online](#)

In diesem Thema werden Probleme beschrieben, die von Ihnen als Administrator beim Erstellen und Verwalten von Benutzerkonten berücksichtigt werden sollten. Sie verwalten Benutzerkonten auf der Registerkarte Benutzer im Multipoint-Manager. Weitere Informationen finden Sie unter [Verwalten von Benutzerkonten](#).

## Typen von Benutzerkonten

Bei einem Benutzerkonto handelt es sich um eine Sammlung von Informationen, die Multipoint Services mitteilt, auf welche Dateien und Ordner ein Benutzer zugreifen kann, welche Änderungen Sie an dem Multipoint Services-System vornehmen können und welche Einstellungen für jeden Benutzer, wie z. B. Desktop Hintergrund. Jede Person greift mit einem eindeutigen Benutzernamen und einem Kennwort auf ihr eigenes Benutzerkonto zu. Multipoint Services unterstützt drei Arten von Benutzerkonten:

- **Administrator Konten** sind für Personen gedacht, die den Multipoint-Manager verwenden, um das Multipoint Services-System zu verwenden und zu verwalten. Weitere Informationen finden Sie unter [Erstellen eines Administratorkontos](#).
- **Standardbenutzerkonten** sind für Personen gedacht, die regelmäßig auf Stationen zugreifen, das System aber nicht verwalten. Normalerweise werden für die meisten Benutzer des MultiPoint Services-Systems Standardbenutzerkonten erstellt. Weitere Informationen finden Sie unter [Erstellen eines Standardbenutzerkontos](#).
- **MultiPoint-Dashboardbenutzerkonten** sind für Personen gedacht, die Sitzungen von Standardbenutzern über das MultiPoint-Dashboard verwalten und die sich über jede Station anmelden können. Weitere Informationen finden Sie unter [Erstellen eines Kontos für MultiPoint-Dashboardbenutzer](#).

## Überlegungen zu Benutzernamen und Kennwörtern

Administratoren können Aufgaben ausführen, die sich auf alle anderen Benutzer des MultiPoint Services-Systems auswirken, wie z.B. die Installation von Software oder die Änderung von Sicherheitseinstellungen. Aus diesem Grund sollten Administratoren über eindeutige Benutzernamen und Kennwörter verfügen, die nur ihnen bekannt sind.

Ein wichtiger Aspekt von Benutzerkonten ist, dass jedem Benutzerkonto eine eindeutige **Dokumente**-Bibliothek in Windows-Explorer zugeordnet wird, die den Ordner **Eigene Dokumente** umfasst. Wenn die Standardbenutzer Ihres MultiPoint Services-Systems private Dokumente in ihrer jeweiligen **Dokumente**-Bibliothek in Windows-Explorer speichern, sollten sie sich beim MultiPoint Services-System ebenfalls mit einem eindeutigen Benutzernamen und Kennwort anmelden, das nur ihnen bekannt ist. Weitere Informationen zum Speichern von Dokumenten in Windows-Explorer finden Sie im Thema [Verwalten von Benutzerdateien](#).

### TIP

Um die Systemsicherheit zu verstärken, sollten alle Benutzer Kennwörter sichere Kenn Wörter sein. Ein sicheres Kennwort ist ein sicheres Kennwort, das nicht leicht erraten oder geknackt werden kann, mindestens acht Zeichen lang ist, den Kontonamen des Benutzers nicht ganz oder teilweise enthält und mindestens drei der vier folgenden Zeichen Kategorien enthält: Großbuchstaben, Kleinbuchstaben, Ziffern und Symbole, die auf einer Tastatur gefunden werden (z. B. !, @, #).

## Weitere Informationen

[Erstellen eines Administratorkontos](#)

[Erstellen eines Standardbenutzerkontos](#)

[Verwalten von Benutzer Dateien Verwalten von Benutzerkonten](#)

# Erstellen eines Administratorkontos

09.04.2020 • 3 minutes to read • [Edit Online](#)

Erstellen Sie *Administratorkonten* für diejenigen Benutzer, die das MultiPoint Services-System verwalten werden. Um zu ermitteln, wer über Administrator Zugriff verfügt, klicken Sie in Multipoint-Manager auf die Registerkarte **Benutzer**. administrative Benutzerkonten werden in der Spalte **Kontotyp** als **Administrator** angezeigt. Administratoren *haben Zugriff* auf alle Multipoint Manager-Aufgaben, die Desktop-und Systemeinstellungen ändern, wie z. B.:

- Erstellen von Konten
- Hinzufügen und Entfernen von Programmen
- Verwalten von *Desktops* und Hardware
- Beenden von *Sitzungen* anderer Benutzer

Administratoren können Aufgaben ausführen, die sich auf alle anderen Benutzer des MultiPoint Services-Systems auswirken, wie z.B. die Installation von Software oder die Änderung von Sicherheitseinstellungen. Aus diesem Grund sollten Administratoren über eindeutige Benutzernamen und Kennwörter verfügen, die nur ihnen bekannt sind.

Weitere Informationen zu Problemen, die Sie als Administrator beim Erstellen und Verwalten von Benutzerkonten berücksichtigen sollten, finden Sie im Thema [Überlegungen zu Benutzerkonten](#).

## NOTE

Sie können auch für sich selbst ein *Standardbenutzerkonto* erstellen, das Sie zur Ausführung von Aufgaben im MultiPoint Services-System verwenden können, die nicht mit der Verwaltung des MultiPoint Services-Systems in Zusammenhang stehen. In diesem Fall melden Sie sich nur dann bei Ihrem Administratorkonto an, wenn Systemverwaltungsaufgaben auszuführen sind.

## So erstellen Sie ein Administratorkonto

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Benutzer**.
2. Klicken Sie unter **Benutzeraufgaben** auf **Benutzerkonto hinzufügen**. Der Assistent **Benutzerkonto hinzufügen** wird geöffnet.
3. Geben Sie in das Feld **Benutzerkonto** einen Anmeldenamen für den Benutzer ein. Typischerweise besteht der Anmeldename des Benutzers aus dem Vor- und Nachnamen, die ohne Leerzeichen in einem Wort zusammengeschrieben werden, oder dem ersten Buchstaben des Vornamens und dem Nachnamen, die ohne Leerzeichen in einem Wort zusammengeschrieben werden.
4. Geben Sie in das Feld **Vollständiger Name** den Namen des Benutzers im gewünschten Format ein, z.B. Vorname, vollständiger Name oder Spitzname.
5. Geben Sie im Feld **Kennwort** ein Kennwort für den Benutzer ein. Dieses Kennwort sollte nur Ihnen und dem Benutzer bekannt sein und muss an einem sicheren Ort gespeichert werden. Das Kennwort kann nur von einem Administrator geändert werden.
6. Geben Sie das Kennwort im Feld **Kennwort bestätigen** erneut ein, und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Seite zum Festlegen der Zugriffsebene die Option **Administrator** aus, und klicken Sie dann auf **Weiter**.

8. MultiPoint Services überprüft alle Informationen und zeigt im Anschluss an die Einrichtung des Kontos eine Meldung an. Wenn der Text **Ein neues Benutzerkonto wurde erfolgreich erstellt** angezeigt wird, klicken Sie auf **Fertig stellen**.

# Erstellen eines Standardbenutzerkontos

09.04.2020 • 2 minutes to read • [Edit Online](#)

Erstellen Sie *Standardbenutzerkonten* für die Benutzer, die regelmäßig auf Stationen zugreifen, das MultiPoint Services-System aber nicht verwalten. Benutzer mit Standardbenutzer Konten können die meisten Anwendungen ausführen und Dateien speichern, aber nicht den Multipoint-Manager ausführen. Um festzustellen, wer über Standardbenutzer Zugriff verfügt, klicken Sie in Multipoint-Manager auf die Registerkarte **Benutzer**. Standardbenutzer Konten werden in der Spalte **Kontotyp** als **Standard** angezeigt.

Wenn Ihre MultiPoint Services-Benutzer private Dokumente in Windows speichern, sollte sich jeder Benutzer mit einem eindeutigen Benutzernamen und Kennwort am MultiPoint Services-System anmelden.

## NOTE

Weitere Informationen zu Problemen, die Sie als *Administrator* beim Erstellen und Verwalten von Benutzerkonten berücksichtigen sollten, finden Sie im Thema [Überlegungen zu Benutzerkonten](#).

## So erstellen Sie ein Standardbenutzerkonto

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Benutzer**.
2. Klicken Sie unter **Benutzeraufgaben** auf **Benutzerkonto hinzufügen**. Der Assistent **Benutzerkonto hinzufügen** wird geöffnet.
3. Geben Sie in das Feld **Benutzerkonto** einen Anmeldenamen für den Benutzer ein. Typischerweise besteht der Anmeldename des Benutzers aus dem Vor- und Nachnamen, die ohne Leerzeichen in einem Wort zusammengeschrieben werden, oder dem ersten Buchstaben des Vornamens und dem Nachnamen, die ohne Leerzeichen in einem Wort zusammengeschrieben werden.
4. Geben Sie in das Feld **Vollständiger Name** den Namen des Benutzers im gewünschten Format ein, z.B. Vorname, vollständiger Name oder Spitzname.
5. Geben Sie im Feld **Kennwort erstellen** ein Kennwort für den Benutzer ein. Dieses Kennwort sollte nur Ihnen und dem Benutzer bekannt sein und muss an einem sicheren Ort gespeichert werden. Das Kennwort kann nur von einem Administrator geändert werden.
6. Geben Sie das Kennwort im Feld **Kennwort bestätigen** erneut ein, und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Seite zum Festlegen der Zugriffsebene die Option **Standardbenutzer** aus, und klicken Sie dann auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**.

# Erstellen eines Kontos für MultiPoint- Dashboardbenutzer

09.04.2020 • 2 minutes to read • [Edit Online](#)

Erstellen Sie MultiPoint-Dashboardbenutzerkonten für die Benutzer, die regelmäßig auf Stationen zugreifen, das MultiPoint Services-System aber nicht verwalten. Benutzer mit Multipoint-dashboardbenutzerkonten können die meisten Anwendungen ausführen und Dateien speichern, aber nicht den Multipoint-Manager ausführen. Um zu sehen, wer über Multipoint-dashboardbenutzerzugriff verfügt, klicken Sie in Multipoint Manager auf die Registerkarte **Benutzer**. Multipoint-dashboardbenutzerkonten werden in der Spalte **Kontotyp** als **Multipoint-  
Dashboardbenutzer**

Wenn Ihre MultiPoint Services-Benutzer private Dokumente in Windows speichern, sollte sich jeder Benutzer mit einem eindeutigen Benutzernamen und Kennwort am MultiPoint Services-System anmelden.

## NOTE

Weitere Informationen zu Problemen, die Sie als *Administrator* beim Erstellen und Verwalten von Benutzerkonten berücksichtigen sollten, finden Sie im Thema [Überlegungen zu Benutzerkonten](#).

## So erstellen Sie ein Konto für MultiPoint- Dashboardbenutzer

1. Klicken Sie im Multipoint-Manager auf die Registerkarte **Benutzer** .
2. Klicken Sie unter **Benutzeraufgaben** auf **Benutzerkonto hinzufügen**. Der Assistent **Benutzerkonto hinzufügen** wird geöffnet.
3. Geben Sie in das Feld **Benutzerkonto** einen Anmeldenamen für den Benutzer ein.
4. Geben Sie in das Feld **Vollständiger Name** den Namen des Benutzers im gewünschten Format ein, z.B. Vorname, vollständiger Name oder Spitzname.
5. Geben Sie im Feld **Kennwort erstellen** ein Kennwort für den Benutzer ein. Dieses Kennwort sollte nur Ihnen und dem Benutzer bekannt sein und muss an einem sicheren Ort gespeichert werden. Das Kennwort kann nur von einem Administrator geändert werden.
6. Geben Sie das Kennwort im Feld **Kennwort bestätigen** erneut ein, und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Seite zum Festlegen der Zugriffsebene die Option **MultiPoint-  
Dashboardbenutzer** aus, und klicken Sie dann auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**.

## Weitere Informationen

[Überlegungen zu Benutzerkonten](#)

# Aktualisieren oder Löschen eines Benutzerkontos

09.04.2020 • 2 minutes to read • [Edit Online](#)

Wenn Sie am MultiPoint Server-System als Administrator angemeldet sind, können Sie jedes Benutzerkonto ändern. Dies umfasst das Ändern der Zugriffsebene für ein Konto, das Ändern eines vollständigen Namens und Kennworts oder das Löschen eines Kontos.

1. Öffnen Sie den Multipoint-Manager im Stations Modus, und klicken Sie dann auf die Registerkarte **Benutzer**.
2. Klicken Sie in der Spalte **Benutzer** auf das Konto, das Sie ändern möchten.
3. Klicken Sie unter *Benutzernamen Aufgabe* auf den entsprechenden Task.

AUSGEWÄHLTE AUFGABE FÜR DAS ELEMENT	BESCHREIBUNG
Vollständigen Namen ändern	Ermöglicht das Ändern des vollständigen Namens für das Konto.
Kennwort ändern	Ermöglicht das Ändern des Kennworts für dieses Konto auf dem MultiPoint Server-System.
Zugriffsebene ändern	Ermöglicht das Ändern des Kontotyps in Administrator oder Standardbenutzer.
Benutzerkonto löschen	Entfernt das Benutzerkonto aus dem MultiPoint Server-System.

## Weitere Informationen

[Erstellen eines Administratorkontos](#)

[Erstellen eines Standardbenutzerkontos](#)

[Verwalten von Benutzerkonten](#)

# Verwalten von virtuellen Desktops

09.04.2020 • 6 minutes to read • [Edit Online](#)

Mit einem VDI-Computer können Sie jede *lokale* Multipoint Services-Station so konfigurieren, dass eine Verbindung mit einem Windows 10 Enterprise-Gast Betriebssystem hergestellt wird, das auf einem virtuellen Hyper-V-Computer auf demselben Multipoint Services-Computer wie die Station ausgeführt wird. Diese Stationen für virtuelle Desktops können mit einer Anwendung angepasst werden, die nicht auf einer Windows Server-Version installiert werden kann.

## Aktivieren des virtuellen Desktop Features

1. Öffnen Sie MultiPoint-Manager, und klicken Sie anschließend auf die Registerkarte **Virtuelle Desktops**.
2. Klicken Sie unter **VDI-Aufgaben** auf **Create virtual desktop** (Virtuellen Desktop erstellen), und rufen Sie Ihre ISO- oder VHD-Datei von Windows 10 Enterprise auf.

Das System wird neu gestartet, dies kann einige Minuten dauern.

## Erstellen einer Vorlage für virtuelle Desktops

1. Öffnen Sie MultiPoint-Manager, und klicken Sie anschließend auf die Registerkarte **Virtuelle Desktops**.
2. Klicken Sie unter **VDI Tasks** (VDI-Aufgaben) auf **Create virtual desktop** (Virtuellen Desktop erstellen), und rufen Sie Ihre ISO- oder VHD-Datei von Windows 10 Enterprise auf.

Wenn Sie die DVD verwenden, sucht das Programm automatisch die WIM-Datei von Windows 10 Enterprise. Klicken Sie andernfalls auf **Durchsuchen**, und navigieren Sie dann zur ISO- bzw. VHD-Datei von Windows 10 Enterprise.

Ändern Sie das Präfix bei Bedarf. Standardmäßig ist es der Name des Hostcomputers.

### NOTE

Das Präfix wird als Name der Vorlage und der virtuellen Desktopstationen verwendet. Die Vorlage erhält den Namen „Präfix“ -t. Die virtuellen Desktopstationen erhalten den Namen „Präfix“ -n, wobei n die Stations-ID ist.

3. Geben Sie einen Namen und ein Kennwort für das lokale Administratorkonto ein, das zum Anmelden bei allen virtuellen Desktopstationen verwendet wird, die auf Grundlage der Vorlage erstellt werden, und klicken Sie dann auf **OK**.

Es dauert einige Minuten, bis die Erstellung der Vorlage abgeschlossen ist.

Als Nächstes erfahren Sie, wie Sie die Vorlage für virtuelle Desktops anpassen.

### NOTE

Wenn der MultiPoint-Server in eine Domäne eingebunden ist, füllt das Dialogfeld ein zusätzliches Feld. Dadurch können Sie bestimmen, ob die von der Vorlage erstellten virtuellen Computer in eine Domäne eingebunden werden sollen.

## Importieren einer Vorlage für virtuelle Desktops

Falls Sie eine Vorlage für virtuelle Desktops auf einem anderen MultiPoint-Server erstellt haben, können Sie diese Vorlage mithilfe der folgenden Schritte importieren.

1. Öffnen Sie MultiPoint-Manager, und klicken Sie anschließend auf die Registerkarte **Virtuelle Desktops**.
2. Klicken Sie unter VDI-Tasks (VDI-Aufgaben) auf **Import Virtual desktop template** (Vorlage für virtuelle Desktops importieren).
3. Suchen Sie die Vorlage und definieren Sie den Pfad und das Präfix für die importierte Vorlage.

## Anpassen der Vorlage für virtuelle Desktops

Nachdem Sie die Vorlage für virtuelle Desktops erstellt haben, können Sie sie mit Anwendungen und Softwareupdates anpassen und Systemeinstellungen konfigurieren.

1. Öffnen Sie MultiPoint-Manager, und klicken Sie anschließend auf die Registerkarte **Virtuelle Desktops**.
2. Wählen Sie die Vorlage für virtuelle Desktops aus, und klicken Sie anschließend auf **Customize virtual desktop template** (Vorlage für virtuelle Desktops anpassen).  
Die Vorlage wird in einem separaten Fenster geöffnet, und es werden zusätzliche Anweisungen dargestellt, die die wichtigsten Schritte zum Anpassen der Vorlage für virtuelle Desktops hervorheben. Lesen Sie diese Anweisungen sorgfältig.

## Erstellen virtueller Desktop Stationen

1. Öffnen Sie den MultiPoint-Manager im Stationsmodus, und klicken Sie anschließend auf die Registerkarte **Virtuelle Desktops**.

### NOTE

Wenn das MultiPoint Services-System nicht im Stationsmodus ausgeführt wird, starten Sie es neu, bevor Sie diese Prozedur abschließen.

2. Wählen Sie im linken-Bereich die Vorlage für virtuelle Desktops aus. Sie trägt den Namen <Präfix -t>.
3. Klicken Sie unter Vorlagenaufgaben auf **Virtuelle Desktopstationen erstellen**, und klicken Sie anschließend auf **OK**.

Die Erstellung der virtuellen Desktopstation kann einige Minuten dauern.

### NOTE

Wenn lokale Stationen gegenwärtig mit einem sitzungsbasierten virtuellen Desktop verbunden sind, müssen Sie diese Stationen abmelden, damit sie eine Verbindung mit einer der neu erstellten virtuellen Desktopstationen herstellen können.

## Überprüfen der neu erstellten angepassten virtuellen Desktopstationen

Sie können Ihre benutzerdefinierten virtuellen Desktopstationen überprüfen, indem Sie sich mit einem lokalen Administratorkonto oder einem Domänenkonto bei mindestens einer virtuellen Desktopstation anmelden und anschließend sicherstellen, dass die neuen VM-basierten virtuellen Desktops ordnungsgemäß funktionieren.

## Deaktivieren von virtuellen Desktops

Wenn Sie virtuelle Desktops deaktivieren, wird auch die Hyper-V-Funktion deaktiviert. Alle Benutzer werden abgemeldet, und das System wird neu gestartet. Alle virtuellen Stationen werden nach dem Neustart des Systems lokalen MultiPoint-Sitzungen zugewiesen.

1. Öffnen Sie den MultiPoint-Manager im Stationsmodus, und klicken Sie anschließend auf die Registerkarte **Virtuelle Desktops**.
2. Klicken Sie unter VDI-Tasks (VDI-Aufgaben) auf **Disable virtual desktops** (Virtuelle Desktops deaktivieren).

# Verwalten von Benutzerdateien

09.04.2020 • 2 minutes to read • [Edit Online](#)

Standardbenutzer und Administratoren können an MultiPoint Services-Stationen Dokumente in Windows-Explorer-Bibliotheken und -Ordnern speichern. Eine Bibliothek ist eine Sammlung von Elementen wie Dateien oder Ordnern. Allgemeine Bibliotheken in Windows-Explorer umfassen unter anderem **Dokumente, Musik, Bilder** und **Videos**. Bei der Arbeit mit Bibliotheken gibt es zwei Möglichkeiten zum Speichern von Dokumenten:

- Das private Speichern von Dokumenten, sodass nur der Benutzer, von dem sie in einer Bibliothek oder einem Ordner gespeichert wurden, darauf Zugriff hat. Beachten Sie, dass Administratoren auf privat gespeicherte Dokumente von Standardbenutzern zugreifen können. Standardbenutzer hingegen haben keinen Zugriff auf privat gespeicherte Dokumente von Administratoren. Weitere Informationen zum Schützen von Inhalten finden Sie im Thema [Schützen von Dateien](#).
- Speichern Sie Dokumente öffentlich, sodass Sie für alle Benutzer im Multipoint Services-System zugänglich sind. Weitere Informationen zum Freigeben von Inhalten für andere Benutzer finden Sie im Thema [Freigeben von Dateien](#).

Die **Dokument** Bibliothek enthält standardmäßig zwei Ordner: **Eigene Dokumente** (privat) und **öffentliche Dokumente** (öffentlich). Andere Dokumentbibliotheken enthalten ähnliche Paare privater und öffentlicher Ordner. Alle Administratoren und Standardbenutzer eines MultiPoint Services-Systems sollten verstehen, wie sich der Speicherort in Windows-Explorer, an dem sie Dokumente und andere Dateien ablegen, auf den Datenschutz bzw. öffentlichen Zugriff für diese Dateien auswirken kann.

Sie können Inhalte auch für andere Benutzer freigeben, indem Sie ein USB-Speichergerät wie z. B. einen USB-Speicherstick oder ein Massen Speichergerät (externe Festplatte) verwenden. Weitere Informationen zum Freigeben von Inhalten mit Speichergeräten finden Sie im Thema [Speichern und Freigeben von Dateien auf einem USB-Flashlaufwerk](#).

# Schützen von Dateien

09.04.2020 • 2 minutes to read • [Edit Online](#)

Dieses Thema gilt für Inhalte wie z.B. Dokumente, die von Ihnen (als *Administrator*) und von *Standardbenutzern* für andere Benutzer in einem MultiPoint Services-System nicht freigegeben werden sollen.

Weitere Informationen zum Datenschutz in MultiPoint Services finden Sie unter [Erwägungen zu Datenschutz und Sicherheit](#).

## So halten Sie Inhalte im Windows-Explorer privat

Um Ihre Dokumente und anderen Inhalt privat zu halten, speichern Sie Ihre Arbeit im Windows-Explorer in der Bibliothek **Dokumente** im Ordner **Eigene Dokumente**. Der Ordner **Eigene Dokumente** ist standardmäßig ein privater Ordner. Beachten Sie jedoch, dass Administratoren auch auf private Ordner im Windows-Explorer zugreifen können.

### WARNING

Während ein externes Speichergerät, wie z.B. ein USB-Flashlaufwerk, mit einem USB-Anschluss auf dem Host oder an einem USB-Hub, der nicht als Stationshub fungiert, verbunden ist, kann es von allen Standardbenutzern und Administratoren angezeigt werden, die am MultiPoint Services-System angemeldet sind. Wenn Sie Bedenken hinsichtlich des Datenschutzes oder der Sicherheit der auf einem externen Speichergerät gespeicherten Inhalte haben, schließen Sie das Gerät nur an einen Stationshub im MultiPoint Services-System an. Informationen zur Verwendung von USB-Speichergeräten finden Sie im Thema [Speichern und Freigeben von Dateien auf einem USB-Flashlaufwerk](#).

## Weitere Informationen

[Verwalten von Benutzerdateien](#)

[Speichern und Freigeben von Dateien auf einem USB-Flashlaufwerk](#)

# Freigeben von Dateien

09.04.2020 • 2 minutes to read • [Edit Online](#)

Inhalte können für andere MultiPoint Services-Benutzer freigegeben werden, indem sie in einem öffentlichen Ordner im Windows-Explorer gespeichert werden. Alle Inhalte, die in einem MultiPoint Services-System in öffentlichen Ordnern im Windows-Explorer gespeichert werden, sind für alle Benutzer im MultiPoint Services-System zugänglich.

Sie können Inhalte auch freigeben, indem Sie sie auf Wechselmedien speichern, wie unter [Speichern und Freigeben von Dateien auf einem USB-Speicherstick](#) beschrieben.

Informationen zur privaten Aufbewahrung von Inhalten finden Sie unter [beibehalten von Dateien privat](#).

## So geben Sie mithilfe öffentlicher Ordner Inhalte für andere Benutzer frei

Sie können Inhalte für andere Benutzer freigeben, indem Sie diese in den Ordner **Öffentliche Dokumente**, **Öffentliche Musik** oder anderen öffentlichen Ordner in Windows-Explorer-Bibliotheken speichern.

Sie können Dateien auch auf mehreren Computern freigeben, die MultiPoint Services in einem Netzwerk ausführen, indem Sie einen neuen Ordner erstellen und diesen dann freigeben.

## So geben Sie Ordner für mehrere Computer in einem MultiPoint Services-Netzwerk frei

1. Klicken Sie mit der rechten Maustaste auf einen Desktop, und klicken Sie dann auf **neu**.
2. Klicken Sie auf **Ordner**, und geben Sie einen Namen für den Ordner ein.
3. Doppelklicken Sie auf den Ordner, um ihn zu öffnen.
4. Klicken Sie auf **Freigeben für**, und klicken Sie dann auf **bestimmte Personen**.
5. Wählen Sie bestimmte Benutzer aus, oder klicken Sie auf **Jeder**.

## Weitere Informationen

[Verwalten von Benutzerdateien](#)

[Speichern und Freigeben von Dateien auf einem USB-Flashlaufwerk](#)

[Schützen von Dateien](#)

# Speichern und Freigeben von Dateien auf einem USB-Flashlaufwerk

09.04.2020 • 2 minutes to read • [Edit Online](#)

Zusätzlich zur Freigabe von Inhalten mithilfe von öffentlichen Ordner in Windows-Explorer können Sie Inhalte auch über ein USB-Speichergerät, z. B. einen USB-Speicherstick oder ein Massen Speichergerät, freigeben. Wenn ein USB-Speichergerät direkt an den Hostcomputer oder einen USB-Hub, der nicht als Stationshub fungiert, angeschlossen wird, wird dieses Speichergerät für alle Benutzer – sowohl *Standardbenutzer* als auch *Administratoren* – im gesamten MultiPoint Services-System als Wechseldatenträger angezeigt.

Sie können einen Wechseldatenträger auch verwenden, um private Dokumente im Windows-Explorer in einem privaten Ordner zu speichern, z.B. im Ordner **Eigene Dokumente** in der Bibliothek **Dokumente**.

## NOTE

Dashboardbenutzer können die Verwendung von USB-Speicher blockieren. Weitere Informationen finden Sie unter [Block or Unblock USB Storage](#) (Blockieren oder Aufheben der Blockierung von USB-Speicher).

## So geben Sie Inhalte frei, die direkt auf einem Wechseldatenträger gespeichert sind

1. Verbinden Sie den Wechseldatenträger mit einem freien USB-Anschluss des Hostcomputers oder mit einem USB-Hub, der im MultiPoint Services-System nicht als *Stationshub* fungiert.
2. Weisen Sie die Benutzer an anderen *Stationen* an, im Windows-Explorer zu, Laufwerk des Wechseldatenträgers zu navigieren und diesen zu öffnen. Auf dieselbe Weise können auch andere Benutzer Inhalte von ihren eigenen Wechseldatenträgern für Sie freigeben.

## So geben Sie Inhalte über öffentliche Ordner frei, die auf einem Wechseldatenträger gespeichert sind

1. Verbinden Sie den Wechseldatenträger mit einem freien USB-Anschluss des Hostcomputers oder mit einem USB-Hub, der im MultiPoint Services-System nicht als *Stationshub* fungiert.
2. Kopieren Sie den freizugebenden Inhalt in einen öffentlichen Ordner im Windows-Explorer, z.B. **Öffentliche Dokumente** in der Bibliothek **Dokumente**.

## So arbeiten Sie privat mit Inhalten, die auf einem USB-Speichergerät gespeichert sind

Verbinden Sie den Wechseldatenträger mit einem freien USB-Anschluss des Stationshubs.

## Weitere Informationen

[Schützen von Dateien](#)

[Freigeben von Dateien](#)

[Verwalten von Benutzerdateien](#)

# Verwalten von Benutzerdesktops mit dem MultiPoint-Dashboard

09.04.2020 • 4 minutes to read • [Edit Online](#)

In einem MultiPoint Services-System ist ein Desktop die Softwarebenutzeroberfläche, die auf dem Monitor jeder *Benutzerstation* angezeigt wird. Das Multipoint-Dashboard ist ein Tool, das Sie bei der Verwaltung dieser Desktops unterstützt.

Im Multipoint-Dashboard können Sie auf der Registerkarte **Startseite** die folgenden Aktionen ausführen:

- Anzeigen von Desktops  
Sie können die Miniaturansichten für jeden aktiven Desktop anzeigen. Informationen zum Anzeigen von Miniaturansichten finden Sie im Thema [View Options for Session Thumbnails](#) (Anzeigeoptionen für Sitzungsminiaturansichten).
- Blockieren oder Aufheben der Blockierung von Stationen  
Sie können Stationen blockieren und die Blockierung aufheben. Darüber hinaus kann auch eine angepasste Nachricht konfiguriert werden, die auf blockierten Stationen angezeigt wird. Weitere Informationen zum Blockieren von Stationen und zum Aufheben der Blockierung oder zum Erstellen einer Nachricht, die auf blockierten Stationen angezeigt wird, finden Sie im Thema [Blockieren einer Station oder Aufheben der Blockierung](#).
- Einschränken der Webverwendung  
Sie können konfigurieren, welche Websites von Benutzern besucht werden können. Informationen zum Festlegen von Websites finden Sie im Thema [Einschränken des Webzugriffs](#).
- Blockieren oder Aufheben der Blockierung von USB-Speicher  
Sie können USB-Speicher entweder für eine einzelne Station oder für alle Stationen blockieren bzw. die Blockierung aufheben. Wenn Speicher blockiert wird, können Benutzer keine USB-Speichergeräte auf ihren Stationen verwenden. Weitere Informationen finden Sie im Thema [Block or Unblock USB Storage](#) (Blockieren oder Aufheben der Blockierung von USB-Speicher).
- Projizieren einer Station auf eine andere Station  
Sie können Ihre Station auf eine andere Station oder andere Stationen projizieren. Ferner können Sie eine andere ausgewählte Station auf alle anderen Stationen projizieren. Informationen zum projizieren einer Station finden Sie im Thema [Projizieren einer Station auf andere Stationen](#).
- Starten oder Schließen von Anwendungen auf einer Station  
Sie können Anwendungen auf einer Station starten oder schließen. Informationen zum Starten oder Schließen von Anwendungen finden Sie im Thema [Starten oder Schließen von Anwendungen auf einer Station](#).
- Kommunizieren mit Chat  
Sie können mit ausgewählten Benutzern über den Chat kommunizieren. Die Chatnachricht ist nur für den Dashboardbenutzer und den Benutzer der ausgewählten Sitzung sichtbar. Weitere Informationen finden Sie unter [Kommunizieren mit Chat](#).
- Ändern der Größe von Miniaturansichten  
Sie können die Größe der Miniaturansichten ändern, die im Multipoint-Dashboard angezeigt werden. Informationen zum Ändern der Größe von Miniaturansichten finden Sie unter [View Options for Session Thumbnails](#) (Anzeigeoptionen für Sitzungsminiaturansichten).
- Anzeigen aller Stationen  
Sie können alle mit Ihrem System verbundenen Stationen anzeigen, einschließlich der nicht aktiven Stationen. Informationen zum Anzeigen aller Stationen finden Sie im Thema [Anzeigen aller Stationen](#).

- Suchen und Sortieren von Miniaturansichten

Sie können die Reihenfolge und Gruppierung von Miniaturansichten auf dem Dashboard definieren.

Verwenden Sie die Suche, um die Miniaturansichten zu filtern.

- Abmelden aller überwachter Stationen

Sie können alle überwachten Stationen auf Ihrem MultiPoint Services-System abmelden. Informationen zum

Abmelden überwachter Stationen finden Sie im Thema [Abmelden von Benutzersitzungen](#).

# Blockieren einer Station oder Aufheben der Blockierung einer Station

09.04.2020 • 2 minutes to read • [Edit Online](#)

Sie können das MultiPoint Services-System für einen oder mehrere Benutzer blockieren, wenn Sie die Benutzer auf etwas aufmerksam machen möchten. Während Benutzer blockiert werden, bleiben Ihre Sitzungen im Computerspeicher des Multipoint Services-Systems aktiv, bis die Blockierung der Stationen aufgehoben wird. Sie können eine Nachricht eingeben, die blockierten Benutzern angezeigt werden soll.

## So blockieren Sie eine Station

1. Wählen Sie im Multipoint-Dashboard das Miniaturbild der Station aus, die Sie blockieren möchten.
2. Klicken Sie auf der Registerkarte "blockieren" auf **blockieren**, und klicken Sie dann auf **ausgewählte Desktops blockieren** oder **alle Desktops blockieren**.

## So heben Sie die Blockierung einer Station auf

1. Wählen Sie im Multipoint-Dashboard das Miniaturbild der Station aus, die Sie entsperren möchten.
2. Klicken Sie auf der Registerkarte "blockieren" auf **Blockierung aufheben**, und klicken Sie dann auf **Blockierung ausgewählter Desktops aufheben**.

## Erstellen einer Nachricht, die blockierten Benutzern angezeigt wird

Bevor Sie einen Benutzer blockieren, empfiehlt es sich, eine Meldung zu erstellen, die auf dem Monitor des Benutzers angezeigt wird, wenn diese blockiert werden. Beispiel: "wenden Sie sich bitte an den Sprecher." **Station blockiert** ist der Standardtext, wenn Sie keine eigene Nachricht erstellen.

1. Klicken Sie auf das Dropdown Menü **blockieren**, und klicken Sie dann auf **Nachricht festlegen**. Die Seite **Nachricht für blockierte Benutzer festlegen** wird geöffnet.
2. Geben Sie die Meldung ein, die Sie auf den gesperrten Stationen anzeigen möchten, und klicken Sie dann auf **OK**.

# Einschränken des Webzugriffs

09.04.2020 • 3 minutes to read • [Edit Online](#)

Zusätzlich zur Überwachung von Benutzeraktivitäten auf einzelnen Desktops können Sie als Administrator den Benutzer Zugriff auf bestimmte Websites einschränken, indem Sie zulässige Websites und Websites angeben, für die Sie den Benutzer Zugriff blockieren möchten.

## So schränken Sie den Webzugriff auf einer Station ein

1. Klicken Sie im Multipoint-Dashboard auf der Registerkarte **webbeschränkung** auf **Konfigurieren**. Die Seite **Webeinschränkung konfigurieren** wird geöffnet. Die Websites, auf die der Benutzer zugreifen kann, sind aufgelistet.
2. Klicken Sie auf das Miniaturbild der Benutzerstation, auf der Sie den Webzugriff einschränken möchten.
3. Klicken Sie unter **Ausgewählte Aufgaben für Elemente** auf **Webzugriff auf dieser Station einschränken**. Die Seite **Webeinschränkung konfigurieren** wird geöffnet. Die Websites, auf die der Benutzer zugreifen kann, sind aufgelistet.
4. Geben Sie zum Hinzufügen einer zulässigen Website die Webadresse ein, und klicken Sie dann auf **Hinzuzufügen**.

### NOTE

Wenn Sie z. b. "contoso.com" eingeben, werden Websites, die relativ zu www.contoso.com sind (z. b. www.NewPage.contoso.com), zugelassen oder blockiert. Durch die Eingabe von "Configuration Manager" werden alle standortbezogenen Websites (einschließlich contoso.com, contoso.uk usw.) entweder zugelassen oder beschränkt.

5. Zum Entfernen einer Webadresse aus der Liste der zulässigen Websites klicken Sie auf die Webadresse, zu der Sie den Zugang entfernen möchten, und klicken Sie dann auf **Entfernen**.

## So schränken Sie den Webzugriff auf allen Stationen ein

1. Klicken Sie im Multipoint-Dashboard auf der Registerkarte **webbeschränkung** auf das Menü Start-Dropdown Menü, und klicken Sie dann auf **Webzugriff auf allen Desktops einschränken**.  
Die Seite **Webeinschränkung konfigurieren** wird geöffnet. Die Websites, auf die der Benutzer zugreifen kann, sind aufgelistet. Führen Sie eine der folgenden Aktionen aus:
  2. Klicken Sie zum Hinzufügen einer zulässigen Website auf **Nur diese Websites zulassen**, geben Sie die Webadresse ein, und klicken Sie dann auf **Hinzufügen**.  
Wenn Sie eine Website hinzufügen möchten, die nicht von Benutzern besucht werden soll, klicken Sie auf **nur diese Websites zulassen**, geben Sie die Webadresse ein, die Sie nicht besuchen möchten, und klicken Sie dann auf **Hinzufügen**.

### NOTE

Wenn Sie z. b. "contoso.com" eingeben, werden Websites, die relativ zu www.contoso.com sind (z. b. www.NewPage.contoso.com), zugelassen oder blockiert. Durch die Eingabe von "Configuration Manager" werden alle standortbezogenen Websites (einschließlich contoso.com, contoso.uk usw.) entweder zugelassen oder beschränkt.

3. Zum Entfernen einer Webadresse aus der Liste der zulässigen oder nicht zulässigen Websites wählen Sie die Webadresse aus und klicken dann auf **Entfernen**.

## Weitere Informationen

[Verwalten von Benutzer Desktops](#)

# Blockieren oder Aufheben der Blockierung von USB-Speicher

09.04.2020 • 2 minutes to read • [Edit Online](#)

Sie können Benutzer daran hindern, USB-Speicher auf ihren Benutzerstationen zu verwenden.

## So blockieren Sie USB-Speicher für ausgewählte Stationen

1. Klicken Sie im MultiPoint-Dashboard auf die Station, die Sie blockieren möchten.
2. Klicken Sie auf **Blockieren > Ausgewählte Desktops blockieren**.

## So blockieren Sie USB-Speicher für alle Stationen

Öffnen Sie das MultiPoint-Dashboard, und wählen Sie anschließend im Dropdownmenü **Block Storage on all stations** (Speicher auf allen Stationen blockieren) aus.

## So heben Sie die Blockierung von USB-Speicher für ausgewählte Stationen auf

Öffnen Sie das MultiPoint-Dashboard, wählen Sie die Miniaturansicht der Station aus, für die Sie die Blockierung aufheben möchten, und klicken Sie anschließend auf **Blockierung aufheben**.

# Projizieren einer Station auf andere Stationen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Als Multipoint-Dashboardbenutzer können Sie Ihren Desktop auf die Station eines einzelnen Benutzers oder an die (nicht-Administrator-) Endstationen eines Benutzers projizieren. Diese Funktion ist nützlich, wenn Sie einem Benutzer oder einer Gruppe von Benutzern eine Aufgabe vorführen möchten.

## So projizieren Sie Ihren Desktop auf die Station eines Standard Benutzers

1. Klicken Sie im Multipoint-Dashboard auf die Miniaturansicht des Desktops, auf dem Sie die Station projizieren möchten.
2. Klicken Sie auf der Registerkarte **Startseite** auf **Ihren Desktop**, und klicken Sie dann auf **Ihren Desktop auf ausgewählte Desktops projizieren**.
3. Um die Projektion zu beenden, klicken Sie auf **Beenden** (entweder auf der Registerkarte **Projektion** oder in der rechten Ecke unterhalb der Multifunktionsleiste).

## So projizieren Sie Ihren Desktop auf alle Stationen

1. Klicken Sie im Multipoint-Dashboard auf der Registerkarte **Start** auf **Ihren Desktop**, und klicken Sie dann auf **Ihren Desktop auf alle Desktops projizieren**.
2. Um die Projektion zu beenden, klicken Sie auf **Beenden** (entweder auf der Registerkarte **Projektion** oder in der rechten Ecke unterhalb der Multifunktionsleiste).

## So projizieren Sie einen anderen Desktop auf alle Desktops

1. Klicken Sie auf die Miniaturansicht des Desktops, den Sie auf alle Desktops projizieren möchten.
2. Klicken Sie auf der Registerkarte **Startseite** auf **ausgewählter Desktop**, und klicken Sie dann auf **ausgewählter Desktop**. Der ausgewählte Desktop wird auf allen Desktops angezeigt.
3. Um die Projektion zu beenden, klicken Sie auf **Beenden** (entweder auf der Registerkarte **Projektion** oder in der rechten Ecke unterhalb der Multifunktionsleiste).

# Starten oder Schließen von Anwendungen auf einer Station

09.04.2020 • 2 minutes to read • [Edit Online](#)

Als Multipoint-Dashboardbenutzer können Sie eine Anwendung auf dem Desktop eines Benutzers, auf ausgewählten Desktops oder auf allen Desktops öffnen oder schließen.

## Starten einer Anwendung auf einer Benutzer Station

1. Klicken Sie im Multipoint-Dashboard auf die Miniaturansicht des Benutzer Desktops, auf dem Sie die Anwendung starten möchten, und klicken Sie dann im Menüband unter **Anwendungen** auf das Dropdown Menü Dropdown –, um das Menü zu starten .
2. Klicken Sie auf **Eine Anwendung auf ausgewählten Desktops starten**. Die Seite **Anwendung starten** wird geöffnet.
3. Klicken Sie auf die Anwendung, die geöffnet werden soll, oder geben Sie unter **Geben Sie die Anwendung ein, die Sie starten, bzw. den Ordner, das Dokument oder die Internetressource ein, den/das/die Sie öffnen möchten** den Namen der Ressource ein, die geöffnet werden soll, und klicken Sie dann auf **OK**.

## Anwendung auf allen Benutzer Stationen starten

1. Klicken Sie im Multipoint-Dashboard auf das Dropdown Menü Dropdown – für **Launch** (im Menüband unter **Anwendungen**).
2. Klicken Sie auf **Eine Anwendung auf allen Desktops starten**. Die Seite **Anwendung starten** wird geöffnet.
3. Klicken Sie auf die Anwendung, die geöffnet werden soll, oder geben Sie unter **Geben Sie die Anwendung ein, die Sie starten, bzw. den Ordner, das Dokument oder die Internetressource ein, den/das/die Sie öffnen möchten** den Namen der Ressource ein, die geöffnet werden soll, und klicken Sie dann auf **OK**.

## Schließen einer Anwendung auf einer Benutzer Station

1. Klicken Sie im Multipoint-Dashboard auf die Miniaturansicht des Desktops, auf dem Sie eine Anwendung schließen möchten.
2. Klicken Sie im Menüband unter **Anwendungen** auf **Schließen**, um die Seite **Anwendung schließen** zu öffnen.
3. Wählen Sie den Namen des Elements (Anwendung, Ordner, Dokument oder Internetressource), das geschlossen werden soll, und klicken Sie dann auf **Anwendung schließen**.

## Weitere Informationen

[Verwalten von Benutzer Desktops](#)

# Kommunizieren mit Chat

09.04.2020 • 2 minutes to read • [Edit Online](#)

MultiPoint-Dashboardbenutzer und Stationsbenutzer können private Nachrichten über den Chat austauschen, wenn dieser in den Servereinstellungen aktiviert wurde.

**So senden Sie vom MultiPoint-Dashboard aus eine Chatnachricht an einen Benutzer**

1. Klicken Sie im Multipoint-Dashboard auf das Miniaturbild oder die Bilder des Benutzers, der eine Nachricht senden soll.
2. Klicken Sie im Menüband auf **Senden**. Es öffnet sich ein Chatfenster.

**NOTE**

Benutzer können mit dem Dashboardbenutzer über den Chat kommunizieren, indem sie das Chatsymbol in der Windows-Taskleiste verwenden. Es wird automatisch angeheftet, wenn der Chat in den Servereinstellungen aktiviert wird.

# Übernehmen der Steuerung einer Benutzersitzung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Als MultiPoint-Dashboardbenutzer können Sie andere Benutzer unterstützen, indem Sie mithilfe des Features „Steuerung übernehmen“ remote auf deren Computer zugreifen.

1. Klicken Sie im Multipoint-Dashboard auf der Registerkarte **Startseite** auf die Miniaturansicht des Desktops für den Benutzer, den Sie unterstützen möchten.
2. Klicken Sie auf der Registerkarte **Unterstützen** auf **Steuerung übernehmen**. Der Desktop des Benutzers wird auf dem Desktop geöffnet, und Sie können mit Tastatur und Maus auf dem Desktop navigieren.
3. Wenn Sie die Unterstützung für den Benutzer abgeschlossen haben, klicken Sie auf **Beenden**.

## NOTE

Möglicherweise müssen Sie den Desktop des Benutzers minimieren, um Ihr Multipoint-Dashboard anzuzeigen.

## Weitere Informationen

[Verwalten von Benutzerdesktops mit dem MultiPoint-Dashboard](#)

# Anzeigeoptionen für Sitzungsminiaturansichten auf dem MultiPoint-Dashboard

09.04.2020 • 3 minutes to read • [Edit Online](#)

Eine einfache Möglichkeit, Benutzeraktivitäten auf einzelnen Desktops zu überwachen, ist die Anzeige von Miniaturbildern jedes aktiven Desktops in Ihrem MultiPoint Services-System. Standardmäßig werden auf der Registerkarte Home auf der Registerkarte **Home** auf dem Multipoint-Dashboard Images von Desktops angezeigt.

Mithilfe des Multipoint-Dashboards können Sie die folgenden Aktionen ausführen:

- Zeigen Sie den Desktop eines Benutzers genauer an, indem Sie seine Ansicht im Dashboard vergrößern.
- Ändern Sie die Größe der Miniaturbilder, die auf dem Dashboard angezeigt werden. Es sind drei Größen für die Ansicht verfügbar: klein, mittel und groß. Die Standardeinstellung ist „mittel“.
- Zeigen Sie alle Desktops im MultiPoint Services-System an, oder wählen Sie eine gefilterte Ansicht aus, in der nur aktive Desktops angezeigt werden.

## So vergrößern Sie die Ansicht eines ausgewählten Desktops auf dem MultiPoint-Dashboard

1. Klicken Sie auf die Registerkarte **Start**, und klicken Sie auf den Desktop, den Sie vergrößern möchten.
2. Klicken Sie auf der Registerkarte **Start** auf **Auswahl vergrößern**. Der Desktop des Benutzers wird im Dashboard geöffnet.
3. Wenn Sie die vergrößerte Ansicht nicht mehr benötigen, klicken Sie auf „Zurück zur Desktopansicht“.

## So ändern Sie die Größe der Desktopminiaturansichten auf dem MultiPoint-Dashboard

1. Klicken Sie auf die Registerkarte **Start**, und wählen Sie die Desktopminiaturansicht, die Sie vergrößern möchten.
2. Klicken Sie auf der Registerkarte **Start** auf **Auswahl vergrößern**. Die Seite **Desktopgröße ändern** wird geöffnet.
3. Klicken Sie auf die gewünschte Größe (**klein**, **Mittel** oder **groß**), und klicken Sie dann auf **OK**.

## So zeigen Sie alle Desktops auf dem MultiPoint-Dashboard an

1. Klicken Sie auf die Registerkarte **Start**, und klicken Sie anschließend auf dem Menüband unter **Desktops** auf **Anzeigen**.
2. Klicken Sie auf **Alle**. Alle Desktops werden auf dem Dashboard angezeigt.
3. Um zur gefilterten Ansicht zurückzuwechseln, klicken Sie auf **Anzeigen** und dann auf **Gefilterte Ansicht**.

**NOTE**

Klicken Sie mit der rechten Maustaste auf eine oder mehrere Miniaturansichten, um zu zusätzlichen Aktionen zu gelangen, die Sie in aktiven oder inaktiven Sitzungen ausführen können, wie **Ausgewählte Benutzer abmelden**. Weitere Informationen finden Sie unter [Abmelden von Benutzersitzungen](#).

## Weitere Informationen

[Verwalten von Benutzerdesktops mit dem MultiPoint-Dashboard](#)

# Abmelden von Benutzersitzungen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Standardbenutzer, MultiPoint-Dashboardbenutzer und Administratoren können sich wie bei jeder anderen Windows-Sitzung bei ihren Desktopsitzungen anmelden und von diesen abmelden. Darüber hinaus können Administratoren und MultiPoint-Dashboardbenutzer die Benutzersitzungen aller überwachten Sitzungen im MultiPoint Services-System beenden.

1. Klicken Sie im Multipoint-Dashboard auf die Registerkarte **Start**.

2. Führen Sie eine der folgenden Aktionen aus:

- Um eine einzelne Benutzersitzung oder ausgewählte Sitzungen abzumelden, klicken Sie auf das Miniaturbild der Sitzung, die Sie beenden möchten, und klicken Sie dann auf das Dropdown Menü oben links. Klicken Sie auf **Benutzer abmelden**, und klicken Sie dann auf **Ausgewählte Benutzer abmelden**. Sie können diese Option auch anzeigen, indem Sie mit der rechten Maustaste auf die ausgewählten Miniaturansichten klicken.
- Um alle Benutzersitzungen abzumelden, klicken Sie auf das Dropdown Menü oben links, klicken Sie auf **Benutzer abmelden**, und klicken Sie dann auf **alle Benutzer abmelden**.

## Weitere Informationen

[Verwalten von Benutzer Desktops](#)

[Abmelden oder Trennen von Benutzersitzungen](#)

[Aussetzen und Benutzersitzung aktiv lassen](#)

# Verwalten von MultiPoint-Systemen mit dem MultiPoint-Dashboard

09.04.2020 • 2 minutes to read • [Edit Online](#)

Im Multipoint-Dashboard können Sie auf der Registerkarte **Systeme** folgende Aktionen ausführen:

- Neustarten oder Herunterfahren ausgewählter Systeme  
Sie können ausgewählte MultiPoint Services-Systeme neu starten oder herunterfahren. Informationen zum Neustarten oder Herunterfahren ausgewählter Systeme finden Sie im Thema [Neustart oder Herunterfahren von MultiPoint-Systemen](#).
- Neuordnen ausgewählter Systeme  
Sie können ausgewählte MultiPoint Services-Systeme neu zuordnen. Informationen zum Neuordnen ausgewählter Systeme finden Sie im Thema [Neuzuordnung ausgewählter MultiPoint-Systeme](#).

## Weitere Informationen

[Neustarten oder Herunterfahren von MultiPoint-Systemen](#)

[Neuzuordnen ausgewählter Multipoint-Systeme](#)

# Neustart oder Herunterfahren

09.04.2020 • 2 minutes to read • [Edit Online](#)

Möglicherweise müssen Sie den Hostcomputer und alle *Stationen* Ihres MultiPoint Server-Systems neu starten, wenn Sie im Anschluss an die Installation von Hardware, Software und Softwareupdates dazu aufgefordert werden. Wenn Sie einer Station neue Hardwaregeräte hinzugefügt haben, möchten Sie diese möglicherweise der Station zuordnen. Weitere Informationen zum *Zuordnen von Stationen* finden Sie im Thema [Wechseln zwischen Modi](#).

Wenn Sie den Computer des Multipoint Services-Systems sicher ausschalten möchten, muss der Computer einen Vorgang zum Herunterfahren durchführen, bei dem alle geöffneten Programme geschlossen werden, Fenster heruntergefahren und der Computer und die zugehörigen *Stationenausgeschaltet* werden. Ziehen Sie weder einfach das Netzkabel aus der Steckdose, noch drücken Sie einfach den **Netzschalter** am Computer. Am Ende des Tages sowie zur Installation neuer Hardware im Computergehäuse sollte der Computer heruntergefahren werden. Wenn Sie dem System externe Hardware hinzufügen, müssen den Server ggf. ebenfalls herunterfahren oder neu starten.

## NOTE

Vor dem Herunterfahren oder Neustarten des Computers, auf dem MultiPoint Services ausgeführt wird, müssen alle Benutzersitzungen beendet werden.

## Starten Sie den Computer neu.

1. Beenden Sie alle Benutzersitzungen. Weitere Informationen zum Beenden einer Benutzersitzung finden Sie im Thema [Beenden einer Benutzersitzung](#).
2. Klicken Sie im Multipoint-Manager auf **Startseite**, und klicken Sie dann auf **Computer neu starten**.

## Herunterfahren des Computers

1. Beenden Sie alle Benutzersitzungen. Weitere Informationen zum Beenden einer Benutzersitzung finden Sie im Thema [Beenden einer Benutzersitzung](#).
2. Klicken Sie im Multipoint-Manager auf die Registerkarte **Start**, und klicken Sie dann auf **Computer herunterfahren**.

## Weitere Informationen

[Beenden einer Benutzersitzung](#)

[Verwalten von Systemaufgaben mithilfe des MultiPoint-Managers](#)

[Wechseln zwischen Modi](#)

[Abmelden oder Trennen von Benutzersitzungen](#)

# Neuzuordnung ausgewählter MultiPoint-Systeme

09.04.2020 • 2 minutes to read • [Edit Online](#)

Das erneute Zuordnen von Stationen im MultiPoint-Dashboard ermöglicht das Zuweisen von Tastaturen und Mäusen zu Monitoren. Lokale Benutzerstationen werden angehalten, während ein MultiPoint Services-System neu zugeordnet wird.

**Caution**

Die Neuzuordnung wird häufig zu Problembehandlungszwecken verwendet. Stationseinstellungen, z.B. Name und Informationen zur automatischen Anmeldung, werden während der Neuzuordnung gelöscht.

**So ordnen Sie ein MultiPoint Services-System neu zu**

1. Klicken Sie in MultiPoint Services auf die Registerkarte **Systeme**.
2. Klicken Sie auf die Miniaturansicht des Servers, der neu gestartet werden soll, und klicken Sie anschließend auf der Registerkarte **Hardware** auf **Remap Selected System** (Ausgewähltes System neu zuordnen).

# Remoteserver-Verwaltungstools

18.05.2020 • 21 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Dieses Thema unterstützt die Remoteserver-Verwaltungstools für Windows 10.

## IMPORTANT

Ab dem Windows 10-Update vom Oktober 2018 ist RSAT als Sammlung von **Features bei Bedarf** in Windows 10 selbst enthalten. Weitere Anweisungen zur Installation finden Sie unter [Wann welche RSAT-Version verwendet werden sollte](#).

Mit RSAT können IT-Administratoren Windows Server-Rollen und -Funktionen von einem Windows 10-PC aus verwalten.

Die Remoteserver-Verwaltungstools beinhalten Server-Manager, Microsoft Management Console-Snap-Ins (MMC), Konsolen, Windows PowerShell-Cmdlets und -Anbieter sowie Befehlszeilentools für die Verwaltung von Rollen und Features, die auf Windows Server ausgeführt werden.

Zu den Remoteserver-Verwaltungstools zählen Windows PowerShell-Cmdlet-Module, die zum Verwalten von Rollen und Features verwendet werden können, die auf Remoteservern ausgeführt werden. Obwohl die Windows PowerShell-Remoteverwaltung unter Windows Server 2016 standardmäßig aktiviert ist, ist sie unter Windows 10 standardmäßig nicht aktiviert. Führen Sie zur Ausführung von Cmdlets, die Teil der Remoteserver-Verwaltungstools sind, für einen Remoteserver `Enable-PSRemoting` in einer Windows PowerShell-Sitzung aus, die mit erhöhten Benutzerrechten (d. h. „Als Administrator ausführen“) nach der Installation der Remoteserver-Verwaltungstools auf Ihrem Windows-Clientcomputer geöffnet wurde.

## Remoteserver-Verwaltungstools für Windows 10

Verwenden Sie die Remoteserver-Verwaltungstools für Windows 10, um bestimmte Technologien auf Computern zu verwalten, auf denen Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 und in eingeschränkten Fällen Windows Server 2012 oder Windows Server 2008 R2 ausgeführt wird.

Die Remoteserver-Verwaltungstools für Windows 10 umfassen Unterstützung für die Remoteverwaltung von Computern, auf denen die Server Core-Installationsoption oder die Konfiguration „Minimale Serverschnittstelle“ von Windows Server 2016. Windows Server 2012 R2 ausgeführt wird (in eingeschränkten Fällen auch die Server Core-Installationsoptionen von Windows Server 2012). Die Remoteserver-Verwaltungstools für Windows 10 können nicht unter allen Versionen des Windows Server-Betriebssystems installiert werden.

### Tools, die in dieser Version verfügbar sind

Eine Liste der Tools, die in den Remoteserver-Verwaltungstools für Windows 10 verfügbar sind, finden Sie in der Tabelle unter [Remoteserver-Verwaltungstools \(Remote Server Administration Tools, RSAT\) für Windows-Betriebssysteme](#).

### Systemanforderungen

Remoteserver-Verwaltungstools für Windows 10 können nur auf Computern mit Windows 10 installiert werden. Remoteserver-Verwaltungstools können nicht auf Computern mit Windows RT 8.1 oder auf anderen SOC-Geräten (System on a Chip) installiert werden.

Remoteserver-Verwaltungstools für Windows 10 können unter x86- und x64-basierten Editionen von Windows 10

ausgeführt werden.

#### **IMPORTANT**

Es ist nicht ratsam, Remoteserver-Verwaltungstools für Windows 10 auf einem Computer zu installieren, auf dem Verwaltungsprogramme für Windows 8.1, Windows 8, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 oder Windows 2000 Server ausgeführt werden. Entfernen Sie alle älteren Versionen von Verwaltungsprogrammen oder Remoteserver-Verwaltungstools – einschließlich ältere Vorabversionen und Versionen der Tools für unterschiedliche Sprachen oder Gebietsschemas – vom Computer, bevor Sie die Remoteserver-Verwaltungstools für Windows 10 installieren.

Um diese Version von Server-Manager für den Zugriff auf und die Verwaltung von Remoteservern mit Windows Server 2012 R2 , Windows Server 2012 oder Windows Server 2008 R2 zu verwenden, müssen Sie mehrere Updates installieren, um die älteren Windows Server-Betriebssysteme mit Hilfe von Server-Manager verwaltbar zu machen. Ausführliche Informationen dazu, wie Sie Windows Server 2012 R2, Windows Server 2012 und Windows Server 2008 R2 für die Verwaltung mit dem Server-Manager in den Remoteserver-Verwaltungstools für Windows 10 vorbereiten können, finden Sie unter [Verwalten von mehreren Remoteservern mit dem Server-Manager](#).

Die Windows PowerShell- und Server-Manager-Remoteverwaltung muss auf Remoteservern aktiviert werden, um diese mithilfe von Tools verwalten zu können, die Teil der Remoteserver-Verwaltungstools für Windows 10 sind. Remoteverwaltung ist auf Servern mit Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 standardmäßig aktiviert. Weitere Informationen zum Aktivieren der deaktivierten Remoteverwaltung finden Sie unter [Verwalten von mehreren Remoteservern mit dem Server-Manager](#).

## Installieren, Deinstallieren und Aktivieren/Deaktivieren der RSAT-Tools

### **Verwenden von FoD (Features on Demand, Features bei Bedarf), um bestimmte RSAT-Tools unter dem Windows 10 October 2018 Update oder höher zu installieren**

Ab dem Windows 10-Update vom Oktober 2018 ist RSAT als Sammlung von Features bei Bedarf in Windows 10 selbst enthalten. Anstatt ein RSAT-Paket herunterzuladen, können Sie jetzt einfach zu **Optionale Features verwalten** unter **Einstellungen** navigieren und auf **Feature hinzufügen** klicken, um die Liste der verfügbaren RSAT-Tools anzuzeigen. Wählen Sie die gewünschten RSAT-Tools aus, und installieren Sie sie. Um den Installationsfortschritt anzuzeigen, klicken Sie auf die Schaltfläche **Zurück**, um den Status auf der Seite **Optionale Features verwalten** anzuzeigen.

Weitere Informationen finden Sie in der [Liste der RSAT-Tools, die über **Features bei Bedarf** verfügbar ist] (<https://docs.microsoft.com/windows-hardware/manufacture/desktop/features-on-demand-non-language-fod#remote-server-administration-tools-rsat>). Zusätzlich zur Installation über die grafische App für **Einstellungen** können Sie auch bestimmte RSAT-Tools über die Befehlszeile oder über Automatisierung mithilfe von [DISM/Add-Capability](#) installieren.

Ein Vorteil von Features bei Bedarf besteht darin, dass die installierten Features über Windows 10-Versionsupgrades hinweg bestehen bleiben.

### **So deinstallieren Sie bestimmte RSAT-Tools unter dem Windows 10-Update vom Oktober 2018 oder höher (nach der Installation mit FoD)**

Öffnen Sie unter Windows 10 die App **Einstellungen**, navigieren Sie zu **Optionale Features verwalten**, wählen Sie die gewünschten RSAT-Tools aus, die Sie entfernen möchten, und deinstallieren Sie sie dann. Beachten Sie, dass Abhängigkeiten in einigen Fällen manuell deinstalliert werden müssen. Insbesondere wenn das RSAT-Tool A vom RSAT-Tool B benötigt wird, tritt bei der Deinstallation von RSAT-Tool A ein Fehler auf, wenn RSAT-Tool B noch installiert ist. Deinstallieren Sie in diesem Fall zuerst das RSAT-Tool B, und deinstallieren Sie dann das RSAT-Tool A. Beachten Sie auch, dass das Deinstallieren eines RSAT-Tools in einigen Fällen möglicherweise zu gelingen scheint, auch wenn das Tool noch installiert ist. In diesem Fall wird das Tool durch das Neustarten des PCs entfernt.

Weitere Informationen finden Sie in der [Liste der RSAT-Tools und seiner Abhängigkeiten](#). Zusätzlich zur Deinstallation über die grafische App für Einstellungen können Sie auch bestimmte RSAT-Tools über die Befehlszeile oder über Automatisierung mithilfe von [DISM/Remove-Capability](#) deinstallieren.

### **Wann sollte welche RSAT-Version verwendet werden?**

Wenn Sie eine Version von Windows 10 vor dem Update vom Oktober 2018 (1809) verwenden, können Sie **Features bei Bedarf** nicht verwenden. Sie müssen das RSAT-Paket herunterladen und installieren.

- **Installieren Sie RSAT-FoDs direkt aus Windows 10, wie oben beschrieben:** Bei der Installation unter Windows 10, Update vom Oktober 2018 (1809) oder höher für die Verwaltung von Windows Server 2019 oder früheren Versionen.
- **Laden Sie das WS\_1803 RSAT-Paket herunter, und installieren Sie es wie unten beschrieben:** Bei der Installation unter Windows 10, Update vom April 2018 (1803) oder früher für die Verwaltung von Windows Server, Version 1803 oder Windows Server, Version 1709.
- **Laden Sie das WS\_2016 RSAT-Paket herunter, und installieren Sie es wie unten beschrieben:** Bei der Installation unter Windows 10, Update vom April 2018 (1803) oder früher für die Verwaltung von Windows Server 2016 oder früheren Versionen.

#### **Herunterladen des RSAT-Pakets, um die Remoteserver-Verwaltungstools für Windows 10 zu installieren**

1. Laden Sie die Remoteserver-Verwaltungstools für das Windows 10-Paket aus dem [Microsoft Download Center](#) herunter. Sie können das Installationsprogramm entweder über die Download Center-Website ausführen oder das Downloadpaket auf einem lokalen Computer oder einer lokalen Freigabe speichern.

#### **IMPORTANT**

Sie können Remoteserver-Verwaltungstools für Windows 10 nur auf Computern installieren, die Windows 10 ausführen. Remoteserver-Verwaltungstools können nicht auf Computern mit Windows RT 8.1 oder auf anderen SOC-Geräten (System on a Chip) installiert werden.

2. Wenn Sie das Downloadpaket auf einem lokalen Computer oder einer Freigabe speichern, doppelklicken Sie auf das Installationsprogramm **WindowsTH-KB2693643-x64.msu** oder **WindowsTH-KB2693643-x86.msu**. Dies richtet sich nach der Architektur des Computers, auf dem Sie die Tools installieren möchten.
3. Wenn Sie im Dialogfeld **Eigenständiges Windows Update-Installationsprogramm** zum Installieren des Updates aufgefordert werden, klicken Sie auf **Ja**.
4. Lesen Sie die Lizenzbedingungen, und akzeptieren Sie sie. Klicken Sie auf **Ich stimme zu**.
5. Es dauert einige Minuten, bis die Installation beendet ist.

#### **So deinstallierst du die Remoteserver-Verwaltungstools für Windows 10 (nach der Installation des RSAT-Pakets)**

1. Klicken Sie auf dem Desktop auf **Start, Alle Apps, Windows System** und **Systemsteuerung**.
2. Klicken Sie unter **Programme** auf **Programm deinstallieren**.
3. Klicken Sie auf **Installierte Updates anzeigen**.
4. Klicken Sie mit der rechten Maustaste auf **Update für Microsoft Windows (KB2693643)**, und klicken Sie dann auf **Deinstallieren**.
5. Wenn Sie gefragt werden, ob Sie das Update wirklich deinstallieren möchten, klicken Sie auf **Ja**.

#### **So deaktivieren Sie bestimmte Tools (nach der Installation des RSAT-Pakets)**

6. Klicken Sie auf dem Desktop auf **Start, Alle Apps, Windows System** und **Systemsteuerung**.
7. Klicken Sie auf **Programme** und dann unter **Programme und Features** auf **Windows-Features ein- oder ausschalten**.

8. Erweitern Sie im Dialogfeld **Windows-Features** die Option **Remoteserver-Verwaltungstools** und dann entweder den Unterpunkt **Rollenverwaltungstools** oder **Featureverwaltungstools**.
9. Deaktivieren Sie die Kontrollkästchen für alle Tools, die Sie deaktivieren möchten.

#### **NOTE**

Wenn Sie Server-Manager deaktivieren, muss der Computer neu gestartet werden, und Tools, auf die über das Menü **Extras** von Server-Manager zugegriffen werden konnte, müssen über den Ordner **Verwaltungstools** geöffnet werden.

10. Klicken Sie auf **OK**, wenn Sie alle Tools deaktiviert haben, die Sie nicht verwenden möchten.

## **Ausführen der Remoteserver-Verwaltungstools**

#### **NOTE**

Nach der Installation der Remoteserver-Verwaltungstools für Windows 10 wird der Ordner **Verwaltungstools** im **Startmenü** angezeigt. Sie können von folgenden Orten auf die Tools zugreifen.

- Das Menü **Extras** in der Server-Manager-Konsole.
- **Systemsteuerung\System und Sicherheit\Verwaltungstools**
- Eine Verknüpfung aus dem Ordner **Verwaltungstools**, die auf dem Desktop gespeichert wird (klicken Sie dazu mit der rechten Maustaste auf den Link **Systemsteuerung\System und Sicherheit\Verwaltungstools** und dann auf **Verknüpfung erstellen**).

Die als Teil der Remoteserver-Verwaltungstools für Windows 10 installierten Tools können nicht zum Verwalten des lokalen Clientcomputers verwendet werden. Unabhängig vom ausgeführten Tool müssen Sie einen Remoteserver oder mehrere Remoteserver angeben, für die das Tool ausgeführt werden soll. Da die meisten Tools in Server-Manager integriert sind, fügen Sie Remoteserver, die Sie verwalten möchten, dem Server Manager-Serverpool hinzu. Danach können Sie den Server mit den Tools im Menü **Extras** verwalten. Weitere Informationen zum Hinzufügen von Servern zum Serverpool und zum Erstellen benutzerdefinierter Gruppen von Servern finden Sie unter [Hinzufügen von Servern zu Server-Manager](#) und [Erstellen und Verwalten von Servergruppen](#).

In den Remoteserver-Verwaltungstools für Windows 10 wird auf alle GUI-basierten Serververwaltungstools (z. B. MMC-Snap-Ins und Dialogfelder) über das Menü **Extras** der Server-Manager-Konsole zugegriffen. Obwohl auf dem Computer mit den Remoteserver-Verwaltungstools für Windows 10 ein clientbasiertes Betriebssystem ausgeführt wird, wird Server-Manager (in Remoteserver-Verwaltungstools für Windows 10 integriert) auf dem Clientcomputer standardmäßig automatisch geöffnet. Beachten Sie, dass in der Server-Manager-Konsole, die auf einem Clientcomputer ausgeführt wird, keine Seite **Lokaler Server** vorhanden ist.

**So starten Sie den Server-Manager auf einem Clientcomputer**

1. Klicken Sie im Menü **Start** auf **Alle Apps** und **Verwaltungstools**.

2. Klicken Sie im Ordner **Verwaltungstools** auf **Server-Manager**.

Obwohl sie im Menü **Extras** der Server-Manager-Konsole nicht aufgeführt sind, werden Windows PowerShell-Cmdlets und Eingabeaufforderungsverwaltungstools für Rollen und Features ebenfalls als Teil der Remoteserver-Verwaltungstools installiert. Wenn Sie z. B. eine Windows PowerShell-Sitzung mit erhöhten Benutzerrechten („Als Administrator ausführen“) öffnen und das Cmdlet `Get-Command -Module RDManagement` ausführen, ist in den Ergebnissen eine Liste von Remotedesktopdienste-Cmdlets enthalten, die nach der Installation der Remoteserver-Verwaltungstools für die Ausführung auf dem lokalen Computer verfügbar sind. Dazu müssen die Cmdlets jedoch einen Remoteserver als Ziel verwenden, auf dem die Rolle „Remotedesktopdienste“ ganz oder teilweise ausgeführt wird.

**So starten Sie Windows PowerShell mit erhöhten Benutzerrechten („Als Administrator ausführen“)**

1. Klicken Sie im Menü **Start** auf **Alle Apps, Windows System** und **Windows PowerShell**.

2. Wenn Sie Windows PowerShell als Administrator über den Desktop ausführen möchten, klicken Sie mit der rechten Maustaste auf die **Windows PowerShell**-Verknüpfung und dann auf **Als Administrator ausführen**.

#### NOTE

Sie können eine Windows PowerShell-Sitzung starten, die einen bestimmten Server als Ziel verwendet, indem Sie mit der rechten Maustaste auf einer Rollen- oder Gruppenseite von Server-Manager auf einen verwalteten Server klicken und dann auf **Windows PowerShell** klicken.

## Bekannte Probleme

### Problem: RSAT-FoD-Installation schlägt mit Fehlercode 0x800f0954 fehl

**Auswirkungen:** RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018) in WSUS-/Configuration Manager-Umgebungen

**Lösung:** Zum Installieren von FoDs auf einem in die Domäne eingebundenen PC, der Updates über WSUS oder Configuration Manager erhält, müssen Sie eine Gruppenrichtlinieneinstellungen ändern, um das Herunterladen von FoDs direkt von Windows Update oder aus einer lokalen Freigabe zu aktivieren. Weitere Informationen und Anweisungen zum Ändern dieser Einstellung finden Sie unter [Vorgehensweise: Verfügbarmachen von Features on Demand und Language Packs bei Verwendung von WSUS/SCCM](#).

### Problem: RSAT-FoD-Installation über die App „Einstellungen“ zeigt Status/Fortschritt nicht an

**Auswirkungen:** RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018)

**Lösung:** Um den Installationsfortschritt anzuzeigen, klicken Sie auf die Schaltfläche **Zurück**, um den Status auf der Seite **Optionalen Features verwalten** anzuzeigen.

### Problem: RSAT-FoD-Deinstallation über die App „Einstellungen“ schlägt möglicherweise fehl

**Auswirkungen:** RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018)

**Lösung:** In einigen Fällen sind Deinstallationsfehler darauf zurückzuführen, dass Abhängigkeiten manuell deinstalliert werden müssen. Insbesondere wenn das RSAT-Tool A vom RSAT-Tool B benötigt wird, tritt bei der Deinstallation von RSAT-Tool A ein Fehler auf, wenn RSAT-Tool B noch installiert ist. Deinstallieren Sie in diesem Fall zuerst das RSAT-Tool B, und deinstallieren Sie dann das RSAT-Tool A. Weitere Informationen finden Sie in der Liste der RSAT-FoDs einschließlich ihrer Abhängigkeiten.

### Problem: Die RSAT-FoD-Installation ist anscheinend erfolgreich, aber das Tool ist weiterhin installiert.

**Auswirkungen:** RSAT-FoDs unter Windows 10, Version 1809 (Update vom Oktober 2018)

**Lösung:** Das Tool wird durch Neustarten des PCs entfernt.

### Problem: RSAT fehlt nach dem Windows 10-Upgrade

**Auswirkungen:** Beliebige RSAT .MSU-Paketinstallation (vor RSAT-FoDs) wird nicht automatisch neu installiert.

**Lösung:** Eine RSAT-Installation kann über Betriebssystemupgrades hinweg nicht beibehalten werden, weil RSAT .MSU als Windows Update-Paket übermittelt wird. Installieren Sie RSAT nach dem Upgrade von

Windows 10 erneut. Beachten Sie, dass diese Einschränkung einer der Gründe für die Umstellung auf FoDs ab Windows 10, Version 1809 ist. Die installierten RSAT-FoDs bleiben in zukünftigen Windows 10-Versionsupgrades erhalten.

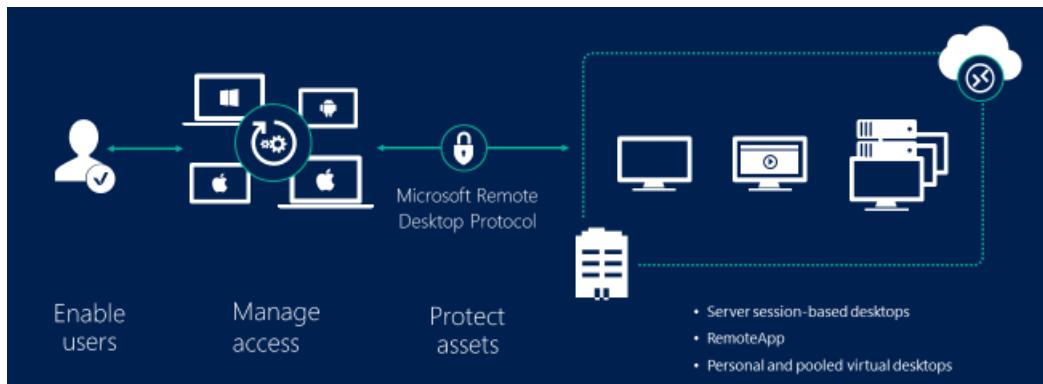
## Weitere Informationen

- [Remoteserver-Verwaltungstools für Windows 10](#)
- [Remoteserver-Verwaltungstools \(Remote Server Administration Tools, RSAT\) für Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2](#)

# Willkommen bei den Remotedesktopdiensten

24.04.2020 • 4 minutes to read • [Edit Online](#)

Remotedesktopdienste (RDS) sind die Plattform der Wahl zum Erstellen von Virtualisierungslösungen für jede Anforderung von Endbenutzern, einschließlich der Bereitstellung individueller virtualisierter Anwendungen, sicherem mobilem und Remote-Desktopzugriff und der Möglichkeit für Endbenutzer, ihre Anwendungen und Desktops in der Cloud auszuführen.



RDS bietet flexible Bereitstellung, Kosteneffizienz und Erweiterbarkeit: alles realisiert mithilfe einer Vielzahl von Bereitstellungsoptionen, einschließlich Windows Server 2016 für lokale Bereitstellungen, Microsoft Azure für Cloudbereitstellungen und eines robusten Spektrums an Partnerlösungen.

Abhängig von Ihrer Umgebung und Ihren Wünschen können Sie die RDS-Lösung für sitzungsbasierte Virtualisierung, als virtuelle Desktopinfrastruktur (VDI) oder als Kombination daraus einrichten:

- **Sitzungsbasierte Virtualisierung:** Nutze die Rechenleistung von Windows Server, um eine kostengünstige Multisessionumgebung für die täglichen Workloads deiner Benutzer bereitzustellen.
- **VDI:** Nutzen Sie den Windows-Client, um die hohe Leistung, App-Kompatibilität und Vertrautheit zu bieten, die Ihre Benutzer von ihrer Windows-Desktopdarstellung gewohnt sind.

Innerhalb dieser Virtualisierungsumgebungen besitzen Sie zusätzliche Flexibilität in dem, was Sie für Ihre Benutzer veröffentlichen:

- **Desktops:** Bieten Sie Ihren Benutzern eine vollständige Desktoperfahrung mit einer Vielzahl von Anwendungen, die Sie installieren und verwalten. Ideal für Benutzer, die diese Computer als primäre Arbeitsstationen nutzen oder von Thin Clients umsteigen, wie etwa von MultiPoint-Diensten.
- **RemoteApps:** Geben Sie einzelne Anwendungen an, die auf dem virtuellen Computer gehostet/ausgeführt werden, sich aber verhalten, als würden sie wie lokale Anwendungen auf dem Desktop des Benutzers ausgeführt. Die Apps haben einen eigenen Eintrag in der Taskleiste, ihre Größe lässt sich verändern, und sie können zwischen Monitoren verschoben werden. Ideal zum Bereitstellen und Verwalten von wichtigen Anwendungen in der sicheren Remoteumgebung, trotzdem können Benutzer an ihren eigenen Desktops arbeiten und sie anpassen.

Für Umgebungen, in denen Kosteneffizienz kritisch ist und Sie die Vorteile der Bereitstellung von vollständigen Desktops in einer sitzungsbasierten Virtualisierungsumgebung ausweiten möchten, können Sie [MultiPoint-Dienste](#) verwenden, um den besten Wert zu realisieren.

Dank dieser Optionen und Konfiguration haben Sie die Flexibilität, die von Ihren Benutzern benötigten Desktops und Anwendungen remote, sicher und kostengünstig bereitzustellen.

## Nächste Schritte

Hier sind einige weiterführende Schritte, die Ihnen helfen sollen, ein besseres Verständnis von RDS zu entwickeln und sogar mit der Bereitstellung Ihrer eigenen Umgebung zu beginnen:

- Verstehen der [unterstützten Konfigurationen](#) für RDS mit den verschiedenen Versionen von Windows und Windows Server
- [Planen und Entwerfen](#) einer RDS-Umgebung, die verschiedenen Anforderungen Rechnung trägt, beispielsweise Hochverfügbarkeit und mehrstufige Authentifizierung.
- Überprüfen der [Remotedesktopdienste-Architekturmodelle](#), die sich optimal für Ihre gewünschte Umgebung eignen.
- Beginnen der [Bereitstellung Ihrer RDS-Umgebung mit ARM und Azure Marketplace](#).

# Remotezugriff

27.03.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

Im Handbuch für den Remote Zugriff erhalten Sie eine Übersicht über die RAS-Server Rolle in Windows Server 2016 und die folgenden Themen:

- [Always on VPN-Bereitstellungs Handbuch](#)
- [Border Gateway Protocol \(BGP\)](#)
- [RAS-Gateway](#)
- [RAS-Serverrolle: Dokumentation](#)
- [RAS-Gateway für SDN](#)
- [Virtual Private Networking \(VPN\)](#)

Weitere Informationen zu anderen Netzwerktechnologien finden Sie unter [Netzwerk in Windows Server 2016](#).

Die Remote Zugriffs-Server Rolle ist eine logische Gruppierung dieser verwandten Netzwerk Zugriffs Technologien: [RAS \(Remote Access Service\)](#), [Routing](#) und [webanwendungsproxy](#). Diese Technologien sind die *Rollendienste* der Serverrolle "Remotezugriff". Wenn Sie die Remote Zugriffs-Server Rolle mit dem **Assistenten zum Hinzufügen von Rollen und Features** oder mit Windows PowerShell installieren, können Sie einen oder mehrere dieser drei Rollen Dienste installieren.

## IMPORTANT

Versuchen Sie nicht, den Remote Zugriff auf einem virtuellen Computer (VM-) in Microsoft Azure bereitzustellen. Die Verwendung des Remote Zugriffs in Microsoft Azure wird nicht unterstützt. Sie können den Remote Zugriff auf einem virtuellen Azure-Computer nicht verwenden, um VPN, DirectAccess oder andere Remote Zugriffs Funktionen in Windows Server 2016 oder früheren Versionen von Windows Server bereitzustellen. Weitere Informationen finden Sie unter [Microsoft Server Software Support for Microsoft Azure Virtual Machines](#).

## RAS-Dienst (RAS)-RAS-Gateway

Wenn Sie den **DirectAccess-und VPN-Rollen Dienst (RAS)** installieren, stellen Sie das RAS-Gateway (**RAS-Gateway**)bereit. Sie können das RAS-Gateway mit einem virtuellen privaten Netzwerk eines einzelnen Mandanten-RAS-Gateways (VPN) Server, eines mehr Instanzen fähigen RAS-Gateway-VPN-Servers und als DirectAccess-Server bereitstellen.

- **RAS-Gateway: einzelnerMandant.** Mithilfe des RAS-Gateways können Sie VPN-Verbindungen bereitstellen, um Endbenutzern Remote Zugriff auf das Netzwerk und die Ressourcen Ihrer Organisation zu bieten. Wenn auf Ihren Clients Windows 10 ausgeführt wird, können Sie Always on VPN bereitstellen, das immer dann eine permanente Verbindung zwischen Clients und Ihrem Organisations Netzwerk unterhält, wenn Remote Computer mit dem Internet verbunden sind. Mit dem RAS-Gateway können Sie auch eine Site-to-Site-VPN-Verbindung zwischen zwei Servern an unterschiedlichen Standorten erstellen, z. b. zwischen Ihrer primären Niederlassung und einer Zweigstelle, und die Netzwerk Adressübersetzung (NAT-) verwenden, damit Benutzer im Netzwerk auf externe Ressourcen zugreifen können, z. b. das Internet. Außerdem unterstützt das RAS-Gateway Border Gateway Protocol (BGP), das dynamische Routing Dienste bereitstellt, wenn Ihre Remote Niederlassungen auch Edge-Gateways aufweisen, die BGP unterstützen.
- **RAS-Gateway: mehrInstanzen fähig.** Wenn Sie die Hyper-V-Netzwerkvirtualisierung verwenden oder VM-

Netzwerke mit virtuellen lokalen Netzwerken (VLANs) bereitgestellt werden, können Sie das RAS-Gateway als mehrinstanzfähiges, softwarebasiertes Edge-Gateway und Router bereitstellen. Beim RAS-Gateway können clouddienstanbieter (CSPs) und Unternehmen das Routing von Daten Center- und clouddatenverkehr zwischen virtuellen und physischen Netzwerken, einschließlich Internet, ermöglichen. Mit dem RAS-Gateway können Ihre Mandanten Punkt-Standort-Standort-VPN-Verbindungen verwenden, um von überall aus auf Ihre VM-Netzwerkressourcen im Rechenzentrum zuzugreifen. Sie können Mandanten auch Standort-zu-Standort-VPN-Verbindungen zwischen ihren Remote Standorten und Ihrem CSP-Rechenzentrum bereitstellen. Darüber hinaus können Sie das RAS-Gateway mit BGP für dynamisches Routing konfigurieren, und Sie können die Netzwerk Adressübersetzung (NAT-) aktivieren, um den Internet Zugriff für virtuelle Computer in VM-Netzwerken bereitzustellen.

#### IMPORTANT

Das RAS-Gateway mit mehr Instanzen fähigen Funktionen ist auch in Windows Server 2012 R2 verfügbar.

- **Always on-VPN.** Always on-VPN ermöglicht Remote Benutzern den sicheren Zugriff auf freigegebene Ressourcen, Intranetwebsites und Anwendungen in einem internen Netzwerk, ohne eine Verbindung mit einem VPN herzustellen.

Weitere Informationen finden Sie unter [RAS-Gateway](#) und [Border Gateway Protocol \(BGP\)](#).

## Routing

Sie können den Remote Zugriff verwenden, um Netzwerk Datenverkehr zwischen Subnetzen in Ihrem lokalen Netzwerk weiterzuleiten. Das Routing bietet Unterstützung für NAT-Router (Netzwerk Adressübersetzung), LAN-Router mit BGP, Routing Information Protocol (RIP) und Multicast fähige Router unter Verwendung von IGMP (Internet Group Management Protocol). Als Router mit vollem Funktionsumfang können Sie RAS entweder auf einem Server Computer oder als virtueller Computer (VM) auf einem Computer bereitstellen, auf dem Hyper-V ausgeführt wird.

Verwenden Sie zum Installieren des Remote Zugriffs als LAN-Router entweder den Assistenten zum Hinzufügen von Rollen und Features in Server-Manager, und wählen Sie die **Remote Zugriffs** -Server Rolle und den **Routing** Rollen Dienst aus. oder geben Sie den folgenden Befehl an einer Windows PowerShell-Eingabeaufforderung ein, und drücken Sie dann die EINGABETASTE.

```
Install-RemoteAccess -VpnType RoutingOnly
```

## Webanwendungs Proxy

Der webanwendungsproxy ist ein Remote Zugriffs-Rollen Dienst in Windows Server 2016. Der Webanwendungsproxy bietet Reverseproxyfunktionen für Webanwendungen in Ihrem Unternehmensnetzwerk, damit Benutzer außerhalb des Unternehmensnetzwerks von allen Geräten auf die Anwendungen zugreifen können. Der webanwendungsproxy authentifiziert den Zugriff auf Webanwendungen mit Active Directory-Verbunddienste (AD FS) (AD FS) und fungiert auch als AD FS Proxy.

Verwenden Sie zum Installieren des Remote Zugriffs als webanwendungsproxy den Assistenten zum Hinzufügen von Rollen und Features in Server-Manager, und wählen Sie die **Server** Rolle RAS und den **webanwendungsproxy** -Rollen Dienst aus. oder geben Sie den folgenden Befehl an einer Windows PowerShell-Eingabeaufforderung ein, und drücken Sie dann die EINGABETASTE.

```
Install-RemoteAccess -VpnType SstpProxy
```

Weitere Informationen finden Sie unter [webanwendungsproxy](#).

---

# Always on der VPN-Bereitstellung für Windows Server und Windows 10

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Remote Zugriff](#)
- [Weiter: Erfahren Sie mehr über die Always on VPN-Features und -Funktionen](#)

Always on-VPN bietet eine einheitliche Lösung für den Remote Zugriff und unterstützt in die Domäne eingebundenen, nicht in die Domäne eingebundenen (Arbeitsgruppen) oder Azure AD –Geräte, auch private Geräte. Mit Always On-VPN muss der Verbindungstyp nicht ausschließlich Benutzer oder Gerät, sondern kann eine Kombination aus beidem sein. Sie könnten z.B. die Geräteauthentifizierung für die Remotegeräteverwaltung aktivieren und dann die Benutzerauthentifizierung für Konnektivität mit internen Unternehmenssites und -diensten.

## Erforderliche Komponenten

Wahrscheinlich verfügen Sie über die bereitgestellten Technologien, die Sie zum Bereitstellen Always on VPN verwenden können. Abgesehen von Ihren DC/DNS-Servern erfordert die Always on-VPN-Bereitstellung einen NPS-Server (RADIUS), einen Zertifizierungsstellen Server (ca) und einen RAS-Server (Routing/VPN). Nachdem Sie die Infrastruktur eingerichtet haben, müssen Sie Clients registrieren und die Clients dann mithilfe mehrerer Netzwerk Änderungen sicher mit Ihrem lokalen Standort verbinden.

- Active Directory Domänen Infrastruktur, einschließlich eines oder mehrerer Domain Name System (DNS)-Server. Sowohl interne als auch externe Domain Name System (DNS-Zonen) sind erforderlich. dabei wird davon ausgegangen, dass die interne Zone eine delegierte Unterdomäne der externen Zone ist (z. b. Corp.contoso.com und contoso.com).
- Active Directory basierte Public Key-Infrastruktur (PKI) und Active Directory Zertifikat Dienste (AD CS).
- Server (virtuell oder physisch, vorhandener oder neuer) zum Installieren von Netzwerk Richtlinien Server (NPS). Wenn Sie bereits über NPS-Server in Ihrem Netzwerk verfügen, können Sie eine vorhandene NPS-Serverkonfiguration ändern, anstatt einen neuen Server hinzuzufügen.
- Remote Zugriff als RAS-Gateway-VPN-Server mit einer kleinen Teilmenge von Features, die IKEv2-VPN-Verbindungen und LAN-Routing unterstützen.
- Umkreis Netzwerk, das zwei Firewalls umfasst. Stellen Sie sicher, dass ihre Firewalls den Datenverkehr, der für die VPN-und RADIUS-Kommunikation erforderlich ist, ordnungsgemäß funktionieren. Weitere Informationen finden Sie unter [Übersicht über Always on VPN-Technologie](#).
- Physischer Server oder virtueller Computer (VM) in Ihrem Umkreis Netzwerk mit zwei physischen Ethernet-Netzwerkadapters, um den Remote Zugriff als RAS-Gateway-VPN-Server zu installieren. Virtuelle Computer erfordern ein virtuelles LAN (VLAN) für den Host.
- Sie müssen mindestens Mitglied der Gruppe Administratoren oder einer entsprechenden Gruppe sein.
- Lesen Sie den Abschnitt Planning dieses Handbuchs, um sicherzustellen, dass Sie für diese Bereitstellung vorbereitet sind, bevor Sie die Bereitstellung ausführen.
- Überprüfen Sie die Entwurfs- und Bereitstellungs Handbücher für die einzelnen verwendeten Technologien. Mithilfe dieser Leitfäden können Sie feststellen, ob die Bereitstellungs Szenarien die Dienste und die Konfiguration bereitstellen, die Sie für das Netzwerk Ihrer Organisation benötigen. Weitere Informationen finden Sie unter [Übersicht über Always on VPN-Technologie](#).

- Die Verwaltungsplattform Ihrer Wahl für die Bereitstellung der Always on-VPN-Konfiguration, da der CSP nicht Hersteller spezifisch ist.

#### **IMPORTANT**

Für diese Bereitstellung ist es nicht erforderlich, dass auf Ihren Infrastruktur Servern, z. b. Computern, auf denen Active Directory Domain Services, Active Directory Zertifikat Dienste und Netzwerk Richtlinien Server ausgeführt wird, Windows Server 2016 ausgeführt wird. Sie können frühere Versionen von Windows Server, wie z. b. Windows Server 2012 R2, für die Infrastruktur Server und für den Server verwenden, auf dem Remote Zugriff ausgeführt wird.

Versuchen Sie nicht, den Remote Zugriff auf einem virtuellen Computer (VM) in Microsoft Azure bereitzustellen. Die Verwendung des Remote Zugriffs in Microsoft Azure wird nicht unterstützt, einschließlich RAS-VPN und DirectAccess. Weitere Informationen finden Sie [unter Microsoft Server Software Support for Microsoft Azure Virtual Machines](#).

## Informationen zu dieser Bereitstellung

Die bereitgestellten Anweisungen führen Sie durch die Bereitstellung des Remote Zugriffs als ein einzelnes Mandanten-VPN-RAS-Gateway für Punkt-zu-Standort-VPN-Verbindungen mithilfe eines der unten erwähnten Szenarien für Remote Client Computer, auf denen Windows 10 ausgeführt wird. Außerdem finden Sie Anweisungen zum Ändern einiger Ihrer vorhandenen Infrastruktur für die Bereitstellung. Außerdem finden Sie in dieser Bereitstellung Links, die Ihnen helfen, mehr über den VPN-Verbindungsprozess, die zu konfigurier fähigen Server, den profileXML VPnv2 CSP-Knoten und andere Technologien zum Bereitstellen Always on VPN zu erfahren.

### Always on von VPN-Bereitstellungs Szenarien:

- Stellen Sie nur Always on-VPN bereit.
- Stellen Sie Always on-VPN mit bedingtem Zugriff für VPN-Konnektivität mithilfe Azure AD bereit.

Weitere Informationen und einen Workflow der dargestellten Szenarien finden Sie unter Bereitstellen [Always on VPN](#).

## Bereitstellung in dieser Bereitstellung nicht

Diese Bereitstellung stellt keine Anweisungen für Folgendes bereit:

- Active Directory Domain Services (AD DS).
- Active Directory Zertifikat Dienste (AD CS) und eine Public Key-Infrastruktur (PKI).
- Dynamic Host Configuration-Protokoll (DHCP).
- Netzwerkhardware, z. b. Ethernet-Verkabelung, Firewalls, Switches und Hubs.
- Zusätzliche Netzwerkressourcen, z. b. Anwendungs-und Dateiserver, auf die Remote Benutzer über eine Always on VPN-Verbindung zugreifen können.
- Internet Konnektivität oder bedingter Zugriff für die Internet Konnektivität mit Azure AD. Weitere Informationen finden Sie unter [bedingter Zugriff in Azure Active Directory](#).

## Nächste Schritte

- [Weitere Informationen zu den Always on VPN-Features und-Funktionen](#)
- [Weitere Informationen zu den Always on-VPN-Erweiterungen](#)
- [Erfahren Sie mehr über die erweiterten Always on-VPN-Features](#)
- [Weitere Informationen zum Always on VPN-Technologie](#)
- [Beginnen der Planung Ihrer Always on-VPN-Bereitstellung](#)



# Always on von VPN-Features und-Funktionen

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows 10

- [Vorheriges: Always on der VPN-Bereitstellung für Windows Server und Windows 10](#)
- [Weiter: Weitere Informationen zu den Always on-VPN-Erweiterungen](#)

In diesem Thema erfahren Sie mehr über die Features und Funktionen von Always on-VPN. Die folgende Tabelle ist keine vollständige Liste, Sie enthält jedoch einige der gängigsten Features und Funktionen, die in Remote Zugriffs Lösungen verwendet werden.

## TIP

Wenn Sie derzeit DirectAccess verwenden, empfiehlt es sich, die Always on-VPN-Funktionalität sorgfältig zu untersuchen, um zu ermitteln, ob Sie alle Ihre Remote Zugriffs Anforderungen erfüllt, bevor Sie von DirectAccess zu Always on VPN migrieren.

FUNKTIONSBEREICH	ALWAYS ON VPN
Nahtlose, transparente Konnektivität mit dem Unternehmensnetzwerk.	Sie können Always on-VPN konfigurieren, um die automatische Auslösung basierend auf Anwendungsstart- oder Namespace Auflösungsanforderungen zu unterstützen.  Definieren mithilfe von: <b>VPNv2/Profile Name/AlwaysOn</b> <b>VPNv2/Profile Name/apptriggerlist</b> <b>VPNv2/Proxy/domainnameinformationlist/autolöst</b>
Verwendung eines dedizierten Infrastruktur Tunnels, um Konnektivität für Benutzer bereitzustellen, die nicht beim Unternehmensnetzwerk angemeldet sind.	Sie können diese Funktion durch Nutzen des Gerätetunnelfeatures im VPN-Profil verwenden.  <b>Hinweis:</b> Der Geräte Tunnel kann nur auf in die Domäne eingebundenen Geräten mithilfe von IKEv2 mit Computer Zertifikat Authentifizierung konfiguriert werden.  Definieren mithilfe von: <b>VPNv2/Profile Name/deaktivieren</b>

FUNKTIONSBEREICH	ALWAYS ON VPN
Verwendung von Manage-Out, um Remote Verbindungen mit Clients über Verwaltungssysteme im Unternehmensnetzwerk zuzulassen.	<p>Sie können diese Funktion durch Nutzen des Gerätetunnelfeatures im VPN-Profil verwenden in Kombination mit der Konfiguration der VPN-Verbindung, so dass die IP-Adressen der VPN-Schnittstelle mit internen DNS-Diensten dynamisch registriert wird.</p> <p><b>Hinweis:</b> Wenn Sie die Datenverkehrs Filter im Geräte Tunnel Profil aktivieren, wird der eingehende Datenverkehr (aus dem Unternehmensnetzwerk an den Client) vom Geräte Tunnel verweigert.</p> <p>Definieren mithilfe von:  <b>VPNv2/Profile Name/deaktivieren</b>  <b>VPNv2/Profile Name/registerdns</b></p>
Fallback, wenn sich Clients hinter Firewalls oder Proxy Servern befinden.	<p>Sie können auf SSTP (von IKEv2) zurückgreifen, indem Sie den automatischen Tunnel-/Protokolltyp innerhalb des VPN-Profils konfigurieren.</p> <p><b>Hinweis:</b> Der Benutzer Tunnel unterstützt SSTP und IKEv2, und der Geräte Tunnel unterstützt IKEv2 nur ohne Unterstützung für das SSTP-Fallback.</p> <p>Definieren mithilfe von:  <b>VPNv2/Profile</b>  <b>Name/nativeprofile/nativeprotocoltype</b></p>
Unterstützung für den End-to-Edge-Zugriffsmodus.	<p>Always On VPN bietet Konnektivität zu Unternehmensressourcen durch Tunnelrichtlinien, die die Authentifizierung und Verschlüsselung erfordern, bis sie das VPN-Gateway erreichen. Standardmäßig enden Tunnel-Sitzungen auf dem VPN-Gateway, das auch als Gateway IKEv2, End-to-Edge-Sicherheit funktioniert.</p>
Unterstützung für die Computerzertifikatauthentifizierung.	<p>Der IKEv2 Protocol Type, der als Teil der Always on VPN-Plattform verfügbar ist, unterstützt speziell die Verwendung von Computer-oder Computer Zertifikaten für die VPN-Authentifizierung.</p> <p><b>Hinweis:</b> IKEv2 ist das einzige unterstützte Protokoll für den Geräte Tunnel, und es gibt keine Support Option für das SSTP-Fallback.</p> <p>Definieren mithilfe von:  <b>VPNv2/Profile</b>  <b>Name/nativeprofile/Authentication/machinemethod</b></p>
Verwenden Sie Sicherheitsgruppen, um die Remote Zugriffs Funktionalität auf bestimmte Clients zu beschränken.	<p>Sie können Always On VPN konfigurieren, um die genaue Autorisierung bei Verwendung von RADIUS zu unterstützen, einschließlich der Verwendung von Sicherheitsgruppen zur Kontrolle des VPN-Zugriffs.</p>

FUNKTIONSBEREICH	ALWAYS ON VPN
Unterstützung für Server hinter einer Edge-Firewall oder einem NAT-Gerät.	<p>Always On VPN ermöglicht die Verwendung von Protokollen wie IKEv2 und SSTP, die die Verwendung eines VPN-Gateways hinter Edge-Firewall oder NAT-Geräten vollständig unterstützen.</p> <p><b>Hinweis:</b> Der Benutzer Tunnel unterstützt SSTP und IKEv2, und der Geräte Tunnel unterstützt IKEv2 nur ohne Unterstützung für das SSTP-Fallback.</p>
Möglichkeit zur Ermittlung der Intranetkonnektivität, wenn eine Verbindung mit dem Unternehmensnetzwerk besteht.	<p>Die Erkennung vertrauenswürdiger Netzwerke bietet die Möglichkeit, Unternehmensnetzwerk Verbindungen zu erkennen, und basiert auf einer Bewertung des Verbindungs spezifischen DNS-Suffixes, das Netzwerkschnittstellen und dem Netzwerk Profil zugewiesen ist.</p> <p>Definieren mithilfe von: <b>VPNv2/Profile Name/treudnetworkerkennungs</b></p>
Konformität mithilfe des Netzwerk Zugriffs Schutzes (Network Access Protection, NAP).	<p>Always On VPN-Client kann mit Azure integriert werden, um bedingten Zugriff der mehrstufigen Authentifizierung, Gerätekompatibilität oder einer Kombination aus beidem zu erzwingen. Beim Einhalten bedingter Zugriffsrichtlinien, stellt Azure AD ein kurzlebiges (standardmäßig 60 Minuten) IPsec-Authentifizierungszertifikat aus, das der Client dann als Gateway VPN-Authentifizierung verwenden kann. Die Geräte Konformität nutzt Configuration Manager/InTune-Konformitäts Richtlinien, die den Integritäts Nachweis Status des Geräts einschließen können. Zu diesem Zeitpunkt bietet der bedingte Zugriff von Azure VPN den besten Ersatz zu vorhandenen NAP-Projektmappen, obwohl keine Art Wiederherstellungsdienst oder Quarantäne-Netzwerkfunktionen vorhanden ist. Weitere Informationen finden Sie unter <a href="#">VPN und bedingter Zugriff</a>.</p> <p>Definieren mithilfe von: <b>VPNv2/Profile Name/devicecompliance</b></p>
Die Möglichkeit, zu definieren, welche Verwaltungsserver vor der Anmeldung für den Benutzer zugänglich sind.	<p>Sie können diese Funktionalität in Always on-VPN mit dem Geräte Tunnel Feature (nur in Version 1709 – für IKEv2 verfügbar) im VPN-Profil in Kombination mit Datenverkehrs Filtern erreichen, um zu steuern, auf welche Verwaltungssysteme im Unternehmensnetzwerk über das Geräte Tunnel</p> <p><b>Hinweis:</b> Wenn Sie die Datenverkehrs Filter im Geräte Tunnel Profil aktivieren, wird der eingehende Datenverkehr (aus dem Unternehmensnetzwerk an den Client) vom Geräte Tunnel verweigert.</p> <p>Definieren mithilfe von: <b>VPNv2/Profile Name/deaktivieren</b> <b>VPNv2/Profilname/trafficfilterlist</b></p>

## Zusätzliche Funktionen

Jedes Element in diesem Abschnitt ist ein Anwendungsfall Szenario oder eine häufig verwendete Remote Zugriffs Funktion, für die Always on VPN eine verbesserte Funktionalität hat – entweder durch eine Funktionserweiterung

oder durch die Beseitigung einer vorherigen Einschränkung.

FUNKTIONSBEREICH	ALWAYS ON VPN
Mit der Domäne verbundene Geräte mit Enterprise-SKUs Anforderung.	<p>Always On VPN unterstützt mit der Domäne verbundene Geräte, solche, die keiner Domäne beigetreten sind (Arbeitsgruppe) oder in Azure AD eingebundene Geräte sowohl für Unternehmens- und BYOD-Szenarien. Always On VPN ist in allen Windows-Versionen verfügbar, und die Plattformfeatures sind für Dritte über UWP VPN-Plug-In-Unterstützung verfügbar.</p> <p><b>Hinweis:</b> Der Geräte Tunnel kann nur auf in die Domäne eingebundenen Geräten konfiguriert werden, auf denen Windows 10 Enterprise oder Education Version 1709 oder höher ausgeführt wird. Die Kontrolle des Geräte Tunnels durch Drittanbieter wird nicht unterstützt.</p>
Unterstützung sowohl für IPv4 als auch für IPv6.	<p>Mit Always On VPN können Benutzer sowohl auf IPv4 als auch IPv6-Ressourcen im Unternehmensnetzwerk zugreifen. Der Always On VPN-Client verwendet einen Dual-Stack-Ansatz, der nicht speziell von IPv6 oder der Notwendigkeit für das VPN-Gateway abhängt, um NAT64 oder DNS64-Übersetzungsdiene bereitzustellen.</p>
Unterstützung für zweistufige oder OTP-Authentifizierung.	<p>Die Always On VPN-Plattform unterstützt EAP, die die Verwendung von verschiedenen Microsoft und Drittanbietern EAP-Typen als Teil der Workflow-Authentifizierung ermöglicht. Always On VPN unterstützt speziell Smartcard (physisch und virtuell) und Windows Hello for Business Zertifikate für zweistufige Authentifizierungsanforderungen. Darüber hinaus unterstützt Always on VPN OTP über MFA (wird nicht nativ unterstützt, wird nur für Plug-ins von Drittanbietern unterstützt) über die Integration von EAP RADIUS.</p> <p>Definieren mithilfe von:  <b>VPNv2/Profile</b>  <b>Name/nativeprofile/Authentifizierung</b></p>
Unterstützung für mehrere Domäne und Gesamtstrukturen.	<p>Die Always On VPN-Plattform hat keine Abhängigkeit von der Active Directory Domain Services (AD DS)-Gesamtstruktur oder Domänen-Topologie (oder zugeordneten Funktions-/Schemata-Ebenen), da der VPN-Client nicht der Domäne beitreten muss, um die Funktion zu nutzen. Gruppenrichtlinien sind keine Abhängigkeit, um VPN-Profileinstellungen zu definieren, da Sie nicht während der Clientkonfiguration verwendet werden. Wo die Integration der Active Directory-Autorisierung erforderlich ist, können Sie dies über RADIUS als Teil des EAP-Authentifizierung und Autorisierung erzielen.</p>

FUNKTIONSBEREICH	ALWAYS ON VPN
Unterstützung für geteiltes oder erzwungenes Tunneling für Internet-/Intranet-Datenverkehrstrennung.	<p>Sie können Always On VPN konfigurieren, um geteiltes oder erzwungenes Tunneling systemintern (Standardmodus) zu unterstützen. Always On VPN bietet zusätzliche Granularität für anwendungsspezifische Routingrichtlinien.</p> <p><b>Hinweis:</b> Der Tunnel Erzwingungs Tunnel wird nur vom Benutzer Tunnel unterstützt. Es können keine anderen VPN-Tunnel parallel zu einem Tunnel vom Typ Tunnel erzwingen aktiviert werden.</p> <p>Definieren mithilfe von:</p> <p><b>VPNv2/Profile</b> <b>Name/nativeprofile/routingpolicytype</b> <b>VPNv2/Profile</b> <b>Name/trafficfilterlist/App/routingpolicytype</b></p>
Unterstützung mehrerer Protokolle.	<p>Always on-VPN kann für die systemeigene Unterstützung von SSTP konfiguriert werden, wenn Secure Sockets Layer Fall Back von IKEv2 erforderlich ist.</p> <p><b>Hinweis:</b> Der Benutzer Tunnel unterstützt SSTP und IKEv2, und der Geräte Tunnel unterstützt IKEv2 nur ohne Unterstützung für das SSTP-Fallback.</p>
Konnektivitätsassistent zum Bereitstellen des Unternehmens Verbindungsstatus.	<p>Always On VPN ist vollständig in den systemeigenen Netzwerkkonnektivitäts-Assistent integriert und bietet Konnektivitätsstatus über die Benutzeroberfläche für alle Netzwerke. Mit der Einführung von Windows 10 Creators Update (Version 1703) sind jetzt der VPN-Verbindungsstatus und die VPN-Verbindungs Steuerung für den Benutzer Tunnel über das netzwerkflyout (für den integrierten VPN-Client von Windows) verfügbar.</p>
Auflösung von Unternehmensressourcen verwenden Kurznamen, vollqualifizierte Domänennamen (FQDN) und DNS-Suffix.	<p>Always On VPN kann eine oder mehrere DNS-Suffixe systemintern als Teil der VPN-Verbindung und IP-Adressenzuweisung definieren, einschließlich Unternehmensressourcen-Namensauflösung für Kurznamen, FQDNs oder gesamte DNS-Namespaces. Always on-VPN unterstützt auch die Verwendung von Richtlinien Tabellen für die Namensauflösung, um die Granularität der Namespace spezifischen Auflösung bereitzustellen.</p> <p><b>Hinweis:</b> Vermeiden Sie die Verwendung von globalen Suffixen, da diese die Kurznamen-Auflösung beeinträchtigen, wenn Sie die namens Auflösungs Richtlinien Tabellen verwenden.</p> <p>Definieren mithilfe von:</p> <p><b>VPNv2/Profile Name/DnsSuffix</b> <b>VPNv2/Profile Name/domainnameinformationlist</b></p>

## Nächste Schritte

- [Weitere Informationen zu den Always on-VPN-Erweiterungen](#)
- [Erfahren Sie mehr über die erweiterten Always on-VPN-Features](#)

- Weitere Informationen zum Always on VPN-Technologie
- Beginnen der Planung Ihrer Always on-VPN-Bereitstellung

# Always On VPN-Verbesserungen

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows 10

- [Vorheriges: Weitere Informationen zu den Always on-VPN-Features](#)
- [Weiter: Erfahren Sie mehr über die Always on VPN-Technologie](#)

Always on-VPN hat gegenüber den Windows-VPN-Lösungen der Vergangenheit viele Vorteile. Die folgenden wichtigen Verbesserungen richten sich Always on-VPN mit der Cloud-First, Mobile-First-Vision von Microsoft:

- **Platt Form Integration:** Always on VPN hat die Integration mit dem Windows-Betriebssystem und Lösungen von Drittanbietern verbessert, um eine robuste Plattform für unzählige Erweiterte Verbindungs Szenarien bereitzustellen.
- **Sicherheit:** Always on-VPN verfügt über neue, erweiterte Sicherheitsfunktionen, mit denen der Typ des Datenverkehrs eingeschränkt wird, welche Anwendungen die VPN-Verbindung verwenden können und welche Authentifizierungsmethoden Sie verwenden können, um die Verbindung zu initiieren. Wenn die Verbindung in den meisten Fällen aktiv ist, ist es besonders wichtig, die Verbindung zu schützen. Weitere Informationen finden Sie unter [VPN-Authentifizierungs Optionen](#).
- **VPN-Konnektivität:** Always on-VPN mit oder ohne Geräte Tunnel bietet automatische auslöserfunktionen. Vor der Always on-VPN war es nicht möglich, eine automatische Verbindung über die Benutzer-oder Geräte Authentifizierung zu initiieren.
- **Netzwerksteuerung:** Always on VPN ermöglicht Administratoren das Angeben von Routing Richtlinien auf einer präziseteren Ebene – sogar bis hin zu der einzelnen Anwendung – die perfekt für branchenspezifische apps geeignet ist, die einen besonderen Remote Zugriff erfordern. Always on-VPN ist auch vollständig mit Internet Protokollversion 4 (IPv4) und Version 6 (IPv6) kompatibel. Anders als bei DirectAccess gibt es keine bestimmte Abhängigkeit von IPv6.

## NOTE

Bevor Sie beginnen, stellen Sie sicher, dass Sie IPv6 auf dem VPN-Server aktivieren. Andernfalls kann keine Verbindung hergestellt werden, und es wird eine Fehlermeldung angezeigt.

- **Konfiguration und Kompatibilität:** Always on-VPN kann auf verschiedene Weise bereitgestellt und verwaltet werden, was always on-VPN mehrere Vorteile gegenüber der anderen VPN-Client Software bietet.

## Platt Form Integration

Microsoft hat die folgenden Integrationsfunktionen in Always on-VPN eingeführt oder verbessert:

WICHTIGE VERBESSERUNG

BESCHREIBUNG

WICHTIGE VERBESSERUNG	BESCHREIBUNG		
<b>Windows Information Protection (WIP)</b>	Die Integration mit WIP ermöglicht die Erzwingung von Netzwerk Richtlinien, um zu bestimmen, ob Datenverkehr über das VPN geleitet werden darf. Wenn das Benutzerprofil aktiv ist und WIP-Richtlinien angewendet werden, wird Always on-VPN automatisch ausgelöst, um eine Verbindung herzustellen. Außerdem ist es bei Verwendung von WIP nicht erforderlich, apptriggerlist- und trafficfilterlist-Regeln separat im VPN-Profil anzugeben (es sei denn, Sie möchten eine erweiterte Konfiguration), da die WIP-Richtlinien und Anwendungs Listen automatisch wirksam werden.		
<b>Windows Hello for Business</b>	Always on VPN bietet systemeigene Unterstützung für Windows Hello for Business (im Zertifikat basierten Authentifizierungsmodus), um eine nahtlose Single Sign-on für die Anmeldung beim Computer und die Verbindung mit dem VPN bereitzustellen. Daher ist keine sekundäre Authentifizierung (Benutzer Anmelde Informationen) für die VPN-Verbindung erforderlich, sodass es möglich ist, eine Always on Verbindung mit Windows Hello for Business-Authentifizierung zu verwenden.		

WICHTIGE VERBESSERUNG	BESCHREIBUNG		
<b>Bedingter Zugriff Microsoft Azure</b>	Der Always on VPN-Client kann in die Azure-Plattform für bedingten Zugriff integriert werden, um die mehrstufige Authentifizierung (Multi-Factor Authentication, MFA), Geräte Konformität oder eine Kombination der beiden zu erzwingen. Wenn die Richtlinien für den bedingten Zugriff erfüllt sind, gibt Azure Active Directory (Azure AD) ein kurzlebiges (standardmäßig 60 Minuten) IP Security (IPSec)-Authentifizierungszertifikat aus, das dann für die Authentifizierung beim VPN-Gateway verwendet werden kann. Die Geräte Konformität verwendet Configuration Manager/Intune-Kompatibilitätsrichtlinien, die den Zustand der Geräte Integritäts Nachweis im Rahmen der Verbindungs Kompatibilitätsprüfung einschließen können.		
<b>Azure MFA</b>	In Kombination mit Remote Authentication Dial-in User Service (RADIUS)-Diensten und der Netzwerk Richtlinien Server-Erweiterung (NPS) für Azure MFA kann die VPN-Authentifizierung starke MFA verwenden.	<b>Drittanbieter-VPN-Plugin</b>	Mit dem universelle Windows-Plattform (UWP) können Drittanbieter-VPN-Anbieter eine einzelne Anwendung für die gesamte Palette von Windows 10-Geräten erstellen. Die UWP bietet eine garantie API-Kernschicht auf allen Geräten, wodurch die Komplexität und Probleme vermieden werden, die häufig mit dem Schreiben von Treibern auf Kernel Ebene verbunden sind. Derzeit sind Windows 10 UWP-VPN-Plug-Ins für <a href="#">Pulse Secure</a> , <a href="#">F5 Access</a> , <a href="#">Check Point Capsule VPN</a> , <a href="#">FortiClient</a> , <a href="#">SonicWALL Mobile Connect</a> und <a href="#">globalprotect</a> vorhanden. Zweifellos werden andere in Zukunft angezeigt.

## Sicherheit

Die wichtigsten Verbesserungen bei der Sicherheit liegen in den folgenden Bereichen:

WICHTIGE VERBESSERUNG	BESCHREIBUNG		
Datenverkehrs Filter	<p>Mithilfe von Datenverkehrs filtern können Sie Client seitige Richtlinien angeben, die bestimmen, welcher Datenverkehr in das Unternehmensnetzwerk zugelassen wird. Auf diese Weise können Administratoren APP-oder Datenverkehrs Beschränkungen für die VPN-Schnittstelle anwenden und deren Verwendung auf bestimmte Quellen, Zielports und IP-Adressen beschränken. Es sind zwei Arten von Filterregeln verfügbar:</p> <ul style="list-style-type: none"> <li>• <b>App-basierte Regeln.</b> App-basierte Firewallregeln basieren auf einer Liste von angegebenen Anwendungen, sodass nur Datenverkehr, der von diesen apps stammt, über die VPN-Schnittstelle geleitet werden darf.</li> <li>• <b>Datenverkehrs basierte Regeln.</b> Datenverkehrs basierte Firewallregeln basieren auf Netzwerk Anforderungen wie Ports, Adressen und Protokollen. Verwenden Sie diese Regeln nur für Datenverkehr, der diesen speziellen Bedingungen entspricht, die über die VPN-Schnittstelle geleitet werden dürfen.</li> </ul> <p><b>Hinweis:</b> Diese Regeln gelten nur für ausgehenden Datenverkehr vom Gerät. Durch die Verwendung von Datenverkehrs Filtern wird der</p>	Pro-App-VPN	Pro-App-VPN ähnelt einem App-basierten Datenverkehrs Filter, aber es geht weiter, um Anwendungs Trigger mit einem App-basierten Datenverkehrs Filter zu kombinieren, sodass die VPN-Konnektivität auf eine bestimmte Anwendung beschränkt ist, im Gegensatz zu allen Anwendungen auf dem VPN-Client. Das Feature wird automatisch initiiert, wenn die APP gestartet wird.

WICHTIGE VERBESSERUNG	BESCHREIBUNG
	eingehende Dateiverkehr
<b>Unterstützung für angepasste IPSec-Kryptografiealgorithmen</b>	aus dem Unternehmensnetzwerk an den Client blockiert.
<b>Native Extensible Authentication Protocol (EAP)-Unterstützung</b>	Always on-VPN unterstützt die Verwendung von RSA- und Elliptic Curve Cryptography – basierten, benutzerdefinierten Kryptografiealgorithmen, um strenge behördliche oder organisatorische Sicherheitsrichtlinien zu erfüllen.  Always on-VPN bietet native Unterstützung für EAP, sodass Sie eine Vielzahl von Microsoft- und Drittanbieter-EAP-Typen als Teil des Authentifizierungs Workflows verwenden können. EAP bietet eine sichere Authentifizierung basierend auf den folgenden Authentifizierungs Typen: <ul style="list-style-type: none"> <li>• Benutzername und Kennwort</li> <li>• Smartcard (physisch und virtuell)</li> <li>• Benutzerzertifikate</li> <li>• Windows Hello for Business</li> <li>• MFA-Unterstützung durch EAP-RADIUS-Integration</li> </ul> Der Anwendungshersteller steuert die Authentifizierungsmethoden für das UWP-VPN-Plug-in von Drittanbietern, obwohl er über ein Array verfügbarer Optionen verfügt, einschließlich der benutzerdefinierten Anmelde Informationstypen und der OTP-Unterstützung.

## VPN-Konnektivität

Im folgenden sind die wichtigsten Verbesserungen bei der Always on VPN-Konnektivität aufgeführt:

WICHTIGE VERBESSERUNG	BESCHREIBUNG
-----------------------	--------------

WICHTIGE VERBESSERUNG	BESCHREIBUNG
<b>Always On</b>	Always on ist ein Windows 10-Feature, das es dem aktiven VPN-Profil ermöglicht, eine automatische Verbindung herzustellen und basierend auf Triggern verbunden zu bleiben – das heißt, die Benutzeranmeldung, die Netzwerkstatus Änderung oder der Geräte Bildschirm aktiv. Always on ist auch in den verbundenen Standbymodus integriert, um die Akku Lebensdauer zu maximieren.
<b>Auslösen von Anwendungen</b>	Sie können VPN-Profile in Windows 10 so konfigurieren, dass beim Starten eines bestimmten Satzes von Anwendungen automatisch eine Verbindung hergestellt wird. Sie können Desktop- und UWP-Anwendungen so konfigurieren, dass eine VPN-Verbindung auslöst.
<b>Namensbasiertes auslösen</b>	Mit Always on-VPN können Sie Regeln definieren, sodass bestimmte Domänen Namen Abfragen die VPN-Verbindung auslöst. Windows 10 unterstützt jetzt eine namensbasierte Auslösung für Computer, die einer Domäne beigetreten sind, und nicht in die Domäne eingebundenen Computern (bisher wurden nur Computer unterstützt, die keiner Domäne beigetreten)
<b>Erkennung vertrauenswürdiger Netzwerke</b>	Always on-VPN umfasst diese Funktion, um sicherzustellen, dass die VPN-Konnektivität nicht ausgelöst wird, wenn ein Benutzer mit einem vertrauenswürdigen Netzwerk innerhalb der Unternehmens Grenze verbunden ist. Sie können diese Funktion mit den zuvor erwähnten auslösenden Methoden kombinieren, um eine nahtlose "nur bei Bedarf Connect"-Benutzer Funktionalität bereitzustellen.
<b>Geräte Tunnel</b>	Always on-VPN bietet Ihnen die Möglichkeit, ein dediziertes VPN-Profil für das Gerät oder den Computer zu erstellen. Anders als bei einem <i>Benutzer Tunnel</i> , der nur eine Verbindung herstellt, nachdem sich ein Benutzer am Gerät oder Computer anmeldet, ermöglicht der <i>Geräte Tunnel</i> dem VPN, vor der Benutzeranmeldung eine Konnektivität herzustellen. Sowohl Geräte Tunnel als auch Benutzer Tunnel arbeiten unabhängig von Ihren VPN-Profilen, können gleichzeitig verbunden werden und können gegebenenfalls verschiedene Authentifizierungsmethoden und andere VPN-Konfigurationseinstellungen verwenden.

## Netzwerk

Im folgenden finden Sie einige der Netzwerk Verbesserungen in Always on-VPN:

WICHTIGE VERBESSERUNG	BESCHREIBUNG
-----------------------	--------------

WICHTIGE VERBESSERUNG	BESCHREIBUNG
Dual-Stack-Unterstützung für IPv4 und IPv6	<p>Always on-VPN unterstützt die Verwendung von IPv4 und IPv6 in einem Dual-Stack-Ansatz. Sie hat keine spezielle Abhängigkeit von einem Protokoll über das andere, was eine maximale IPv4/IPv6-Anwendungs Kompatibilität in Kombination mit der Unterstützung zukünftiger IPv6-Netzwerk Anforderungen ermöglicht.</p> <p><b>Hinweis:</b> Bevor Sie beginnen, stellen Sie sicher, dass Sie IPv6 auf dem VPN-Server aktivieren. Andernfalls kann keine Verbindung hergestellt werden, und es wird eine Fehlermeldung angezeigt.</p>
Anwendungsspezifische Routing Richtlinien	<p>Zusätzlich zum Definieren von Richtlinien für die globale VPN-Verbindungs Weiterleitung für die Trennung von Internet-und Intranetdatenverkehr können Routing Richtlinien hinzugefügt werden, um die Verwendung von Split-Tunneln oder Tunnel Erzwingungen pro Anwendung zu steuern. Mit dieser Option können Sie besser steuern, welche apps mit welchen Ressourcen über den VPN-Tunnel interagieren können.</p>
Ausschluss Routen	<p>Always on-VPN unterstützt die Möglichkeit, Ausschluss Routen anzugeben, die speziell das Routing Verhalten steuern, um zu definieren, welcher Datenverkehr nur das VPN durchlaufen soll, und nicht über die physische Netzwerkschnittstelle.</p> <p><b>Anmerkungen:</b></p> <ul style="list-style-type: none"> <li>-Ausschluss Routen funktionieren derzeit für Datenverkehr im gleichen Subnetz wie der Client, z. b. LINKLOCAL.</li> <li>-Ausschluss Routen funktionieren nur in einem Split-Tunnel-Setup.</li> </ul>

## Konfiguration und Kompatibilität

Im folgenden finden Sie einige der Konfigurations-und Kompatibilitäts Verbesserungen in Always on VPN:

WICHTIGE VERBESSERUNG	BESCHREIBUNG
Kompatibilität von VPN-Gateways von Drittanbietern	<p>Für den Always on-VPN-Client ist die Verwendung eines Microsoft-basierten VPN-Gateways für den Betrieb nicht erforderlich. Durch die Unterstützung des IKEv2-Protokolls ermöglicht der Client die Interoperabilität mit VPN-Gateways von Drittanbietern, die diesen nach Industriestandard tunnelingtyp unterstützen. Sie können auch eine Interoperabilität mit VPN-Gateways von Drittanbietern erzielen, indem Sie ein UWP-VPN-Plug-in zusammen mit einem benutzerdefinierten tunnelingtyp verwenden, ohne Always on Features und Vorteile der VPN-Plattform zu beeinträchtigen.</p> <p><b>Hinweis:</b></p> <p>Wenden Sie sich bei Konfigurationen und Kompatibilität mit Always on VPN und dem Geräte Tunnel unter Verwendung von IKEv2 an Ihren Gateway-oder Drittanbieter für die Back-End-Appliance.</p>

WICHTIGE VERBESSERUNG	BESCHREIBUNG
<b>Industriestandard IKEv2 VPN-Protokoll Unterstützung</b>	Der Always on VPN-Client unterstützt IKEv2, eines der heute am häufigsten verwendeten nach Industriestandard-tunnelingprotokollen. Diese Kompatibilität maximiert die Interoperabilität mit VPN-Gateways von Drittanbietern.
<b>Platt Form Unterstützung</b>	Das aalwys on-VPN unterstützt in die Domäne eingebundenen, nicht in die Domäne eingebundenen (Arbeitsgruppen) oder Azure AD – Geräte, die sowohl Unternehmen als auch Bring your own Device (BYOD)-Szenarien ermöglichen. Außerdem ist Always on-VPN in allen Windows-Editionen verfügbar.
<b>Verschiedene Verwaltungs-und Bereitstellungs Mechanismen</b>	Sie können viele Verwaltungs-und Bereitstellungs Mechanismen verwenden, um VPN-Einstellungen ( <i>VPN-Profil</i> ) zu verwalten, darunter Windows PowerShell, Microsoft Endpoint Configuration Manager, InTune oder das Drittanbieter-Tool für die Verwaltung mobiler Geräte (Mobile Device Management, MDM) und Windows Configuration Designer. Diese Optionen vereinfachen die Konfiguration Always on VPN unabhängig von den von Ihnen verwendeten Client Verwaltungs Tools.
<b>Definition des standardisierten VPN-Profil</b>	Always on VPN unterstützt die Konfiguration mit einem Standard-XML-Profil (profileXML) und bietet ein Standardmäßiges Konfigurations Vorlagen Format, das von den meisten Verwaltungs-und Bereitstellungs Toolsets verwendet wird

## Nächste Schritte

- [Erfahren Sie mehr über die erweiterten Always on-VPN-Features](#)
- [Weitere Informationen zum Always on VPN-Technologie](#)
- [Beginnen der Planung Ihrer Always on-VPN-Bereitstellung](#)

# Übersicht über Always on VPN-Technologie

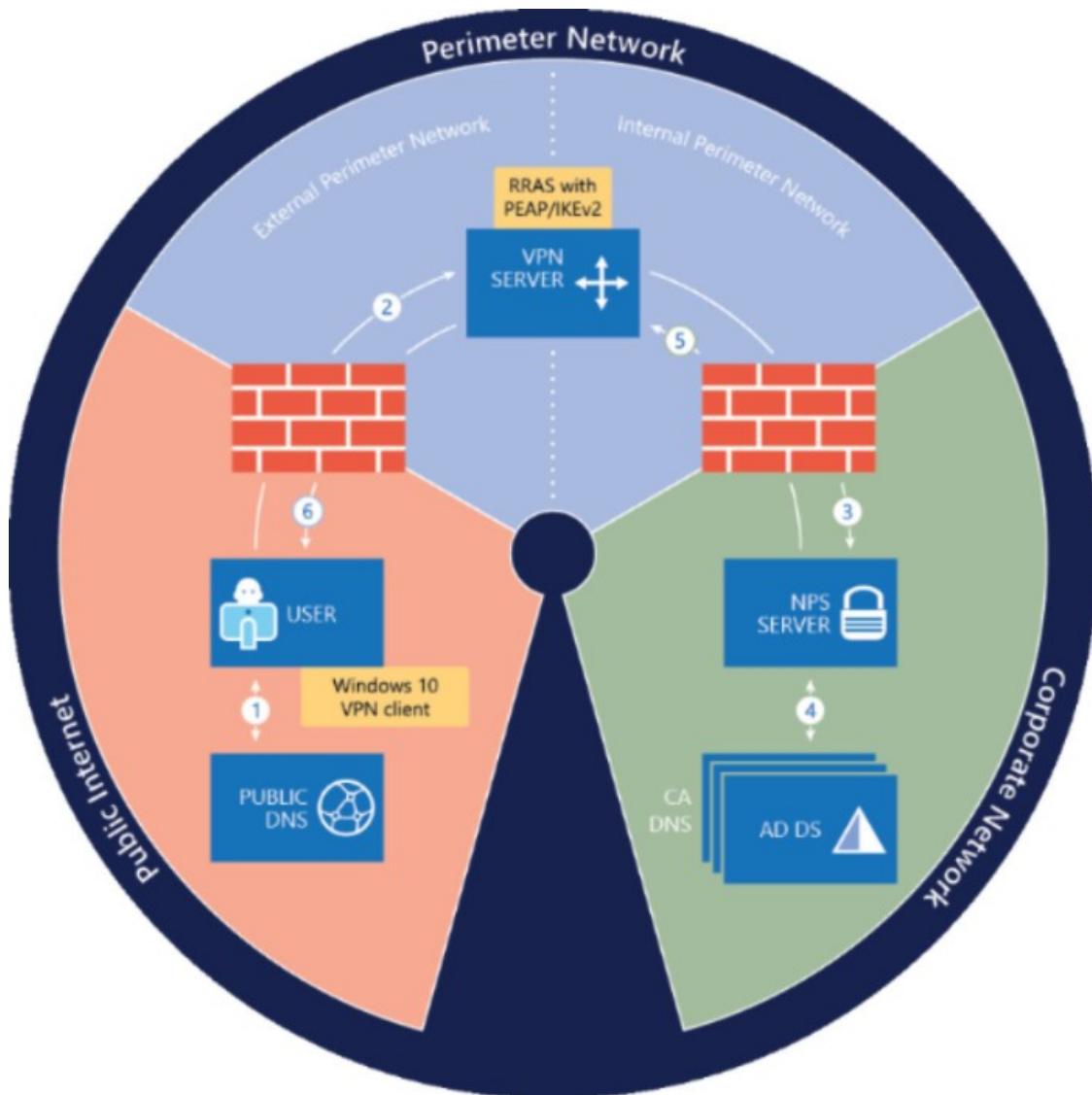
09.04.2020 • 23 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges](#): Weitere Informationen zu den Always on-VPN-Erweiterungen
- [Weiter](#): Erfahren Sie mehr über die erweiterten Features von Always on VPN

Für diese Bereitstellung müssen Sie einen neuen RAS-Server installieren, auf dem Windows Server 2016 ausgeführt wird. Außerdem müssen Sie einen Teil der vorhandenen Infrastruktur für die Bereitstellung ändern.

Die folgende Abbildung zeigt die Infrastruktur, die für die Bereitstellung Always on VPN erforderlich ist.



Der in dieser Abbildung dargestellte Verbindungsprozess besteht aus den folgenden Schritten:

1. Mit öffentlichen DNS-Servern führt der Windows 10-VPN-Client eine namens Auflösungs Abfrage für die IP-Adresse des VPN-Gateways aus.
2. Mithilfe der von DNS zurückgegebenen IP-Adresse sendet der VPN-Client eine Verbindungsanforderung an das VPN-Gateway.

3. Das VPN-Gateway wird auch als Remote Authentication Dial-in User Service (RADIUS)-Client konfiguriert. der VPN-RADIUS-Client sendet die Verbindungsanforderung für die Verarbeitung von Verbindungsanforderungen an den NPS-Server der Organisation/des Unternehmens.
4. Der NPS-Server verarbeitet die Verbindungsanforderung, einschließlich der Autorisierung und Authentifizierung, und bestimmt, ob die Verbindungsanforderung zugelassen oder verweigert wird.
5. Der NPS-Server leitet eine Access-Accept-oder Access-Deny-Antwort an das VPN-Gateway weiter.
6. Die Verbindung wird basierend auf der Antwort, die der VPN-Server vom NPS-Server empfangen hat, initiiert oder beendet.

Weitere Informationen zu den einzelnen Infrastrukturkomponenten, die in der obigen Abbildung dargestellt werden, finden Sie in den folgenden Abschnitten.

**NOTE**

Wenn Sie bereits einige dieser Technologien in Ihrem Netzwerk bereitgestellt haben, können Sie die Anweisungen in diesem Bereitstellungs Leit Faden verwenden, um eine zusätzliche Konfiguration der Technologien für diesen Bereitstellungs Zweck auszuführen.

## Domain Name System (DNS)

Sowohl interne als auch externe Domain Name System (DNS-Zonen) sind erforderlich. dabei wird davon ausgegangen, dass die interne Zone eine delegierte Unterdomäne der externen Zone ist (z. b. Corp.contoso.com und contoso.com).

Erfahren Sie mehr über [Domain Name System \(DNS\)](#) oder das Haupt [Netzwerk Handbuch](#).

**NOTE**

Andere DNS-Entwürfe, z. b. Split-Brain-DNS (mit dem gleichen Domänen Namen intern und extern in separaten DNS-Zonen) oder nicht verknüpfte interne und externe Domänen (z. b. Conto. local und contoso.com) sind ebenfalls möglich. Weitere Informationen zum Bereitstellen von Split-Brain-DNS finden Sie unter [Verwenden der DNS-Richtlinie für Split-Brain-DNS-Bereitstellung](#)

## Firewalls

Stellen Sie sicher, dass die Firewalls zulassen, dass der Datenverkehr, der für die VPN-und RADIUS-Kommunikation erforderlich ist, richtig funktioniert.

Weitere Informationen finden Sie unter [Konfigurieren von Firewalls für RADIUS-Datenverkehr](#).

## Remote Zugriff als RAS-Gateway-VPN-Server

In Windows Server 2016 ist die Remote Zugriffs-Server Rolle so konzipiert, dass Sie sowohl einen Router als auch einen RAS-Server ausführt. Daher unterstützt es eine Vielzahl von Features. Für diese Anleitung für die Bereitstellung benötigen Sie nur eine kleine Teilmenge dieser Features: Unterstützung für IKEv2-VPN-Verbindungen und LAN-Routing.

IKEv2 ist ein VPN-Tunnelingprotokoll, das in Internet Engineering Task Force Request for Comments 7296 beschrieben wird. Der Hauptvorteil von IKEv2 besteht darin, dass Unterbrechungen in der zugrunde liegenden Netzwerkverbindung toleriert werden. Wenn beispielsweise die Verbindung vorübergehend unterbrochen wird oder ein Benutzer einen Client Computer von einem Netzwerk auf einen anderen verschiebt, stellt IKEv2 die VPN-Verbindung automatisch wieder her, wenn die Netzwerkverbindung wieder hergestellt wird – ohne

## Benutzereingriff.

Mithilfe des RAS-Gateways können Sie VPN-Verbindungen bereitstellen, um Endbenutzern Remote Zugriff auf das Netzwerk und die Ressourcen Ihrer Organisation zu bieten. Wenn Remote Computer mit dem Internet verbunden sind, wird bei der Bereitstellung Always on VPN eine permanente Verbindung zwischen Clients und Ihrem Organisations Netzwerk aufrechterhalten. Mit dem RAS-Gateway können Sie auch eine Site-to-Site-VPN-Verbindung zwischen zwei Servern an unterschiedlichen Standorten erstellen, z. b. zwischen Ihrer primären Niederlassung und einer Zweigstelle, und die Netzwerk Adressübersetzung (Network Address Translation, NAT) verwenden, damit Benutzer im Netzwerk auf extern zugreifen können. Ressourcen, z. b. das Internet. Außerdem unterstützt das RAS-Gateway Border Gateway Protocol (BGP), das dynamische Routing Dienste bereitstellt, wenn Ihre Remote Niederlassungen auch Edge-Gateways aufweisen, die BGP unterstützen.

RAS-Gateways können mithilfe von Windows PowerShell-Befehlen und der Microsoft Management Console (MMC) für den Remote Zugriff verwaltet werden.

## Netzwerkrichtlinienserver (Network Policy Server, NPS)

Mit NPS können Sie Organisationen weite Netzwerk Zugriffsrichtlinien für die Authentifizierung und Autorisierung von Verbindungsanforderungen erstellen und erzwingen. Wenn Sie NPS als RADIUS-Server (Remote Authentication Dial-in User Service) verwenden, konfigurieren Sie Netzwerk Zugriffs Server, z. b. VPN-Server, als RADIUS-Clients in NPS.

Sie können auch Netzwerkrichtlinien konfigurieren, mit denen NPS Verbindungsanforderungen autorisiert, und Sie können die RADIUS-Kontoführung so konfigurieren, dass NPS Kontoführungsinformationen in Protokolldateien auf der lokalen Festplatte oder in einer Microsoft SQL Server-Datenbank protokolliert.

Weitere Informationen finden Sie unter [Netzwerk Richtlinien Server \(Network Policy Server, NPS\)](#).

## Active Directory-Zertifikatsdienste

Der Server der Zertifizierungsstelle (Certification Authority, ca) ist eine Zertifizierungsstelle, die Active Directory Zertifikat Dienste ausgeführt wird. Für die VPN-Konfiguration ist eine Active Directory basierte Public Key-Infrastruktur (PKI) erforderlich.

Organisationen können AD CS verwenden, um die Sicherheit zu erhöhen, indem Sie die Identität einer Person, eines Geräts oder Diensts an einen entsprechenden öffentlichen Schlüssel binden. AD CS umfasst auch Features, mit denen Sie die Zertifikat Registrierung und die Sperrung in einer Vielzahl von skalierbaren Umgebungen verwalten können. Weitere Informationen finden Sie unter [Übersicht über Active Directory Zertifikat Dienste](#) und [Entwurfs Leit Fäden für die Public Key-Infrastruktur](#).

Während der Fertigstellung der Bereitstellung konfigurieren Sie die folgenden Zertifikat Vorlagen für die Zertifizierungsstelle.

- Die Zertifikat Vorlage für die Benutzeroauthentifizierung
- Die Zertifikat Vorlage für die VPN-Server Authentifizierung
- Die Zertifikat Vorlage für die NPS-Server Authentifizierung

## Zertifikatvorlagen

Zertifikat Vorlagen können die Verwaltung einer Zertifizierungsstelle (Certification Authority, ca) erheblich vereinfachen, da Sie Zertifikate ausstellen können, die für ausgewählte Tasks vorkonfiguriert sind. Mit dem MMC-Snap-in "Zertifikat Vorlagen" können Sie die nachfolgend aufgeführten Aufgaben ausführen.

- Anzeigen der Eigenschaften für jede Zertifikat Vorlage.
- Kopieren und ändern Sie Zertifikat Vorlagen.

- Steuern Sie, welche Benutzer und Computer Vorlagen lesen und für Zertifikate registrieren können.
- Ausführen weiterer Verwaltungsaufgaben im Zusammenhang mit Zertifikat Vorlagen

Zertifikat Vorlagen sind ein wesentlicher Bestandteil einer Unternehmens Zertifizierungsstelle (Certification Authority, ca). Sie sind ein wichtiges Element der Zertifikat Richtlinie für eine-Umgebung, die den Satz von Regeln und Formaten für die Zertifikat Registrierung,-Verwendung und-Verwaltung ist.

Weitere Informationen finden Sie unter [Zertifikat Vorlagen](#).

### **Zertifikate für digitale Server**

Dieser Leitfaden zur Bereitstellung enthält Anweisungen für die Verwendung von Active Directory Zertifikat Diensten (AD CS) zum Registrieren und automatischen Registrieren von Zertifikaten für RAS-und NPS-Infrastruktur Server. AD CS ermöglicht Ihnen das Erstellen einer Public Key-Infrastruktur (PKI) und die Bereitstellung von Kryptografie mit öffentlichem Schlüssel, digitalen Zertifikaten und Funktionen für digitale Signaturen in Ihrer Organisation.

Wenn Sie Zertifikate für digitale Server für die Authentifizierung zwischen Computern im Netzwerk verwenden, stellen die Zertifikate Folgendes bereit:

1. Vertraulichkeit durch Verschlüsselung.
2. Integrität durch digitale Signaturen.
3. Authentifizierung durch Zuordnen von Zertifikat Schlüsseln zu Computern, Benutzern oder Geräte Konten in einem Computernetzwerk.

Weitere Informationen finden Sie unterschritt-für- [Schritt-Anleitung für AD CS: Bereitstellung mit zweistufigen PKI-Hierarchie](#).

## **Active Directory-Domänendienste (AD DS)**

Mit AD DS wird eine verteilte Datenbank bereitgestellt, in der Informationen zu Netzwerkressourcen und anwendungsspezifische Daten aus AD-fähigen Anwendungen gespeichert und verwaltet werden. Administratoren können AD DS verwenden, um die Elemente eines Netzwerks (z. B. Benutzer, Computer und andere Geräte) in einer hierarchischen Struktur aus Einschlussbeziehungen zu organisieren. Diese hierarchische Struktur umfasst die Active Directory-Gesamtstruktur, Domänen in der Gesamtstruktur sowie die Organisationseinheiten in den einzelnen Domänen. Ein Server, auf dem AD DS ausgeführt wird, wird als Domänencontroller bezeichnet.

AD DS enthält die Benutzerkonten, Computer Konten und Konto Eigenschaften, die für die Authentifizierung von Benutzer Anmelde Informationen und das Auswerten der Autorisierung von VPN-Verbindungsanforderungen für das Protected Extensible Authentication-Protokoll (PAP) erforderlich sind. Weitere Informationen zum Bereitstellen von AD DS finden Sie im Windows Server 2016- [Kern Netzwerk Handbuch](#).

Während der Ausführung der Schritte in dieser Bereitstellung konfigurieren Sie die folgenden Elemente auf dem Domänen Controller.

- Aktivieren der automatischen Registrierung von Zertifikaten in Gruppenrichtlinie für Computer und Benutzer
- Erstellen der Gruppe "VPN-Benutzer"
- Erstellen der VPN-Server Gruppe
- Erstellen der NPS-Server Gruppe

### **Active Directory-Benutzer und -Computer**

Active Directory Benutzer und Computer ist eine Komponente von AD DS, die Konten enthält, die physische

Entitäten darstellen, z. b. einen Computer, eine Person oder eine Sicherheitsgruppe. Bei einer Sicherheitsgruppe handelt es sich um eine Sammlung von Benutzer- oder Computer Konten, die von Administratoren als einzelne Einheit verwaltet werden können. Benutzer- und Computer Konten, die einer bestimmten Gruppe angehören, werden als Gruppenmitglieder bezeichnet.

Benutzerkonten in Active Directory Benutzern und Computern verfügen über DFÜ-Eigenschaften, die NPS während der Autorisierung auswertet, es sei denn, die Eigenschaft **Netzwerk Zugriffsberechtigung** des Benutzerkontos ist so festgelegt, dass der **Zugriff über die NPS-Netzwerk Richtlinie gesteuert** wird. Dies ist die Standardeinstellung für alle Benutzerkonten. In einigen Fällen kann diese Einstellung jedoch eine andere Konfiguration aufweisen, die den Benutzer daran hindert, eine VPN-Verbindung herzustellen. Um diese Möglichkeit zu schützen, können Sie den NPS-Server so konfigurieren, dass Benutzerkonto-Einwähleigenschaften ignoriert werden.

Weitere Informationen finden Sie unter [Konfigurieren von NPS zum Ignorieren von Benutzerkonto-DFÜ-Eigenschaften](#).

### Gruppenrichtlinienverwaltung

Gruppenrichtlinie Management ermöglicht die Verzeichnis basierte Änderungs- und Konfigurations Verwaltung von Benutzer- und Computereinstellungen, einschließlich Sicherheits- und Benutzerinformationen. Mit Gruppenrichtlinie können Sie Konfigurationen für Gruppen von Benutzern und Computern definieren.

Mit Gruppenrichtlinie können Sie Einstellungen für Registrierungseinträge, Sicherheit, Software Installation, Skripts, Ordner Umleitung, Remoteinstallations Dienste und Internet Explorer-Wartung angeben. Die Gruppenrichtlinie Einstellungen, die Sie erstellen, sind in einem Gruppenrichtlinie Objekt (GPO) enthalten. Durch Zuordnen eines Gruppenrichtlinien Objekts zu ausgewählten Active Directory System Containern – Websites, Domänen und Organisationseinheiten – können Sie die Einstellungen des GPO auf die Benutzer und Computer in diesen Active Directory Containern anwenden. Zum Verwalten von Gruppenrichtlinie Objekten in einem Unternehmen können Sie die Gruppenrichtlinienverwaltungs-Editor Microsoft Management Console (MMC) verwenden.

## Windows 10-VPN-Clients

Stellen Sie zusätzlich zu den Serverkomponenten sicher, dass auf den Client Computern, die Sie für die Verwendung von VPN konfigurieren, Windows 10 Anniversary Update (Version 1607) ausgeführt wird. Die Windows 10-VPN-Clients müssen Ihrer Active Directory Domäne beitreten.

Der Windows 10-VPN-Client ist sehr konfigurierbar und bietet viele Optionen. Um die spezifischen Features dieses Szenarios besser zu veranschaulichen, identifiziert Tabelle 1 die VPN-Funktions Kategorien und die spezifischen Konfigurationen, auf die diese Bereitstellung verweist. Sie konfigurieren die einzelnen Einstellungen für diese Features mithilfe des VPnv2-Konfigurations Dienstanbieters (CSP), der später in dieser Bereitstellung beschrieben wird.

Tabelle 1. In dieser Bereitstellung erörterte VPN-Features und -Konfigurationen

VPN-FEATURE	KONFIGURATION DER BEREITSTELLUNGS SZENARIEN
Verbindungstyp	Native IKEv2
Routing	Tunnelung aufteilen
Namensauflösung	Domänen Namen-Informationsliste und DNS-Suffix
Ängste	Erkennung von Always on und vertrauenswürdigen Netzwerken

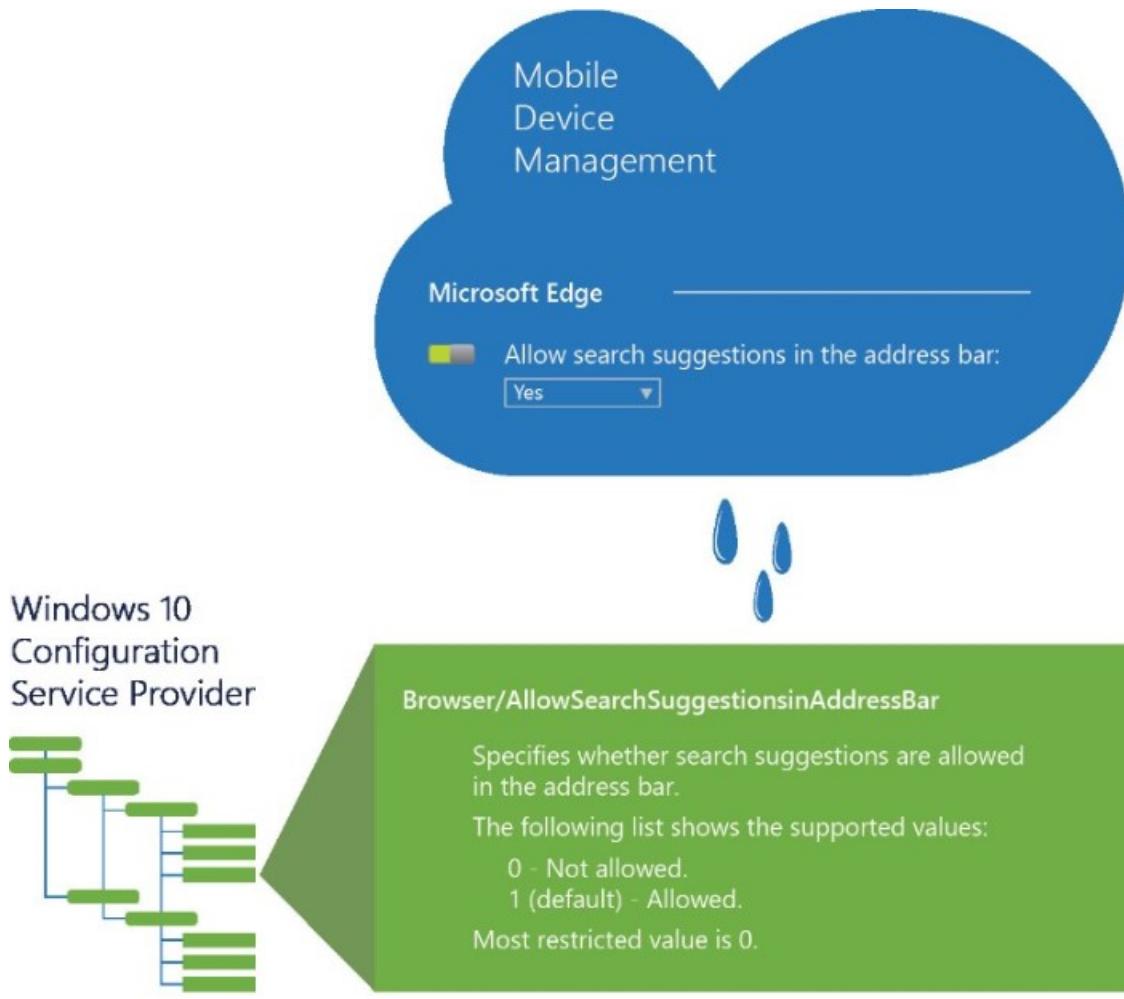
VPN-FEATURE	KONFIGURATION DER BEREITSTELLUNGS SZENARIEN
Authentifizierung	Peer-TLS mit TPM – geschützte Benutzerzertifikate

#### NOTE

"Peer-TLS" und "TPM" sind "geschütztes Extensible Authentication Protocol with Transport Layer Security" und "Trusted Platform Module".

### VPNv2-CSP-Knoten

In dieser Bereitstellung verwenden Sie den Knoten profileXML VPNv2 CSP, um das VPN-Profil zu erstellen, das an Windows 10-Client Computer übermittelt wird. Konfigurations Dienstanbieter (CSPs) sind Schnittstellen, die verschiedene Verwaltungsfunktionen innerhalb des Windows-Clients verfügbar machen. konzeptionell funktionieren CSPs ähnlich wie Gruppenrichtlinie. Jeder CSP verfügt über Konfigurations Knoten, die einzelne Einstellungen darstellen. Ebenso wie Gruppenrichtlinie Einstellungen können Sie CSP-Einstellungen mit Registrierungs Schlüsseln, Dateien, Berechtigungen usw. verknüpfen. Ähnlich wie bei der Verwendung des Gruppenrichtlinienverwaltungs-Editor zum Konfigurieren von Gruppenrichtlinie Objekten (GPOs) konfigurieren Sie die CSP-Knoten mithilfe einer MDM-Lösung (Mobile Device Management, Verwaltung mobiler Geräte), wie z. b. Microsoft InTune. MDM-Produkte wie InTune bieten eine benutzerfreundliche Konfigurationsoption, mit der der CSP im Betriebssystem konfiguriert wird.



Einige CSP-Knoten können jedoch nicht direkt über eine Benutzeroberfläche (UI) wie die Intune-Verwaltungskonsole konfiguriert werden. In diesen Fällen müssen Sie die Oma-URI-Einstellungen (Open Mobile Alliance Uniform Resource Identifier) manuell konfigurieren. Sie konfigurieren Oma-URLs mithilfe des Oma-Geräte Verwaltungs Protokolls (OMA-DM), einer universellen Geräte Verwaltungs Spezifikation, die von den

meisten modernen Apple-, Android- und Windows-Geräten unterstützt wird. Solange Sie der OMA-DM-Spezifikation entsprechen, sollten alle MDM-Produkte auf die gleiche Weise mit diesen Betriebssystemen interagieren.

Windows 10 bietet viele CSPs, aber bei dieser Bereitstellung liegt der Schwerpunkt auf der Verwendung von VPnv2 CSP zum Konfigurieren des VPN-Clients. Der VPnv2 CSP ermöglicht die Konfiguration der einzelnen VPN-Profilinstellungen in Windows 10 über einen eindeutigen CSP-Knoten. Außerdem ist der VPnv2-CSP ein Knoten namens *profileXML*, der es Ihnen ermöglicht, alle Einstellungen in einem Knoten anstatt einzeln zu konfigurieren. Weitere Informationen zu *profileXML* finden Sie im Abschnitt "Übersicht über *profileXML*" weiter unten in dieser Bereitstellung. Ausführliche Informationen zu den einzelnen VPnv2-CSP-Knoten finden Sie unter [VPnv2 CSP](#).

## Nächste Schritte

- [Erfahren Sie mehr über die erweiterten Always on-VPN-Features](#)
- [Beginnen der Planung Ihrer Always on-VPN-Bereitstellung](#)

## Verwandte Themen

- [Microsoft-Server Softwareunterstützung für Microsoft Azure Virtual Machines](#): in diesem Artikel wird die Unterstützungs Richtlinie für die Ausführung von Microsoft-Server Software in der Microsoft Azure-Umgebung für virtuelle Maschinen (Infrastructure-as-a-Service) erläutert.
- [Remote Zugriff](#): dieses Thema enthält eine Übersicht über die Remote Zugriffs-Server Rolle in Windows Server 2016.
- [Technische Anleitung für das Windows 10-VPN](#): Dieses Handbuch führt Sie durch die Entscheidungen, die Sie für Windows 10-Clients in Ihrer Enterprise-VPN-Lösung treffen und wie Sie die Bereitstellung konfigurieren. Dieses Handbuch verweist auf den VPnv2-Konfigurations Dienstanbieter (CSP) und stellt Konfigurations Anweisungen für die Verwaltung mobiler Geräte (MDM) mithilfe von Microsoft InTune und der VPN-Profil Vorlage für Windows 10 bereit.
- [Handbuch zum Hauptnetzwerk](#): Dieses Handbuch enthält Anweisungen zum Planen und Bereitstellen der Kernkomponenten, die für ein voll funktionsfähiges Netzwerk und eine neue Active Directory Domäne in einer neuen Gesamtstruktur erforderlich sind.
- [Domain Name System \(DNS\)](#): dieses Thema enthält eine Übersicht über DNS (Domain Name Systems). In Windows Server 2016 ist DNS eine Server Rolle, die Sie mithilfe von Server-Manager oder Windows PowerShell-Befehlen installieren können. Wenn Sie eine neue Active Directory Gesamtstruktur und Domäne installieren, wird DNS automatisch mit Active Directory als globaler Katalogserver für die Gesamtstruktur und Domäne installiert.
- [Übersicht über Active Directory Zertifikat Dienste](#): Dieses Dokument bietet eine Übersicht über die Active Directory Zertifikat Dienste (AD CS) in Windows Server® 2012. AD CS ist die Serverrolle, die es Ihnen ermöglicht, eine Public Key Infrastructure (PKI) zu erstellen und Verschlüsselung für öffentliche Schlüssel, digitale Zertifikate und Funktionen für digitale Signaturen in Ihrer Organisation bereitzustellen.
- [Entwurfs Leit Faden für die Public Key-Infrastruktur](#): dieses wiki bietet Anleitungen zum Entwerfen von Public Key-Infrastrukturen (PKIs). Bevor Sie eine PKI-und Zertifizierungsstellen Hierarchie konfigurieren, sollten Sie die Sicherheitsrichtlinie und die CPS-Anweisung (Certificate Practice Statement) Ihrer Organisation kennen.
- [Schritt-für-Schritt-Anleitung für AD CS: Bereitstellung der PKI-Hierarchie mit zwei Ebenen](#): Diese Schritt-für-Schritt-Anleitung beschreibt die Schritte, die zum Einrichten einer grundlegenden Konfiguration von Active Directory® Zertifikat Diensten (AD CS) in einer Lab-Umgebung erforderlich sind AD CS in

Windows Server® 2008 R2 bietet anpassbare Dienste zum Erstellen und Verwalten von Zertifikaten für öffentliche Schlüssel, die in Software Sicherheitssystemen verwendet werden, die Public Key-Technologien einsetzen.

- [Netzwerk Richtlinien Server \(Network Policy Server, NPS\)](#): dieses Thema enthält eine Übersicht über den Netzwerk Richtlinien Server unter Windows Server 2016. Mit einem Netzwerkrichtlinienserver (Network Policy Server, NPS) können Sie organisationsweite Netzwerkgzugriffsrichtlinien für die Authentifizierung und Autorisierung von Verbindungsanforderungen erstellen und erzwingen.

# Erweiterte Features von Always on-VPN

09.04.2020 • 15 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Erfahren Sie mehr über die Always on VPN-Technologie](#)
- [Weiter: Beginnen der Planung der Always on-VPN-Bereitstellung](#)

Neben den bereitgestellten Bereitstellungs Szenarien können Sie weitere erweiterte VPN-Features hinzufügen, um die Sicherheit und Verfügbarkeit Ihrer VPN-Verbindung zu verbessern. Beispielsweise kann der VPN-Server diese Features verwenden, um sicherzustellen, dass der Verbindungs Client fehlerfrei ist, bevor er eine Verbindung zulässt.

## Hohe Verfügbarkeit

Im folgenden finden Sie zusätzliche Optionen für hohe Verfügbarkeit.

OPTION	BESCHREIBUNG
Server Resilienz und Lastenausgleich	<p>In Umgebungen, die Hochverfügbarkeit erfordern oder eine große Anzahl von Anforderungen unterstützen, können Sie die Leistung und Resilienz des Remote Zugriffs steigern, indem Sie den Lastenausgleich zwischen mehreren Servern verwenden, auf denen ein Netzwerk Richtlinien Server (Network Policy Server, NPS) ausgeführt wird, und die Aktivierung des RAS-Server Clustering</p> <p>Verwandte Dokumente:</p> <ul style="list-style-type: none"><li>• <a href="#">NPS-Proxy Server-Lastenausgleich</a></li><li>• <a href="#">Bereitstellen des Remotezugriffs in einem Cluster</a></li></ul>
Stabilität des geografischen Standorts	<p>Für die IP-basierte Geolokalisierung können Sie globale Traffic Manager mit DNS in Windows Server 2016 verwenden. Um einen stabileren geografischen Lastenausgleich zu erreichen, können Sie Lösungen für den Lastenausgleich auf globaler Ebene wie Microsoft Azure Traffic Manager verwenden.</p> <p>Verwandte Dokumente:</p> <ul style="list-style-type: none"><li>• <a href="#">Übersicht über Traffic Manager</a></li><li>• <a href="#">Microsoft Azure Traffic Manager</a></li></ul>

## Erweiterte Authentifizierung

Im folgenden finden Sie zusätzliche Authentifizierungs Optionen.

OPTION	BESCHREIBUNG
--------	--------------

OPTION	BESCHREIBUNG
Windows Hello for Business	<p>In Windows 10 ersetzt Windows Hello for Business Kenn Wörter durch eine starke zweistufige Authentifizierung auf PCs und mobilen Geräten. Diese Authentifizierung besteht aus einem neuen Typ von Benutzer Anmelde Informationen, der an ein Gerät gebunden ist und eine biometrische oder persönliche Identifikationsnummer (PIN) verwendet.</p> <p>Der Windows 10-VPN-Client ist kompatibel mit Windows Hello for Business. Nachdem sich der Benutzer mit einer Geste anmeldet, verwendet die VPN-Verbindung das Windows Hello for Business-Zertifikat für die Zertifikat basierte Authentifizierung.</p> <p>Verwandte Dokumente:</p> <ul style="list-style-type: none"> <li>• <a href="#">Windows Hello for Business</a></li> <li>• Technische Fallstudie: <a href="#">Aktivieren des Remote Zugriffs mit Windows Hello for Business in Windows 10</a></li> </ul>
Azure Multi-Factor Authentication (MFA)	<p>Azure MFA verfügt über Cloud-und lokale Versionen, die Sie in den Windows-VPN-Authentifizierungsmechanismus integrieren können.</p> <p>Weitere Informationen zur Funktionsweise dieses Mechanismus finden Sie unter <a href="#">integrieren der RADIUS-Authentifizierung in Azure Multi-Factor Authentication-Server</a>.</p>

## Erweiterte VPN-Features

Im folgenden finden Sie zusätzliche Optionen für erweiterte Funktionen.

OPTION	BESCHREIBUNG
Filtern von Datenverkehr	<p>Wenn Sie die Auswahl der Anwendungen erzwingen müssen, auf die VPN-Clients zugreifen können, können Sie VPN-Datenverkehrs Filter aktivieren.</p> <p>Weitere Informationen finden Sie unter <a href="#">VPN-Sicherheitsfeatures</a>.</p>
Durch Apps ausgelöstes VPN	<p>Sie können VPN-Profile so konfigurieren, dass Sie automatisch eine Verbindung herstellen, wenn bestimmte Anwendungen oder Anwendungs Typen gestartet werden.</p> <p>Weitere Informationen zu dieser und anderen auslösenden Optionen finden Sie unter von <a href="#">automatisch ausgelöste VPN-Profil Optionen</a>.</p>

OPTION	BESCHREIBUNG
Bedingter VPN-Zugriff	<p>Bedingter Zugriff und Geräte Konformität können von verwalteten Geräten verlangt werden, dass Sie die Standards erfüllen, bevor Sie eine Verbindung mit dem VPN herstellen können. Eine der erweiterten Features für den bedingten VPN-Zugriff ermöglicht es Ihnen, die VPN-Verbindungen auf solche einzuschränken, auf denen das Client Authentifizierungszertifikat die OID "Aad Conditional Access" von <b>1.3.6.1.4.1.311.87</b> enthält.</p> <p>Um die VPN-Verbindungen einzuschränken, müssen Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Öffnen Sie auf dem NPS-Server das Snap-in "<b>Netzwerk Richtlinien Server</b>".</li> <li>2. Erweitern Sie <b>Richtlinien &gt; Netzwerk Richtlinien</b>.</li> <li>3. Klicken Sie mit der rechten Maustaste auf die <b>Netzwerk Richtlinie VPN-Verbindungen (virtuelles privates Netzwerk)</b>, und wählen Sie <b>Eigenschaften</b>.</li> <li>4. Wählen Sie die Registerkarte <b>Einstellungen</b> aus.</li> <li>5. Wählen Sie <b>Hersteller spezifisch</b>, und klicken Sie dann auf <b>Hinzufügen</b>.</li> <li>6. Wählen Sie die Option <b>Allowed-Certificate-OID</b> aus, und klicken Sie dann auf <b>Hinzufügen</b>.</li> <li>7. Fügen Sie die Aad Conditional Access OID of <b>1.3.6.1.4.1.311.87</b> als Attribut Wert ein, und wählen Sie dann zweimal <b>OK</b> aus.</li> <li>8. Wählen Sie <b>Schließen</b>, und klicken Sie dann auf <b>anwenden</b>.</li> </ol> <p>Nachdem Sie diese Schritte ausgeführt haben, schlägt die Verbindung fehl, wenn VPN-Clients versuchen, eine Verbindung mit einem anderen Zertifikat als dem kurzlebigen cloudzertifikat herzustellen.</p> <p>Weitere Informationen zum bedingten Zugriff finden Sie unter <a href="#">VPN und bedingter Zugriff</a>.</p>

## Blockieren von VPN-Clients, die widerrufene Zertifikate verwenden

Nachdem Sie Updates installiert haben, kann der RRAS-Server die Zertifikat Sperrung für VPNs erzwingen, die IKEv2-und Computer Zertifikate für die Authentifizierung verwenden, z. b. Geräte Tunnel-Always-on-VPNs. Dies bedeutet, dass der RRAS-Server für solche VPNs VPN-Verbindungen zu Clients verweigern kann, die versuchen, ein gesperrtes Zertifikat zu verwenden.

### Verfügbarkeit

In der folgenden Tabelle sind die Versionen aufgeführt, die die Fixes für jede Windows-Version enthalten.

BETRIEBSSYSTEMVERSION	VERSION
Windows Server, Version 1903	<a href="#">KB4501375</a>
Windows Server 2019 Windows Server, Version 1809	<a href="#">KB4505658</a>
Windows Server, Version 1803	<a href="#">KB4507466</a>

BETRIEBSSYSTEMVERSION	VERSION
Windows Server, Version 1709	<a href="#">KB4507465</a>
Windows Server 2016, Version 1607	<a href="#">KB4503294</a>

## Vorgehensweise beim Konfigurieren der Voraussetzungen

1. Installieren Sie die Windows-Updates, sobald Sie verfügbar werden.
2. Stellen Sie sicher, dass alle VPN-Client- und RRAS-Server-Zertifikate, die Sie verwenden, über CDP-Einträge verfügen und dass der RRAS-Server die entsprechenden CRLs erreichen kann.
3. Verwenden Sie auf dem RRAS-Server das PowerShell-Cmdlet `Set-vpnauthprotocol`, um den Parameter `rootcertificatenametoaccept` zu konfigurieren.

Im folgenden Beispiel werden die zu diesem Zweck aufgeführten Befehle aufgelistet. Im Beispiel stellt CN = die Stamm Zertifizierungsstelle von "CN =" den Distinguished Name der Stamm Zertifizierungsstelle dar.

```
$cert1 = ( Get-ChildItem -Path cert:LocalMachine\root | Where-Object -FilterScript { $_.Subject -Like "*CN=Contoso Root Certification Authority*" } )
Set-VpnAuthProtocol -RootCertificateNameToAccept $cert1 -PassThru
```

## Konfigurieren des RRAS-Servers, um die Zertifikat Sperrung für VPN-Verbindungen zu erzwingen, die auf IKEv2-Computer-Zertifikaten basieren

1. Führen Sie in einem Eingabe Aufforderungs Fenster den folgenden Befehl aus:

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\Ikev2 /f /v CertAuthFlags /t REG_DWORD /d "4"
```

2. Starten Sie den Routing-und RAS-Dienst neu.

Um die Zertifikat Sperrung für diese VPN-Verbindungen zu deaktivieren, legen Sie `certauthflags` = 2 fest, oder entfernen Sie den Wert `certauthflags`, und starten Sie dann den Routing-und RAS-Dienst neu.

## Widerrufen eines VPN-Client-Zertifikats für eine VPN-Verbindung, die auf einem IKEv2-Computer-Zertifikat basiert

1. Widerrufen Sie das VPN-Client-Zertifikat von der Zertifizierungsstelle.
2. Veröffentlichen Sie eine neue CRL von der Zertifizierungsstelle.
3. Öffnen Sie auf dem RRAS-Server ein Administrator Eingabe Aufforderungs Fenster, und führen Sie dann die folgenden Befehle aus:

```
certutil -urlcache * delete
certutil -setreg chain\ChainCacheResyncFiletime @now
```

## Überprüfen, ob die Zertifikat Sperrung für Zertifikat basierte VPN-Verbindungen auf IKEv2-Computern funktioniert

### NOTE

Bevor Sie dieses Verfahren verwenden, stellen Sie sicher, dass Sie das Betriebs Ereignisprotokoll CAPI2 aktivieren.

1. Führen Sie die vorherigen Schritte aus, um ein VPN-Client-Zertifikat aufzuheben.

2. Versuchen Sie, mithilfe eines Clients, der über das gesperrte Zertifikat verfügt, eine Verbindung mit dem VPN herzustellen. Der RRAS-Server sollte die Verbindung ablehnen und eine Meldung wie "die Anmelde Informationen für die IKE-Authentifizierung sind nicht zulässig" anzeigen.
3. Öffnen Sie auf dem RRAS-Server Ereignisanzeige, und navigieren Sie zu **Anwendungs-und Dienst Protokolle/Microsoft/Windows/CAPI2**.
4. Suchen Sie nach einem Ereignis, das die folgenden Informationen enthält:

- Protokoll Name: **Microsoft-Windows-CAPI2/Operational Microsoft-Windows-CAPI2/Operational**
- Ereignis-ID: **41**
- Das Ereignis enthält den folgenden Text: **Subject = "Client FQDN"** (*Client-FQDN* steht für den voll qualifizierten Domänen Namen des Clients, der über das gesperrte Zertifikat verfügt).

Das -Feld der Ereignisdaten sollte einschließen, dass **das Zertifikat gesperrt ist**. Sehen Sie sich beispielsweise die folgenden Ausschnitte eines Ereignisses an:

```

Log Name:      Microsoft-Windows-CAPI2/Operational Microsoft-Windows-CAPI2/Operational
Source:        Microsoft-Windows-CAPI2
Date:          5/20/2019 1:33:24 PM
Event ID:      41
...
Event Xml:
<Event xmlns="https://schemas.microsoft.com/win/2004/08/events/event">
  <UserData>
    <CertVerifyRevocation>
      <Certificate fileRef="C97AE73E9823E8179903E81107E089497C77A720.cer"
subjectName="client01.corp.contoso.com" />
      <IssuerCertificate fileRef="34B1AE2BD868FE4F8BFDC96E47C87C12BC01E3A.cer" subjectName="Contoso Root
Certification Authority" />
      ...
      <Result value="80092010">The certificate is revoked.</Result>
    </CertVerifyRevocation>
  </UserData>
</Event>
```

## Zusätzlicher Schutz

### **TPM-Schlüssel Nachweis (Trusted Platform Module)**

Ein Benutzerzertifikat, das über einen TPM-geprüften Schlüssel verfügt, bietet eine höhere Sicherheitsgarantie, die durch nicht Exportierbarkeit, Anti-hammerung und Isolation der von TPM bereitgestellten Schlüssel gesichert wird.

Weitere Informationen zum TPM-Schlüssel Nachweis in Windows 10 finden Sie unter [TPM Key Nachweis](#).

## Nächster Schritt

[Planen der Always on-VPN-Bereitstellung](#): führen Sie vor der Installation der Remote Zugriffs-Server Rolle auf dem Computer, den Sie als VPN-Server verwenden möchten, die folgenden Aufgaben aus. Nach der entsprechenden Planung können Sie Always on VPN bereitstellen und optional den bedingten Zugriff für VPN-Konnektivität mithilfe Azure AD konfigurieren.

## Verwandte Themen

- [NPS-Proxy Server-Lastenausgleich](#): Remote Authentication Dial-in User Service (RADIUS)-Clients, bei denen es sich um Netzwerk Zugriffs Server wie VPN-Server (virtuelles privates Netzwerk) und drahtlos

Zugriffspunkte handelt, erstellen Sie Verbindungsanforderungen und senden diese an RADIUS-Server wie z. b. NPS. In einigen Fällen kann ein NPS-Server zu viele Verbindungsanforderungen gleichzeitig empfangen, was zu einer Beeinträchtigung der Leistung oder einer Überlastung führt.

- [Übersicht über Traffic Manager](#): dieses Thema bietet einen Überblick über Azure Traffic Manager, mit dem Sie die Verteilung von Benutzer Datenverkehr für Dienst Endpunkte steuern können. Traffic Manager verwendet die Domain Name System (DNS), um Client Anforderungen auf der Grundlage einer Datenverkehrs Routing-Methode und der Integrität der Endpunkte an den am besten geeigneten Endpunkt weiterzuleiten.
- [Windows Hello for Business](#): dieses Thema enthält die Voraussetzungen, wie z. b. reine Cloud-bereit Stellungen und Hybrid Bereitstellungen. Außerdem werden in diesem Thema häufig gestellte Fragen zu Windows Hello for Business aufgeführt.
- [Technische Fallstudie: Aktivieren des Remote Zugriffs mit Windows Hello for Business in Windows 10](#): in dieser technischen Fallstudie erfahren Sie, wie Microsoft den Remote Zugriff mit Windows Hello for Business implementiert. Bei Windows Hello for Business handelt es sich um einen privaten/öffentlichen oder Zertifikat basierten Authentifizierungs Ansatz für Unternehmen und Consumer, die über die Kenn Wörter hinausgehen. Diese Form der Authentifizierung basiert auf Schlüsselpaar-Anmelde Informationen, die Kenn Wörter ersetzen können und gegen Verstöße, Dieb zierungen und Phishing verstößen.
- [Integrieren der RADIUS-Authentifizierung in Azure Multi-Factor Authentication-Server](#): in diesem Thema wird schrittweise erläutert, wie Sie eine RADIUS-Client Authentifizierung mit Azure Multi-Factor Authentication-Server hinzufügen und konfigurieren. RADIUS ist ein Standardprotokoll zum Annehmen und Verarbeiten von Authentifizierungsanforderungen. Der Azure-Multi-Factor Authentication-Server kann als RADIUS-Server fungieren.
- [VPN-Sicherheitsfeatures](#): in diesem Thema finden Sie VPN-Sicherheitsrichtlinien für das Sperren von VPN, die WIP-Integration (Windows Information Protection) mit VPN und Datenverkehrs Filter.
- [Automatisch ausgelöste VPN-Profil Optionen](#): dieses Thema bietet Ihnen automatisch ausgelöste VPN-Profil Optionen, z. b. app-Trigger, namensbasierte Trigger und Always on.
- [VPN und bedingter Zugriff](#): in diesem Thema erhalten Sie einen Überblick über die cloudbasierte Plattform für den bedingten Zugriff, die eine Geräte Kompatibilitäts Option für Remote Clients bereitstellt. Beim bedingten Zugriff handelt es sich um ein richtlinienbasiertes Auswertungsmodul, mit dem Sie Zugriffsregeln für alle mit Azure Active Directory (Azure AD) verknüpften Anwendungen erstellen können.
- [TPM-SchlüsselNachweis](#): in diesem Thema erhalten Sie einen Überblick über Trusted Platform Module (TPM) und die Schritte zum Bereitstellen von TPM-Schlüssel Nachweis. Außerdem finden Sie Informationen zur Problembehandlung und zu den Schritten, um Probleme zu beheben.

# Always On VPN bereitstellen

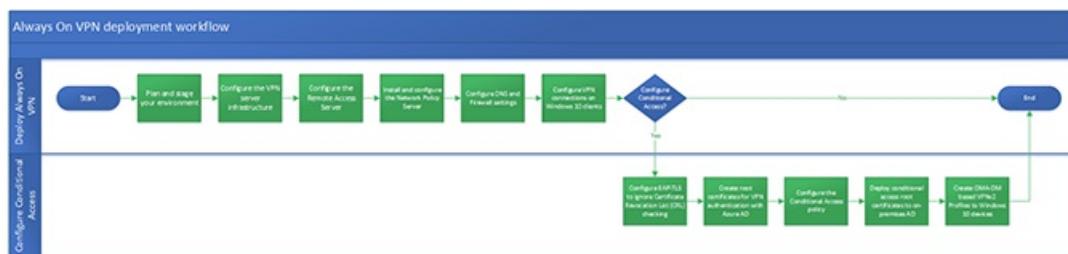
09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Vorheriges:** Erfahren Sie mehr über die erweiterten Features für Always on-VPN
  - **Weiter:** Schritt 1: Beginnen der Planung der Always on-VPN-Bereitstellung

In diesem Abschnitt erfahren Sie mehr über den Workflow für die Bereitstellung von Always on-VPN-Verbindungen für in die Domäne eingebundenen Windows 10-Client Computern. Wenn Sie den **bedingten Zugriff konfigurieren** möchten, um zu optimieren, wie VPN-Benutzer auf Ihre Ressourcen zugreifen, finden Sie unter [bedingter Zugriff für VPN-Konnektivität mithilfe von Azure AD](#) Weitere Informationen. Weitere Informationen zum bedingten Zugriff für VPN-Konnektivität mithilfe von Azure AD finden Sie unter [bedingter Zugriff in Azure Active Directory](#).

Das folgende Diagramm veranschaulicht den Workflow Prozess für die verschiedenen Szenarien beim Bereitstellen Always on VPN:



**IMPORTANT**

Für diese Bereitstellung ist es nicht erforderlich, dass auf Ihren Infrastruktur Servern, z. B. Computern, auf denen Active Directory Domain Services, Active Directory Zertifikat Dienste und Netzwerk Richtlinien Server ausgeführt wird, Windows Server 2016 ausgeführt wird. Sie können ältere Versionen von Windows Server, wie z. B. Windows Server 2012 R2, für die Infrastruktur Server und für den Server verwenden, auf dem Remote Zugriff ausgeführt wird.

## Schritt 1: Planen der Always on VPN-Bereitstellung

In diesem Schritt beginnen Sie mit der Planung und Vorbereitung ihrer Always on-VPN-Bereitstellung. Vor der Installation der Remote Zugriffs-Server Rolle auf dem Computer, den Sie als VPN-Server verwenden möchten. Nach dem ordnungsgemäßen Planen können Sie Always On VPN bereitstellen und optional den bedingten Zugriff für VPN-Konnektivität mit Azure AD konfigurieren.

## Schritt 2: Konfigurieren der Always on VPN-Server Infrastruktur

In diesem Schritt installieren und konfigurieren Sie die serverseitigen Komponenten, die zur Unterstützung des VPN erforderlich sind. Zu den serverseitigen Komponenten gehört das Konfigurieren der PKI für die Verteilung der Zertifikate, die von Benutzern, dem VPN-Server und dem NPS-Server verwendet werden. Außerdem konfigurieren Sie RRAS für die Unterstützung von IKEv2-Verbindungen und den NPS-Server zum Ausführen der Autorisierung für die VPN-Verbindungen.

Zum Konfigurieren der Serverinfrastruktur müssen Sie die folgenden Aufgaben ausführen:

- Auf einem mit Active Directory Domain Services konfigurierten Server: Aktivieren Sie die automatische Zertifikat Registrierung in Gruppenrichtlinie für Computer und Benutzer, erstellen Sie die Gruppe "VPN-Benutzer", die Gruppe "VPN-Server" und die Gruppe "NPS-Server", und fügen Sie jeder Gruppe Mitglieder hinzu.
- Auf einer Active Directory Zertifikat Server-Zertifizierungsstelle: Erstellen Sie die Zertifikat Vorlagen Benutzeroauthentifizierung, VPN-Server Authentifizierung und NPS-Server Authentifizierung.
- Auf in die Domäne eingebundenen Windows 10-Clients: Registrieren und Validieren von Benutzer Zertifikaten

## Schritt 3. Konfigurieren des Remote Zugriffs Servers für die Always on-VPN

In diesem Schritt konfigurieren Sie das RAS-VPN, um IKEv2-VPN-Verbindungen zuzulassen, Verbindungen von anderen VPN-Protokollen zu verweigern und einen statischen IP-Adresspool für die Ausstellung von IP-Adressen für die Verbindung mit autorisierten VPN-Clients zuzuweisen.

Zum Konfigurieren von RAS müssen Sie die folgenden Aufgaben ausführen:

- Registrieren und Validieren des VPN-Serverzertifikats
- Installieren und Konfigurieren des RAS-VPN

## Schritt 4: Installieren und Konfigurieren des NPS-Servers

In diesem Schritt installieren Sie den Netzwerk Richtlinien Server (Network Policy Server, NPS) mithilfe von Windows PowerShell oder dem Server-Manager Assistenten zum Hinzufügen von Rollen und Features. Außerdem können Sie NPS so konfigurieren, dass alle Authentifizierungs-, Autorisierungs-und Buchhaltungsaufgaben für Verbindungsanforderungen verarbeitet werden, die vom VPN-Server empfangen werden.

Zum Konfigurieren von NPS müssen Sie die folgenden Aufgaben ausführen:

- Registrieren des NPS-Servers in Active Directory
- Konfigurieren der RADIUS-Kontoführung für Ihren NPS-Server
- Hinzufügen des VPN-Servers als RADIUS-Client in NPS
- Konfigurieren der Netzwerk Richtlinie in NPS
- Automatische Registrierung des NPS-Server Zertifikats

## Schritt 5: Konfigurieren von DNS-und Firewalleinstellungen für Always on-VPN

In diesem Schritt konfigurieren Sie DNS-und Firewalleinstellungen. Wenn Remote-VPN-Clients eine Verbindung herstellen, verwenden Sie die gleichen DNS-Server, die von den internen Clients verwendet werden. auf diese Weise können Namen auf die gleiche Weise wie die übrigen internen Arbeitsstationen aufgelöst werden.

## Schritt 6: Konfigurieren von Windows 10-Client Always on-VPN-Verbindungen

In diesem Schritt konfigurieren Sie die Windows 10-Client Computer für die Kommunikation mit dieser Infrastruktur über eine VPN-Verbindung. Sie können verschiedene Technologien zum Konfigurieren von Windows 10-VPN-Clients verwenden, einschließlich Windows PowerShell, Microsoft Endpoint Configuration Manager und InTune. Alle drei erfordern ein XML-VPN-Profil, um die entsprechenden VPN-Einstellungen zu konfigurieren.

## Schritt 7: Optionale Konfigurieren des bedingten Zugriffs für VPN-Konnektivität

In diesem optionalen Schritt können Sie optimieren, wie autorisierte VPN-Benutzer auf Ihre Ressourcen zugreifen. Mit Azure AD bedingten Zugriff für VPN-Konnektivität können Sie die VPN-Verbindungen schützen. Der bedingte Zugriff ist eine Richtlinien basierte Evaluierungs-Engine, mit der Sie Zugriffsregeln für alle Azure AD verbundenen Anwendungen erstellen können. Weitere Informationen finden Sie unter [Azure Active Directory \(Azure AD\) bedingtem Zugriff](#).

## Nächster Schritt

[Schritt 1: Planen Sie die Always on-VPN-Bereitstellung](#): vor der Installation der RAS-Server Rolle auf dem Computer, den Sie als VPN-Server verwenden möchten. Nach dem ordnungsgemäßen Planen können Sie Always On VPN bereitstellen und optional den bedingten Zugriff für VPN-Konnektivität mit Azure AD konfigurieren.

# Schritt 1 Planen der Always On VPN-Bereitstellung

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges](#): Erfahren Sie mehr über den Workflow für die Bereitstellung Always on VPN
- [Weiter](#): Schritt 2: Konfigurieren der Server Infrastruktur

In diesem Schritt beginnen Sie mit der Planung und Vorbereitung ihrer Always on-VPN-Bereitstellung. Bevor Sie die Remote Zugriffs-Server Rolle auf dem Computer installieren, den Sie als VPN-Server verwenden möchten, führen Sie die folgenden Aufgaben aus. Nach dem ordnungsgemäßen Planen können Sie Always On VPN bereitstellen und optional den bedingten Zugriff für VPN-Konnektivität mit Azure AD konfigurieren.

## Überlegungen zur Standard-Konfiguration

Always On-VPN-verfügt über viele Konfigurationsoptionen. Aber Sie Ihr VPN-Konfiguration auswählen, sind jedoch die folgende Informationen an:

- **Verbindungstyp.** Verbindung Protokollauswahl ist wichtig und letztendlich geht hand in hand mit dem Typ der Authentifizierung, die Sie verwenden möchten. Weitere Informationen über die Tunneling-Protokolle verfügbar sind, finden Sie unter [VPN-Verbindungstypen](#).
- **Routing.** In diesem Kontext bestimmen Routingregeln an, ob der Benutzer andere Netzwerk Routen während der Verbindung mit dem VPN verwenden können.
  - *Getrenntes Tunneln* der gleichzeitige Zugriff auf andere Netzwerke wie das Internet ermöglicht.
  - *Erzwingen von Tunneln* muss der gesamte Datenverkehr an das VPN ausschließlich durchlaufen und lässt keine gleichzeitigen Zugriff auf andere Netzwerke.
- **Auslösen.** *Auslösen von* bestimmt, wie und wann eine VPN-Verbindung initiiert wird (z. B. wenn eine app öffnet, wenn das Gerät manuell, durch den Benutzer aktiviert ist). Zum Auslösen von Optionen, finden Sie unter den [VPN-Profil automatisch ausgelöste Optionen](#).
- **Gerät oder die Benutzerauthentifizierung.** Always On-VPN-verwendet Zertifikate für Geräte und vom Gerät initiiert Verbindung über ein Feature namens [Gerät Tunnel](#). Diese Verbindung kann automatisch initiiert werden und ist persistent, ähnlich wie eine tunnelverbindung des DirectAccess-Infrastruktur.

### TIP

Beim Migrieren von DirectAccess zu Always On-VPN-sollten Sie die verschiedenen Konfigurationsoptionen, die vergleichbar sind, was Sie haben, und erweitern Sie dann von dort ab.

Mithilfe von Benutzerzertifikaten, der Always On-VPN-Client verbindet sich automatisch, aber dies erfolgt auf Benutzerebene (nach der Benutzeranmeldung) anstatt auf Geräteebene (vor der Benutzeranmeldung). Die benutzererfahrung ist weiterhin für den Benutzer nahtlos, aber sie unterstützt erweiterte Authentifizierungsmechanismen, z.B. Windows Hello for Business.

## Vorbereiten des Remote Zugriffs Servers

Sie müssen auf dem Computer, der als VPN-Server verwendet wird, folgende Schritte ausführen:

- **Stellen Sie sicher, dass die VPN-Server Software und die Hardwarekonfiguration korrekt sind.**  
Installieren Sie Windows Server 2016 auf dem Computer, den Sie als RAS-VPN-Server verwenden möchten. Auf diesem Server müssen zwei physische Netzwerkadapter installiert sein, eine zum Herstellen einer Verbindung mit dem externen Umkreis Netzwerk und eine, um eine Verbindung mit dem internen Umkreis Netzwerk herzustellen.
- **Identifizieren Sie, welcher Netzwerkadapter eine Verbindung mit dem Internet herstellt und welcher Netzwerkadapter eine Verbindung mit Ihrem privaten Netzwerk herstellt.** Konfigurieren Sie den Netzwerkadapter für das Internet mit einer öffentlichen IP-Adresse, während der Adapter für das Intranet eine IP-Adresse aus dem lokalen Netzwerk verwenden kann.

#### TIP

Wenn Sie nicht möchten, dass Sie eine öffentliche IP-Adresse in Ihrem Umkreis Netzwerk verwenden, können Sie die Edge-Firewall mit einer öffentlichen IP-Adresse konfigurieren und dann die Firewall so konfigurieren, dass VPN-Verbindungsanforderungen an den VPN-Server weiterleiten.

- **Verbinden Sie den VPN-Server mit dem Netzwerk.** Installieren Sie den VPN-Server in einem Umkreis Netzwerk zwischen der Edge-Firewall und der Umkreis Firewall.

## Planen von Authentifizierungsmethoden

IKEv2 ist ein VPN-Tunnelingprotokoll, das in [Internet Engineering Task Force Request for Comments 7296](#) beschrieben wird. Der Hauptvorteil von IKEv2 besteht darin, dass Unterbrechungen in der zugrunde liegenden Netzwerkverbindung toleriert werden. Wenn z. B. ein vorübergehender Verbindungsverlust oder ein Benutzer einen Client Computer von einem Netzwerk auf einen anderen verschiebt, stellt beim erneuten Herstellen der Netzwerkverbindung die VPN-Verbindung automatisch – ohne Benutzereingriff wieder her.

#### TIP

Sie können den RAS-VPN-Server so konfigurieren, dass IKEv2-Verbindungen unterstützt werden, während nicht verwendete Protokolle deaktiviert werden, wodurch die Sicherheitsanforderungen des Servers reduziert werden.

## Planen von IP-Adressen für Remote Clients

Sie können den VPN-Server so konfigurieren, dass er VPN-Clients Adressen von einem statischen Adresspool, den Sie konfigurieren, oder von IP-Adressen eines DHCP-Servers zuweist.

## Vorbereiten der Umgebung

- **Stellen Sie sicher, dass Sie über die Berechtigungen zum Konfigurieren der externen Firewall verfügen und dass Sie über eine gültige öffentliche IP-Adresse verfügen.** Öffnen von Ports in der Firewall zur Unterstützung von IKEv2-VPN-Verbindungen. Außerdem benötigen Sie eine öffentliche IP-Adresse, um Verbindungen von externen Clients zu akzeptieren.
- **Wählen Sie einen Bereich statischer IP-Adressen für VPN-Clients aus.** Bestimmen Sie die maximale Anzahl von gleichzeitigen VPN-Clients, die Sie unterstützen möchten. Planen Sie außerdem einen Bereich statischer IP-Adressen im internen Umkreis Netzwerk, um diese Anforderung zu erfüllen, nämlich den *statischen Adresspool*. Wenn Sie DHCP zum Angeben von IP-Adressen für die interne DMZ verwenden, müssen Sie möglicherweise auch einen Ausschluss für diese statischen IP-Adressen in DHCP erstellen.

- Stellen Sie sicher, dass Sie die öffentliche DNS-Zone bearbeiten können. Fügen Sie Ihrer öffentlichen DNS-Domäne DNS-Einträge zur Unterstützung der VPN-Infrastruktur hinzu.
- Stellen Sie sicher, dass alle VPN-Benutzer über Benutzerkonten in Active Directory Benutzer (AD DS) verfügen. Bevor Benutzer über VPN-Verbindungen eine Verbindung mit dem Netzwerk herstellen können, müssen Sie über Benutzerkonten in AD DS verfügen.

## Vorbereiten von Routing und Firewall

Installieren Sie den VPN-Server innerhalb des Umkreis Netzwerks, von dem das Umkreis Netzwerk in interne und externe Umkreis Netzwerke partitioniert wird. Abhängig von Ihrer Netzwerkumgebung müssen Sie möglicherweise mehrere Routing Änderungen vornehmen.

- **Optionale Konfigurieren Sie die Port Weiterleitung.** Die Edge-Firewall muss die einem IKEv2-VPN zugeordneten Ports und Protokoll-IDs öffnen und Sie an den VPN-Server weiterleiten. In den meisten Umgebungen erfordert dies, dass Sie die Port Weiterleitung konfigurieren. Leiten Sie die UDP-Ports 500 und 4500 an den VPN-Server um.
- **Konfigurieren Sie das Routing so, dass die DNS-Server und VPN-Server das Internet erreichen können.** Diese Bereitstellung verwendet IKEv2 und Network Address Translation (NAT). Stellen Sie sicher, dass der VPN-Server alle erforderlichen internen Netzwerke und Netzwerkressourcen erreichen kann. Netzwerk oder Ressourcen, die vom VPN-Server nicht erreichbar sind, sind auch über VPN-Verbindungen von Remote Standorten aus nicht erreichbar.

In den meisten Umgebungen können Sie zum Erreichen des neuen internen Umkreis Netzwerks statische Routen auf der Edge-Firewall und dem VPN-Server anpassen. In komplexeren Umgebungen müssen Sie jedoch möglicherweise statische Routen zu internen Routern hinzufügen oder interne Firewallregeln für den VPN-Server und den Block von IP-Adressen, die VPN-Clients zugeordnet sind, anpassen.

## Nächste Schritte

[Schritt 2: Konfigurieren der Serverinfrastruktur:](#) in diesem Schritt installieren und konfigurieren Sie die serverseitigen Komponenten, die zur Unterstützung des VPN erforderlich sind. Zu den serverseitigen Komponenten gehört das Konfigurieren der PKI für die Verteilung der Zertifikate, die von Benutzern, dem VPN-Server und dem NPS-Server verwendet werden.

# Schritt 2 Konfigurieren der Serverinfrastruktur

09.04.2020 • 31 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 1: Planen der Always on VPN-Bereitstellung](#)
- [Weiter: Schritt 3. Konfigurieren des Remote Zugriffs Servers für die Always on-VPN](#)

In diesem Schritt installieren und konfigurieren Sie die serverseitigen Komponenten, die zur Unterstützung des VPN erforderlich sind. Zu den serverseitigen Komponenten gehört das Konfigurieren der PKI für die Verteilung der Zertifikate, die von Benutzern, dem VPN-Server und dem NPS-Server verwendet werden. Außerdem konfigurieren Sie RRAS für die Unterstützung von IKEv2-Verbindungen und den NPS-Server zum Ausführen der Autorisierung für die VPN-Verbindungen.

## Konfigurieren der automatischen Zertifikat Registrierung in Gruppenrichtlinie

In diesem Verfahren konfigurieren Sie Gruppenrichtlinie auf dem Domänen Controller, damit Domänen Mitglieder automatisch Benutzer-und Computer Zertifikate anfordern. Auf diese Weise können VPN-Benutzer Benutzerzertifikate anfordern und abrufen, die VPN-Verbindungen automatisch authentifizieren. Ebenso ermöglicht diese Richtlinie NPS-Servern das automatische anfordern von Server Authentifizierungs Zertifikaten.

Sie registrieren Zertifikate manuell auf VPN-Servern.

### TIP

Informationen zu nicht in Domänen eingebundenen Computern finden Sie unter Zertifizierungsstellen [Konfiguration für Computer, die keiner Domäne beigetreten](#)sind. Da der RRAS-Server keiner Domäne beigetreten ist, kann die automatische Registrierung nicht zum Registrieren des VPN Gateway-Zertifikats verwendet werden. Verwenden Sie daher eine Offline-Zertifikat Anforderungs Prozedur.

1. Öffnen Sie auf einem Domänen Controller Gruppenrichtlinie-Verwaltung.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf Ihre Domäne (z. b. Corp.contoso.com), und wählen Sie dann Gruppenrichtlinien Objekt **in dieser Domäne erstellen und verknüpfen aus**.
3. Geben Sie im Dialogfeld Neues Gruppenrichtlinien Objekt die **Richtlinie**für die automatische Registrierung ein, und klicken Sie dann auf **OK**.
4. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Richtlinie**für die automatische Registrierung, und wählen Sie dann **Bearbeiten**aus.
5. Führen Sie im Gruppenrichtlinienverwaltungs-Editor die folgenden Schritte aus, um die automatische Registrierung von Computer Zertifikaten zu konfigurieren:
  - a. Navigieren Sie im Navigationsbereich zu **Computer Konfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für öffentliche Schlüssel**.
  - b. Klicken Sie im Detailfenster mit der rechten Maustaste auf **Zertifikat Dienst Client – automatische**Registrierung, und wählen Sie dann **Eigenschaften**aus.

- c. Wählen Sie im Dialogfeld Zertifikat Dienst Client – Eigenschaften für automatische Registrierung unter **Konfigurations Modell** die Option **aktiviert** aus.
  - d. Wählen Sie **Abgelaufene Zertifikate erneuern, ausstehende Zertifikate aktualisieren und gesperrte Zertifikate entfernen** und **Zertifikate, die Zertifikatvorlagen verwenden, aktualisieren** aus.
  - e. Wählen Sie OK.
6. Führen Sie im Gruppenrichtlinienverwaltungs-Editor die folgenden Schritte aus, um die automatische Registrierung von Benutzer Zertifikaten zu konfigurieren:
- a. Navigieren Sie im Navigationsbereich zu **Benutzerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für öffentliche Schlüssel**.
  - b. Klicken Sie im Detailbereich mit der rechten Maustaste auf **Zertifikatdienstclient - Automatische Registrierung**, und wählen Sie **Eigenschaften** aus.
  - c. Wählen Sie im Dialogfeld Zertifikat Dienst Client – Eigenschaften für automatische Registrierung unter **Konfigurations Modell** die Option **aktiviert** aus.
  - d. Wählen Sie **Abgelaufene Zertifikate erneuern, ausstehende Zertifikate aktualisieren und gesperrte Zertifikate entfernen** und **Zertifikate, die Zertifikatvorlagen verwenden, aktualisieren** aus.
  - e. Wählen Sie OK.
  - f. Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.

7. Schließen Sie Gruppenrichtlinienverwaltung.

### **Zertifizierungsstellen Konfiguration für Computer, die keiner Domäne beigetreten sind**

Da der RRAS-Server keiner Domäne beigetreten ist, kann die automatische Registrierung nicht zum Registrieren des VPN Gateway-Zertifikats verwendet werden. Verwenden Sie daher eine Offline-Zertifikat Anforderungs Prozedur.

1. Generieren Sie auf dem RRAS-Server eine Datei mit dem Namen **vpngateway.inf**, die auf der in Anhang a (Abschnitt 0) bereitgestellten Beispiel Zertifikat Richtlinien Anforderung basiert, und passen Sie die folgenden Einträge an:
  - Ersetzen Sie im Abschnitt [newrequest] VPN.contoso.com, der für den Antragsteller Namen verwendet wird, durch den ausgewählten [Customer] VPN Endpoint-voll qualifizierten Namen.
  - Ersetzen Sie im Abschnitt [Extensions] VPN.contoso.com, das für den alternativen Antragsteller Namen verwendet wird, durch den ausgewählten [Customer] VPN Endpoint-voll qualifizierten Namen.
2. Speichern oder kopieren Sie die Datei "**vpngateway.inf**" an einen ausgewählten Speicherort.
3. Navigieren Sie an einer Eingabeaufforderung mit erhöhten Rechten zu dem Ordner, der die Datei "**vpngateway.inf**" enthält, und geben Sie Folgendes ein:
 

```
certreq -new VPNGateway.inf VPNGateway.req
```
4. Kopieren Sie die neu erstellte **vpngateway.req**-Ausgabedatei auf einen Zertifizierungsstellen Server oder eine Arbeitsstation mit privilegiertem Zugriff (PW).
5. Speichern oder kopieren Sie die Datei "**vpngateway.req**" an einen ausgewählten Speicherort auf dem Zertifizierungsstellen Server oder auf der Arbeitsstation mit privilegiertem Zugriff (PW).

6. Navigieren Sie an einer Eingabeaufforderung mit erhöhten Rechten zu dem Ordner, der die im vorherigen Schritt erstellte vpngateway.req-Datei enthält, und geben Sie Folgendes ein:

```
certreq -attrib "CertificateTemplate:[Customer]VPNGateway" -submit VPNGateway.req VPNGateway.cer
```

7. Wenn Sie im Fenster "Zertifizierungsstellen Liste" aufgefordert werden, wählen Sie die entsprechende Unternehmens Zertifizierungsstelle für die Zertifikat Anforderung aus.
8. Kopieren Sie die neu erstellte **vpngateway.CER**-Ausgabedatei auf den RRAS-Server.
9. Speichern oder kopieren Sie die Datei "**vpngateway.CER**" an einen ausgewählten Speicherort auf dem RRAS-Server.
10. Navigieren Sie an einer Eingabeaufforderung mit erhöhten Rechten zu dem Ordner, der die im vorherigen Schritt erstellte vpngateway.CER-Datei enthält, und geben Sie Folgendes ein:

```
certreq -accept VPNGateway.cer
```

11. Führen Sie das MMC-Snap-in "Zertifikate" aus, wie [hier](#) beschrieben: Auswählen der Option **Computer Konto**.
12. Stellen Sie sicher, dass für den RRAS-Server ein gültiges Zertifikat mit den folgenden Eigenschaften vorhanden ist:
- **Beabsichtigte Zwecke:** Server Authentifizierung, IP-Sicherheits-IKE-zwischen
  - **Zertifikat Vorlage:** [Customer] VPN-Server

**Beispiel: vpngateway.inf-Skript**

Hier sehen Sie ein Beispielskript für eine Richtlinie für Zertifikat Anforderungen, die verwendet wird, um ein VPN-Gatewayzertifikat mithilfe eines Out-of-Band-Prozesses anzufordern.

**TIP**

Eine Kopie des Skripts vpngateway.inf finden Sie im IP-Kit für VPN-Angebote unter dem Ordner Zertifikat Anforderungs Richtlinien. Aktualisieren Sie nur "Subject" und "\_Continue\_" mit kundenspezifischen Werten.

```
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=vpn.contoso.com"
Exportable = FALSE
KeyLength = 2048
KeySpec = 1
KeyUsage = 0xA0
MachineKeySet = True
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
RequestType = PKCS10

[Extensions]
2.5.29.17 = "{text}"
_continue_ = "dns=vpn.contoso.com&"
```

## Erstellen der Gruppen VPN-Benutzer, VPN-Server und NPS-Server

In diesem Verfahren können Sie eine neue Active Directory (AD)-Gruppe hinzufügen, die die Benutzer enthält, die das VPN verwenden dürfen, um eine Verbindung mit Ihrem Organisations Netzwerk herzustellen.

Diese Gruppe dient zwei Zwecken:

- Es definiert, welche Benutzer die automatische Registrierung für die für das VPN erforderlichen Benutzerzertifikate durchführen dürfen.
- Es definiert, welche Benutzer der NPS für den VPN-Zugriff autorisiert.

Wenn Sie mit einer benutzerdefinierten Gruppe den VPN-Zugriff eines Benutzers widerrufen möchten, können Sie diesen Benutzer aus der Gruppe entfernen.

Außerdem fügen Sie eine Gruppe hinzu, die VPN-Server und eine andere Gruppe mit NPS-Servern enthält. Sie verwenden diese Gruppen, um Zertifikat Anforderungen auf ihre Mitglieder einzuschränken.

#### **NOTE**

Wir empfehlen, dass VPN-Server, die sich im DMA/Umkreis befinden, nicht in die Domäne aufgenommen werden. Wenn Sie jedoch bevorzugen, dass die VPN-Server der Domäne beitreten, um eine bessere Verwaltbarkeit zu erzielen (Gruppenrichtlinien, Sicherungs-/Überwachungs-Agent, keine lokalen Benutzer zu verwalten usw.), fügen Sie der VPN-Serverzertifikat Vorlage eine Ad-Gruppe hinzu.

### **Konfigurieren der Gruppe "VPN-Benutzer"**

1. Öffnen Sie auf einem Domänen Controller Active Directory Benutzer und Computer.
2. Klicken Sie mit der rechten Maustaste auf einen Container oder eine Organisationseinheit, und wählen Sie neu und dann Gruppe aus.
3. Geben Sie unter Gruppenname den Namen **VPN-Benutzerein**, und klicken Sie auf OK.
4. Klicken Sie mit der rechten Maustaste auf **VPN-Benutzer** und wählen Sie Eigenschaften
5. Wählen Sie im Dialogfeld Eigenschaften von VPN-Benutzer auf der Registerkarte **Mitglieder** die Option Hinzufügенаus.
6. Fügen Sie im Dialogfeld Benutzer auswählen alle Benutzer hinzu, die VPN-Zugriff benötigen, und wählen Sie OK aus.
7. Schließen Sie Active Directory-Benutzer und -Computer.

### **Konfigurieren der VPN-Server und NPS-Server Gruppen**

1. Öffnen Sie auf einem Domänen Controller Active Directory Benutzer und Computer.
2. Klicken Sie mit der rechten Maustaste auf einen Container oder eine Organisationseinheit, und wählen Sie neu und dann Gruppe aus.
3. Geben Sie unter Gruppenname den Namen **VPN-Serveein**, und klicken Sie auf OK.
4. Klicken Sie mit der rechten Maustaste auf **VPN-Server** und wählen Sie Eigenschaften
5. Wählen Sie im Dialogfeld Eigenschaften von VPN-Server auf der Registerkarte **Mitglieder** die Option Hinzufügенаus.
6. Wählen Sie Objekttypenaus, aktivieren Sie das Kontrollkästchen Computer , und klicken Sie dann auf OK.
7. Geben Sie unter Geben Sie die zu ausgewählenden Objektnamenein die Namen Ihrer VPN-Server ein, und klicken Sie dann auf OK.
8. Wählen Sie OK aus, um das Dialogfeld VPN-Server Eigenschaften zu schließen.

9. Wiederholen Sie die vorherigen Schritte für die NPS-Server Gruppe.

10. Schließen Sie Active Directory-Benutzer und -Computer.

## Erstellen der Benutzer Authentifizierungs Vorlage

In diesem Verfahren konfigurieren Sie eine benutzerdefinierte Client-Server-Authentifizierungs Vorlage. Diese Vorlage ist erforderlich, da Sie die Gesamtsicherheit des Zertifikats verbessern möchten, indem Sie aktualisierte Kompatibilitäts Grade auswählen und den Kryptografieanbieter der Microsoft-Plattform auswählen. Mit dieser letzten Änderung können Sie das TPM auf den Client Computern zum Sichern des Zertifikats verwenden. Eine Übersicht über das TPM finden Sie unter [Übersicht](#) über die Trusted Platform Module-Technologie.

### IMPORTANT

Der Kryptografieanbieter für Microsoft-Plattformen erfordert einen TPM-Chip, falls Sie einen virtuellen Computer ausführen, und Sie erhalten die folgende Fehlermeldung: "Es wurde kein gültiger CSP auf dem lokalen Computer gefunden". Wenn Sie versuchen, das Zertifikat manuell zu registrieren, müssen Sie "Microsoft Software Key Storage" prüfen. Anbieter "und nach" der Microsoft-Plattform-Kryptografieanbieter "auf der Registerkarte" Kryptografie "in den Zertifikat Eigenschaften".

### Dringlichkeit

1. Öffnen Sie auf der Zertifizierungsstelle die Zertifizierungsstelle.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Zertifikat Vorlagen**, und wählen Sie **Verwalten** aus.
3. Klicken Sie in der Konsole Zertifikat Vorlagen mit der rechten Maustaste auf **Benutzer**, und wählen Sie **Doppelte Vorlage** aus.

### WARNING

Wählen Sie vor Schritt 10 nicht **anwenden** oder **OK** aus. Wenn Sie diese Schaltflächen vor dem Eingeben aller Parameter auswählen, werden viele Optionen korrigiert und können nicht mehr bearbeitet werden. Wenn z. b. auf der Registerkarte **Cryptography** der *Legacy-Kryptografiespeicheranbieter* im Feld Anbieter Kategorie angezeigt wird, wird dieser deaktiviert und verhindert weitere Änderungen. Die einzige Alternative besteht darin, die Vorlage zu löschen und neu zu erstellen.

4. Führen Sie im Dialogfeld Eigenschaften der neuen Vorlage auf der Registerkarte **Allgemein** die folgenden Schritte aus:
  - a. Geben Sie unter **Vorlagen Anzeige Name** den Namen **VPN-Benutzerauthentifizierung** ein.
  - b. Deaktivieren Sie das Kontrollkästchen **Zertifikat in Active Directory veröffentlichen**.
5. Führen Sie auf der Registerkarte **Sicherheit** die folgenden Schritte aus:
  - a. Wählen Sie **Hinzufügen**.
  - b. Geben Sie im Dialogfeld Benutzer, Computer, Dienst Konten oder Gruppen auswählen die Option **VPN-Benutzer** ein, und klicken Sie dann auf **OK**.
  - c. Wählen Sie unter **Gruppen- oder Benutzernamen** die Option **VPN-Benutzer** aus.
  - d. Aktivieren Sie in **Berechtigungen für VPN-Benutzer** der Spalte **zulassen** die Kontroll Kästchen **registrieren** und **automatisch registrieren**.

**TIP**

Stellen Sie sicher, dass das Kontrollkästchen Lesen aktiviert ist. Anders ausgedrückt: Sie benötigen die Leseberechtigungen für die Registrierung.

- e. Klicken Sie unter **Gruppen- oder Benutzernamenauf Domänen Benutzer**, und wählen Sie dann **Entfernen** aus.
6. Führen Sie auf der Registerkarte **Kompatibilität** die folgenden Schritte aus:
  - a. Wählen Sie unter **Zertifizierungsstelle** die Option **Windows Server 2012 R2** aus.
  - b. Klicken Sie im Dialogfeld **resultierende Änderungen** auf **OK**.
  - c. Wählen Sie unter **Zertifikat Empfänger** den Eintrag **Windows 8.1/Windows Server 2012 R2** aus.
  - d. Klicken Sie im Dialogfeld **resultierende Änderungen** auf **OK**.
7. Deaktivieren Sie auf der Registerkarte **Anforderungs Verarbeitung** das Kontrollkästchen **Exportieren von privatem Schlüssel zulassen**.
8. Führen Sie auf der Registerkarte **Cryptography** die folgenden Schritte aus:
  - a. Wählen Sie unter **Anbieter Kategorie** die Option **Schlüsselspeicher Anbieter** aus.
  - b. Für **SELECT-Anforderungen** muss einer der folgenden Anbieter verwendet werden.
  - c. Aktivieren Sie das Kontrollkästchen **Kryptografieanbieter für Microsoft-Plattform**.
9. Wenn Sie auf der Registerkarte **Antragsteller Name** keine e-Mail-Adresse für alle Benutzerkonten aufgelistet haben, deaktivieren Sie die Kontrollkästchen **e-Mail-Name** in **Antragsteller Name** und **e-Mail-Name** einschließen.
10. Wählen Sie **OK** aus, um die Zertifikat Vorlage VPN-Benutzeroauthentifizierung zu speichern.
11. Schließen Sie die Zertifikatvorlagenkonsole.
12. Klicken Sie im Navigationsbereich des Zertifizierungsstellen-Snap-Ins mit der rechten Maustaste auf **Zertifikat Vorlagen**, wählen Sie **neu** und dann auszustellende **Zertifikat Vorlage** aus.
13. Wählen Sie **VPN-Benutzeroauthentifizierung**, und klicken Sie dann auf **OK**.
14. Schließen Sie das Snap-in "Zertifizierungsstelle".

## Erstellen der Vorlage für die VPN-Server Authentifizierung

In diesem Verfahren können Sie eine neue Server Authentifizierungs Vorlage für den VPN-Server konfigurieren. Durch das Hinzufügen der IPSec-IKE-zwischen Anwendungs Richtlinie (IP Security, IPSec) kann der Server Zertifikate filtern, wenn mehr als ein Zertifikat mit der erweiterten Schlüssel Verwendung der Server Authentifizierung verfügbar ist.

**IMPORTANT**

Da VPN-Clients über das öffentliche Internet auf diesen Server zugreifen, unterscheiden sich die Antragsteller Namen und alternativen Namen von dem internen Servernamen. Daher können Sie dieses Zertifikat nicht automatisch auf VPN-Servern registrieren.

## Voraussetzung

In die Domäne eingebundenen VPN-Servern

### Dringlichkeit

1. Öffnen Sie auf der Zertifizierungsstelle die Zertifizierungsstelle.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Zertifikat Vorlagen**, und wählen Sie **Verwalten** aus.
3. Klicken Sie in der Konsole Zertifikat Vorlagen mit der rechten Maustaste auf **RAS-und IAS-Server**, und wählen Sie **Doppelte Vorlage**.
4. Geben Sie im Dialogfeld Eigenschaften der neuen Vorlage auf der Registerkarte **Allgemein** unter **Vorlagen Anzeige Name** einen beschreibenden Namen für den VPN-Server ein, z. B. **VPN-Server Authentifizierung** oder **RADIUS-Server**.
5. Führen Sie auf der Registerkarte **Erweiterungen** die folgenden Schritte aus:
  - a. Wählen Sie **Anwendungsrichtlinien** und dann **Bearbeiten** aus.
  - b. Wählen Sie im Dialogfeld **Anwendungsrichtlinien Erweiterung bearbeiten** die Option **Hinzufügen** aus.
  - c. Wählen Sie im Dialogfeld **Anwendungs Richtlinie hinzufügen** die Option **IP-Sicherheit IKE zwischenaus**, und klicken Sie dann auf **OK**.

Das Hinzufügen der IP-Sicherheits-IKE Intermediate zur EKU unterstützt Szenarien, in denen mehrere Server Authentifizierungs Zertifikate auf dem VPN-Server vorhanden sind. Wenn IP-Sicherheits-IKE Intermediate vorhanden ist, verwendet IPSec nur das Zertifikat mit beiden EKU-Optionen. Andernfalls kann die IKEv2-Authentifizierung mit Fehler 13801 fehlschlagen: die Anmelde Informationen für die IKE-Authentifizierung sind nicht zulässig.
  - d. Wählen Sie **OK** aus, um zum Dialogfeld **Eigenschaften der neuen Vorlage** zurückzukehren.
6. Führen Sie auf der Registerkarte **Sicherheit** die folgenden Schritte aus:
  - a. Wählen Sie **Hinzufügen**.
  - b. Geben Sie im Dialogfeld **Benutzer, Computer, Dienst Konten oder Gruppen auswählen** die Option **VPN-Server** ein, und klicken Sie dann auf **OK**.
  - c. Wählen Sie unter **Gruppen-oder Benutzernamend** die Option **VPN-Server** aus.
  - d. Aktivieren Sie in **Berechtigungen für VPN-Server** in der Spalte **zulassen** das Kontrollkästchen **registrieren**.
  - e. Wählen Sie unter **Gruppen-oder Benutzernamen RAS-und IAS-Server** aus, und klicken Sie dann auf **Entfernen**.
7. Führen Sie auf der Registerkarte **Antragsteller Name** die folgenden Schritte aus:
  - a. Wählen Sie **in der Anforderung bereitstellen** aus.
  - b. Wählen Sie im Dialogfeld **Zertifikat Vorlagen Warnung** die Option **OK** aus.
8. Optionale Wenn Sie den bedingten Zugriff für VPN-Konnektivität konfigurieren, klicken Sie auf die Registerkarte **Anforderungs Verarbeitung**, und wählen Sie dann die Option **zum Exportieren von privatem Schlüssel zulassen** aus.
9. Wählen Sie **OK** aus, um die VPN-Server Zertifikat Vorlage zu speichern.
10. Schließen Sie die Zertifikatvorlagenkonsole.

11. Klicken Sie im Navigationsbereich des Zertifizierungsstellen-Snap-Ins mit der rechten Maustaste auf **Zertifikat Vorlagen**, klicken Sie auf **neu**, und klicken Sie dann auf Auszustellende **Zertifikat Vorlage**.
  12. Starten Sie die Zertifizierungsstellen Dienste neu. (\*)
  13. Klicken Sie im Navigationsbereich des Zertifizierungsstellen-Snap-Ins mit der rechten Maustaste auf **Zertifikat Vorlagen**, wählen Sie **neu** und dann auszustellende **Zertifikat Vorlageaus**.
  14. Wählen Sie den Namen aus Schritt 4 oben aus, und klicken Sie auf **OK**.
  15. Schließen Sie das Snap-in "Zertifizierungsstelle".
- Sie können den Zertifizierungsstellen Dienst durch Ausführen des folgenden Befehls in cmd Abbrechen/starten:

```
Net Stop "certsvc"  
Net Start "certsvc"
```

## Erstellen der NPS-Server Authentifizierungs Vorlage

Die dritte und letzte zu Erstell Bare Zertifikat Vorlage ist die NPS-Server Authentifizierungs Vorlage. Die NPS-Server Authentifizierungs Vorlage ist eine einfache Kopie der RAS-und IAS-Server Vorlage, die für die NPS-Server Gruppe gesichert ist, die Sie zuvor in diesem Abschnitt erstellt haben.

Dieses Zertifikat wird für die automatische Registrierung konfiguriert.

### Dringlichkeit

1. Öffnen Sie auf der Zertifizierungsstelle die Zertifizierungsstelle.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Zertifikat Vorlagen**, und wählen Sie **Verwaltenaus**.
3. Klicken Sie in der Konsole Zertifikat Vorlagen mit der rechten Maustaste auf **RAS-und IAS-Server**, und wählen Sie **Doppelte Vorlageaus**.
4. Geben Sie im Dialogfeld Eigenschaften der neuen Vorlage auf der Registerkarte **Allgemein** unter **Vorlagen Anzeige Nameden** Namen **NPS-Server Authentifizierungein**.
5. Führen Sie auf der Registerkarte **Sicherheit** die folgenden Schritte aus:
  - a. Wählen Sie **Hinzufügen**.
  - b. Geben Sie im Dialogfeld **Benutzer, Computer, Dienst Konten oder Gruppen auswählen** die **NPS-Serverein**, und klicken Sie dann auf **OK**.
  - c. Wählen Sie unter **Gruppen-oder Benutzernamendie** Option **NPS-Serveraus**.
  - d. Aktivieren Sie in **Berechtigungen für NPS-Serverin** der Spalte **zulassen** die Kontroll Kästchen **registrieren und automatisch registrieren**.
  - e. Wählen Sie unter **Gruppen-oder Benutzernamen RAS-und IAS-Serveraus**, und klicken Sie dann auf **Entfernen**.
6. Wählen Sie **OK** aus, um die NPS-Server Zertifikat Vorlage zu speichern.
7. Schließen Sie die Zertifikatvorlagenkonsole.
8. Klicken Sie im Navigationsbereich des Zertifizierungsstellen-Snap-Ins mit der rechten Maustaste auf **Zertifikat Vorlagen**, wählen Sie **neu** und dann auszustellende **Zertifikat Vorlageaus**.

9. Wählen Sie **NPS-Server Authentifizierung** aus, und klicken Sie auf **OK**.
10. Schließen Sie das Snap-in "Zertifizierungsstelle".

## Registrieren und Validieren des Benutzer Zertifikats

Da Sie Gruppenrichtlinie für die automatische Registrierung von Benutzer Zertifikaten verwenden, müssen Sie die Richtlinie nur aktualisieren, und Windows 10 registriert automatisch das Benutzerkonto für das korrekte Zertifikat. Anschließend können Sie das Zertifikat in der Zertifikat Konsole überprüfen.

### Dringlichkeit

1. Melden Sie sich bei einem in die Domäne eingebundenen Client Computer als Mitglied der Gruppe "**VPN-Benutzer**" an.
2. Drücken Sie Windows-Taste + R, geben Sie **gpupdate/forceein**, und drücken Sie die EINGABETASTE.
3. Geben Sie im Menü Start den Befehl **Certmgr. mscein**, und drücken Sie die EINGABETASTE.
4. Wählen Sie im Zertifikate-Snap-in unter **persönlich** die Option **Zertifikate** aus. Die Zertifikate werden im Bereich Details angezeigt.
5. Klicken Sie mit der rechten Maustaste auf das Zertifikat mit Ihrem aktuellen Domänen Benutzernamen, und wählen Sie dann **Öffnen** aus.
6. Vergewissern Sie sich auf der Registerkarte **Allgemein**, dass das Datum unter **gültig ab** das heutige Datum ist. Wenn dies nicht der Fall ist, haben Sie möglicherweise das falsche Zertifikat ausgewählt.
7. Wählen Sie **OK** aus, und schließen Sie das Snap-in Zertifikate.

## Registrieren und Validieren der Server Zertifikate

Im Gegensatz zum Benutzerzertifikat müssen Sie das Zertifikat des VPN-Servers manuell registrieren. Nachdem Sie diese registriert haben, überprüfen Sie Sie mithilfe desselben Prozesses, den Sie für das Benutzerzertifikat verwendet haben. Ebenso wie das Benutzerzertifikat registriert der NPS-Server automatisch sein Authentifizierungszertifikat, sodass Sie es nur überprüfen müssen.

### NOTE

Möglicherweise müssen Sie die VPN-und NPS-Server neu starten, damit Sie Ihre Gruppenmitgliedschaften aktualisieren können, bevor Sie diese Schritte ausführen können.

### Registrieren und Validieren des VPN-Serverzertifikats

1. Geben Sie im Startmenü des VPN-Servers **certlm. mscein**, und drücken Sie die EINGABETASTE.
2. Klicken Sie mit der rechten Maustaste auf **persönlich**, wählen Sie **alle Aufgaben** aus, und wählen Sie dann **Neues Zertifikat anfordern**, um den Zertifikatregistrierungs-Assistenten
3. Wählen Sie auf der Seite Vorbereitung die Option **weiter** aus.
4. Wählen Sie auf der Seite Zertifikat Registrierungs Richtlinie auswählen die Option **weiter** aus.
5. Aktivieren Sie auf der Seite Zertifikate anfordern das Kontrollkästchen neben dem VPN-Server, um es auszuwählen.
6. Wählen Sie unter dem Kontrollkästchen VPN-Server die Option **Weitere Informationen sind erforderlich** aus, um das Dialogfeld Zertifikat Eigenschaften zu öffnen, und führen Sie die folgenden Schritte aus:

- a. Wählen Sie die Registerkarte **Betreff** aus, und wählen Sie unter Antragsteller **Name** die Option **allgemeiner Name** in **Typ**.
- b. Geben Sie unter Antragsteller **Name** unter **Wert** den Namen der externen Domänen Clients ein, die für die Verbindung mit dem VPN verwendet werden, z. B. VPN.contoso.com, und klicken Sie dann auf **Hinzufügen**.
- c. Wählen Sie unter **alternativer Name** in **Typ** die Option **DNS** aus.
- d. Geben Sie unter **alternativer Name** unter **Wert** den Namen aller Servernamen ein, die von Clients zum Herstellen einer Verbindung mit dem VPN verwendet werden, z. B. VPN.contoso.com, VPN, 132.64.86.2.
- e. Wählen Sie nach Eingabe der einzelnen Namen **Hinzufügen** aus.
- f. Klicken Sie abschließend auf **OK**.

7. Wählen Sie **Anmelden** aus.

8. Wählen Sie **Fertig stellen** aus.

9. Wählen Sie im Zertifikate-Snap-in unter **persönlich** die Option **Zertifikate** aus.

Die aufgelisteten Zertifikate werden im Bereich Details angezeigt.

10. Klicken Sie mit der rechten Maustaste auf das Zertifikat mit dem Namen des VPN-Servers, und wählen Sie dann **Öffnen** aus.
11. Vergewissern Sie sich auf der Registerkarte **Allgemein**, dass das Datum unter **gültig ab** das heutige Datum ist. Wenn dies nicht der Fall ist, haben Sie möglicherweise das falsche Zertifikat ausgewählt.
12. Wählen Sie auf der Registerkarte **Details** die Option **Erweiterte Schlüssel Verwendung** aus, und überprüfen Sie, ob **IP-Sicherheits-IKE zwischen** und **Server Authentifizierung** in der Liste angezeigt werden.
13. Wählen Sie **OK** aus, um das Zertifikat zu schließen.
14. Schließen Sie das Snap-In Zertifikate.

#### **Validieren des NPS-Serverzertifikats**

1. Starten Sie den NPS-Server neu.
2. Geben Sie im Startmenü des NPS-Servers **certlm. mscein**, und drücken Sie die EINGABETASTE.
3. Wählen Sie im Zertifikate-Snap-in unter **persönlich** die Option **Zertifikate** aus.
4. Klicken Sie mit der rechten Maustaste auf das Zertifikat mit dem Namen des NPS-Servers, und wählen Sie dann **Öffnen** aus.
5. Vergewissern Sie sich auf der Registerkarte **Allgemein**, dass das Datum unter **gültig ab** das heutige Datum ist. Wenn dies nicht der Fall ist, haben Sie möglicherweise das falsche Zertifikat ausgewählt.
6. Wählen Sie **OK** aus, um das Zertifikat zu schließen.
7. Schließen Sie das Snap-In Zertifikate.

## Nächste Schritte

[Schritt 3. Konfigurieren des RAS-Servers für Always on VPN:](#) in diesem Schritt konfigurieren Sie das RAS-VPN, um IKEv2-VPN-Verbindungen zuzulassen, Verbindungen von anderen VPN-Protokollen zu verweigern und einen

statischen IP-Adresspool für die Ausstellung von IP-Adressen für die Verbindung mit autorisierten VPN-Clients zuzuweisen.

# Schritt 3: Konfigurieren des RAS-Servers für Always On VPN

09.04.2020 • 16 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 2: Konfigurieren der Server Infrastruktur](#)
- [Vorheriges: Schritt 4: Installieren und Konfigurieren des Netzwerk Richtlinien Servers \(NPS\)](#)

RRAS ist so konzipiert, dass Sie sowohl einen Router als auch einen RAS-Server ausführen, da er eine Vielzahl von Features unterstützt. Für diese Bereitstellung benötigen Sie nur eine kleine Teilmenge dieser Features: Unterstützung für IKEv2-VPN-Verbindungen und LAN-Routing.

IKEv2 ist ein VPN-Tunnelingprotokoll, das in Internet Engineering Task Force Request for Comments 7296 beschrieben wird. Der Hauptvorteil von IKEv2 besteht darin, dass Unterbrechungen in der zugrunde liegenden Netzwerkverbindung toleriert werden. Wenn beispielsweise die Verbindung vorübergehend unterbrochen wird oder ein Benutzer einen Client Computer von einem Netzwerk auf einen anderen verschiebt, stellt IKEv2 die VPN-Verbindung automatisch wieder her, wenn die Netzwerkverbindung wieder hergestellt wird – ohne Benutzereingriff.

Konfigurieren Sie den RRAS-Server für die Unterstützung von IKEv2-Verbindungen, während nicht verwendete Protokolle deaktiviert werden, wodurch die Sicherheitsanforderungen des Servers reduziert werden. Außerdem konfigurieren Sie den Server für die Zuweisung von Adressen zu VPN-Clients aus einem statischen Adresspool. Sie können Adressen entweder aus einem Pool oder einem DHCP-Server zuweisen. die Verwendung eines DHCP-Servers erhöht jedoch die Komplexität des Entwurfs und bietet nur minimale Vorteile.

## IMPORTANT

Folgendes ist wichtig:

- Installieren Sie zwei Ethernet-Netzwerkadapter auf dem physischen Server. Wenn Sie den VPN-Server auf einem virtuellen Computer installieren, müssen Sie zwei externe virtuelle Switches erstellen, eine für jeden physischen Netzwerkadapter. Erstellen Sie dann zwei virtuelle Netzwerkadapter für die VM, wobei jeder Netzwerkadapter mit einem virtuellen Switch verbunden ist.
- Installieren Sie den Server in Ihrem Umkreis Netzwerk zwischen Ihren Edge-und internen Firewalls, mit einem Netzwerkadapter, der mit dem externen Umkreis Netzwerk verbunden ist, und einem Netzwerkadapter, der mit dem internen Umkreis Netzwerk verbunden ist.

## WARNING

Bevor Sie beginnen, stellen Sie sicher, dass Sie IPv6 auf dem VPN-Server aktivieren. Andernfalls kann keine Verbindung hergestellt werden, und es wird eine Fehlermeldung angezeigt.

## Installieren des Remote Zugriffs als RAS-Gateway-VPN-Server

In diesem Verfahren installieren Sie die Remote Zugriffs Rolle als einzelner Mandanten-RAS-Gateway-VPN-Server. Weitere Informationen finden Sie unter [Remote Access](#).

## Installieren der Remote Zugriffs Rolle mithilfe von Windows PowerShell

1. Öffnen Sie Windows PowerShell als **Administrator**.
2. Geben Sie folgendes Cmdlet ein, und führen Sie es aus:

```
Install-WindowsFeature DirectAccess-VPN -IncludeManagementTools
```

Nachdem die Installation abgeschlossen ist, wird die folgende Meldung in Windows PowerShell angezeigt.

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{RAS Connection Manager Administration Kit}

## Installieren Sie die Remote Zugriffs Rolle mit Server-Manager

Mithilfe des folgenden Verfahrens können Sie die Remote Zugriffs Rolle mithilfe von Server-Manager installieren.

1. Wählen Sie auf dem VPN-Server in Server-Manager die Option **Verwalten** aus, und wählen Sie **Rollen und Features hinzufügen** aus.

Der Assistent zum Hinzufügen von Rollen und Features wird geöffnet.

2. Wählen Sie auf der Seite Vorbereitung die Option **weiter** aus.
3. Wählen Sie auf der Seite Installationstyp auswählen die Option **rollenbasierte oder featurebasierte Installation** aus, und klicken Sie auf **weiter**.
4. Wählen Sie auf der Seite Zielserver auswählen die Option **einen Server aus dem Server Pool auswählen** aus .
5. Wählen Sie unter Server Pool den lokalen Computer aus, und klicken Sie auf **weiter**.
6. Wählen Sie auf der Seite Server Rollen auswählen unter **Rollen** die Option **Remote Zugriff** aus, und klicken Sie dann auf **weiter**.
7. Wählen Sie auf der Seite Features auswählen die Option **weiter** aus.
8. Wählen Sie auf der Seite Remote Zugriff die Option **weiter** aus.
9. Wählen Sie auf der Seite Rollen Dienst auswählen unter **Rollen Dienst** die Option **DirectAccess und VPN (RAS)** aus.

Das Dialogfeld **Assistent zum Hinzufügen von Rollen und Features** wird geöffnet.

11. Klicken Sie im Dialogfeld Rollen und Features hinzufügen auf **Features hinzufügen**, und klicken Sie dann auf **weiter**.
12. Wählen Sie auf der Seite Webserver Rolle (IIS) die Option **weiter** aus.
13. Wählen Sie auf der Seite Rollen Dienste auswählen die Option **weiter** aus.
14. Überprüfen Sie auf der Seite Installations Auswahl bestätigen Ihre Auswahl, und wählen Sie dann **Installieren** aus.
15. Wenn die Installation abgeschlossen ist, wählen Sie **Schließen** aus.

## Konfigurieren des Remote Zugriffs als VPN-Server

In diesem Abschnitt können Sie das RAS-VPN so konfigurieren, dass es IKEv2-VPN-Verbindungen zulässt, Verbindungen von anderen VPN-Protokollen ablehnen und einen statischen IP-Adresspool für die Ausstellung

von IP-Adressen für die Verbindung mit autorisierten VPN-Clients zuweisen.

1. Wählen Sie auf dem VPN-Server in Server-Manager das **Benachrichtigungs** Kennzeichen aus.
2. Wählen Sie im Menü **Aufgaben** die Option **Assistenten für die ersten Schritte öffnen** aus.

Der Assistent zum Konfigurieren des Remote Zugriffs wird geöffnet.

**NOTE**

Der Assistent zum Konfigurieren des Remote Zugriffs kann hinter Server-Manager geöffnet werden. Wenn Sie der Ansicht sind, dass es zu lange dauert, bis der Assistent geöffnet ist, verschieben oder minimieren Sie Server-Manager, um herauszufinden, ob der Assistent dahinter liegt. Falls nicht, warten Sie, bis der Assistent initialisiert wurde.

3. Wählen Sie **nur VPNbereitstellen** aus.

Der Routing-und RAS-Microsoft Management Console (MMC) wird geöffnet.

4. Klicken Sie mit der rechten Maustaste auf den VPN-Server, und wählen Sie dann **Konfigurieren und Remote Zugriff aktivieren** aus.

Der Setup-Assistent für den Routing-und RAS-Server wird geöffnet.

5. Wählen Sie in der Willkommenseite des Setup-Assistenten für den Routing-und RAS-Server die Option **weiteraus**.

6. Wählen Sie unter **Konfiguration** die Option **benutzerdefinierte Konfiguration** aus, und klicken Sie dann auf **weiter**.

7. Wählen Sie unter **benutzerdefinierte Konfiguration** die Option **VPN-Zugriff**, und klicken Sie dann auf **weiter**.

Der Assistent zum Abschließen des Routing-und RAS-Servers wird geöffnet.

8. Wählen Sie **Fertig stellen** aus, um den Assistenten zu schließen, und klicken Sie dann auf **OK**, um das Dialogfeld Routing und RAS zu schließen

9. Wählen Sie **Dienst starten**, um den Remote Zugriff zu starten.

10. Klicken Sie in der Remote Zugriffs-MMC mit der rechten Maustaste auf den VPN-Server, und wählen Sie **Eigenschaften** aus.

11. Wählen Sie unter "Eigenschaften" die Registerkarte "**Sicherheit**" aus, und

- a. Wählen Sie **Authentifizierungs Anbieter** und dann **RADIUS-Authentifizierung** aus.

- b. Wählen Sie **Konfigurieren** aus.

Das Dialogfeld RADIUS-Authentifizierung wird geöffnet.

- c. Wählen Sie **Hinzufügen**.

Das Dialogfeld RADIUS-Server hinzufügen wird geöffnet.

- d. Geben Sie unter **Server Nameden** voll qualifizierten Domänen Namen (Fully Qualified Domain Name, FQDN) des NPS-Servers in Ihrer Organisation/Ihrem Unternehmensnetzwerk ein.

Wenn der NetBIOS-Name des NPS-Servers beispielsweise NPS1 lautet und Ihr Domänen Name Corp.contoso.com lautet, geben Sie **NPS1.Corp.contoso.com** ein.

- e. Wählen Sie unter **gemeinsamer geheimer Schlüssel** die Option **ändern** aus.

Das Dialogfeld Geheimnis ändern wird geöffnet.

f. Geben Sie unter **neues Geheimnis** eine Text Zeichenfolge ein.

g. Geben Sie in **neues Geheimnis bestätigen** die gleiche Text Zeichenfolge ein, und klicken Sie dann auf **OK**.

**IMPORTANT**

Speichern Sie diese Text Zeichenfolge. Wenn Sie den NPS-Server in Ihrer Organisation/Ihrem Unternehmensnetzwerk konfigurieren, fügen Sie diesen VPN-Server als RADIUS-Client hinzu. Während dieser Konfiguration verwenden Sie den gleichen gemeinsamen geheimen Schlüssel, damit die NPS-und VPN-Server kommunizieren können.

12. Überprüfen Sie in **RADIUS-Server hinzufügen** die Standardeinstellungen für:

- **Timeout**
- **Anfängliche Bewertung**
- **Port**

13. Ändern Sie ggf. die Werte entsprechend den Anforderungen für Ihre Umgebung, und wählen Sie **OK** aus.

Ein NAS ist ein Gerät, das ein gewisses Maß an Zugriff auf ein größeres Netzwerk bietet. Ein NAS, das eine RADIUS-Infrastruktur verwendet, ist auch ein RADIUS-Client, der Verbindungsanforderungen und Buchhaltungs Nachrichten an einen RADIUS-Server zur Authentifizierung, Autorisierung und Kontoführung sendet.

14. Überprüfen Sie die Einstellung für den **Kontoführungs Anbieter**:

WENN SIE MÖCHTEN...	DANN ...
Remote Zugriffs Aktivität auf dem RAS-Server protokolliert	Stellen Sie sicher, dass Windows-Konto <b>Führung</b> ausgewählt ist.
NPS zum Durchführen von Buchhaltungs Diensten für VPN	Ändern Sie den Konto <b>Buchhaltungs Anbieter</b> in die RADIUS-Konto <b>Führung</b> , und konfigurieren Sie dann den NPS als Buchhaltungs Anbieter.

15. Wählen Sie die Registerkarte **IPv4** aus.

a. Wählen Sie **statischer Adresspool** aus.

b. Wählen Sie **Hinzufügen**, um einen IP-Adresspool zu konfigurieren.

Der statische Adresspool sollte Adressen aus dem internen Umkreis Netzwerk enthalten. Diese Adressen sind über die interne Netzwerkverbindung auf dem VPN-Server, nicht über das Unternehmensnetzwerk.

c. Geben Sie in **Start-IP-Adresse** die IP-Startadresse in dem Bereich ein, der den VPN-Clients zugewiesen werden soll.

d. Geben Sie unter **End-IP-Adresse** die IP-Endadresse in dem Bereich ein, der den VPN-Clients zugewiesen werden soll, oder geben Sie die **Nummer der Adresse** ein, die Sie zur Verfügung stellen möchten. Wenn Sie DHCP für dieses Subnetz verwenden, stellen Sie sicher, dass Sie einen entsprechenden Adress Ausschluss auf Ihren DHCP-Servern konfigurieren.

e. Optionale Wenn Sie DHCP verwenden, wählen Sie **Adapter** aus, und wählen Sie in der Ergebnisliste den Ethernet-Adapter aus, der mit Ihrem internen Umkreis Netzwerk verbunden ist.

16. Optionale Wenn Sie den bedingten Zugriff für VPN-Konnektivität konfigurieren, wählen Sie in der Dropdown Liste **Zertifikat** unter **SSL-Zertifikat Bindung** die VPN-Server Authentifizierung aus.
17. Optionale Wenn Sie den bedingten Zugriff für VPN-Konnektivität konfigurieren, erweitern Sie in der NPS-MMC Richtlinien\Netzwerk Richtlinien , und gehen Sie wie folgt vor:
  - a. Rechts: die **Verbindungen mit der Netzwerk Richtlinie für den Routing-und RAS-Server von Microsoft** und wählen **Eigenschaften** aus.
  - b. Wählen Sie den **Zugriff gewähren aus**. Gewähren Sie Zugriff, wenn die **Verbindungsanforderung mit dieser Richtlinien Option übereinstimmt**.
  - c. Wählen Sie unter Typ des Netzwerk Zugriffs Servers in der Dropdown-Datei den Eintrag **RAS- Server (VPN-Dial-up)** aus.
18. Klicken Sie in der MMC für Routing und RAS mit der rechten Maustaste auf **Ports**, und wählen Sie dann **Eigenschaften** aus.

Das Dialogfeld Eigenschaften von Ports wird geöffnet.
19. Wählen Sie **WAN Miniport (SSTP)** aus, und wählen Sie **Konfigurieren** aus. Das Dialogfeld Device-WAN-Miniport konfigurieren (SSTP) wird geöffnet.
  - a. Deaktivieren Sie die Kontrollkästchen **RAS- Verbindungen (nur eingehend)** und **Routing Verbindungen nach Bedarf (eingehend und ausgehend)** .
  - b. Wählen Sie **OK**.
20. Wählen Sie **WAN Miniport (L2TP)** , und wählen Sie **Konfigurieren** aus. Das Dialogfeld Device-WAN-Miniport konfigurieren (L2TP) wird geöffnet.
  - a. Geben Sie unter Maximale Anzahl von **Ports** die Anzahl der Ports ein, die der maximalen Anzahl gleichzeitiger VPN-Verbindungen entsprechen soll, die Sie unterstützen möchten.
  - b. Wählen Sie **OK**.
21. Wählen Sie **WAN Miniport (PPTP)** aus, und wählen Sie **Konfigurieren** aus. Das Dialogfeld Device-WAN-Miniport konfigurieren (PPTP) wird geöffnet.
  - a. Geben Sie unter Maximale Anzahl von **Ports** die Anzahl der Ports ein, die der maximalen Anzahl gleichzeitiger VPN-Verbindungen entsprechen soll, die Sie unterstützen möchten.
  - b. Wählen Sie **OK**.
22. Wählen Sie **WAN Miniport (IKEv2)** , und wählen Sie **Konfigurieren** aus. Das Dialogfeld Device-WAN-Miniport konfigurieren (IKEv2) wird geöffnet.
  - a. Geben Sie unter Maximale Anzahl von **Ports** die Anzahl der Ports ein, die der maximalen Anzahl gleichzeitiger VPN-Verbindungen entsprechen soll, die Sie unterstützen möchten.
  - b. Wählen Sie **OK**.
23. Wenn Sie dazu aufgefordert werden, wählen Sie **Ja** aus, um den Server neu zu starten, und wählen Sie **Schließen** aus, um den Server

## Nächster Schritt

[Schritt 4: Installieren und Konfigurieren des Netzwerk Richtlinien Servers \(NPS\)](#): in diesem Schritt installieren Sie den Netzwerk Richtlinien Server (Network Policy Server, NPS) mithilfe von Windows PowerShell oder des Server-Manager Assistenten zum Hinzufügen von Rollen und Features. Außerdem können Sie NPS so konfigurieren, dass

alle Authentifizierungs-, Autorisierungs- und Buchhaltungsaufgaben für Verbindungsanforderungen verarbeitet werden, die vom VPN-Server empfangen werden.

# Schritt 4 Installieren und Konfigurieren des Netzwerk Richtlinien Servers (NPS)

09.04.2020 • 16 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2019, Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Weiter: Schritt 3. Konfigurieren des Remote Zugriffs Servers für die Always on-VPN](#)
- [Weiter: Schritt 5: Konfigurieren von DNS- und Firewalleinstellungen](#)

In diesem Schritt installieren Sie den Netzwerk Richtlinien Server (Network Policy Server, NPS) für die Verarbeitung von Verbindungsanforderungen, die vom VPN-Server gesendet werden:

- Führen Sie eine Autorisierung aus, um zu überprüfen, ob der Benutzer über die Berechtigung
- Authentifizierung wird durchgeführt, um die Identität des Benutzers zu überprüfen.
- Durchführen der Buchhaltung zum Protokollieren der Aspekte der Verbindungsanforderung, die Sie beim Konfigurieren der RADIUS-Kontoführung in NPS ausgewählt haben.

Mit den Schritten in diesem Abschnitt können Sie die folgenden Elemente ausführen:

1. Auf dem Computer oder virtuellen Computer, der für den NPS-Server geplant und in Ihrer Organisation oder im Unternehmensnetzwerk installiert ist, können Sie NPS installieren.

## TIP

Wenn Sie bereits über einen oder mehrere NPS-Server in Ihrem Netzwerk verfügen, müssen Sie die NPS-Server Installation nicht ausführen. stattdessen können Sie dieses Thema verwenden, um die Konfiguration eines vorhandenen NPS-Servers zu aktualisieren.

## NOTE

Der Netzwerk Richtlinien Server-Dienst kann nicht unter Windows Server Core installiert werden.

2. Auf dem NPS-Server "Organization/Corporate" können Sie NPS so konfigurieren, dass er als RADIUS-Server verwendet wird, der die vom VPN-Server empfangenen Verbindungsanforderungen verarbeitet.

## Installieren des Netzwerkrichtlinienservers

In diesem Verfahren installieren Sie NPS mithilfe von Windows PowerShell oder dem Server-Manager Assistenten zum Hinzufügen von Rollen und Features. NPS ist ein Rollendienst der Serverrolle Netzwerkrichtlinien- und Zugriffsdienste.

## TIP

Standardmäßig überwacht NPS RADIUS-Datenverkehr auf den Ports 1812, 1813, 1645 und 1646 für alle installierten Netzwerkadapter. Wenn Sie NPS installieren und die Windows-Firewall mit erweiterter Sicherheit aktivieren, werden Firewallausnahmen für diese Ports automatisch sowohl für IPv4-als auch für IPv6-Datenverkehr erstellt. Wenn Ihre Netzwerk Zugriffs Server für das Senden von RADIUS-Datenverkehr über andere Ports als diese Standardeinstellungen konfiguriert sind, entfernen Sie die Ausnahmen, die bei der NPS-Installation unter Windows-Firewall mit erweiterter Sicherheit erstellt wurden, und erstellen Sie Ausnahmen für die Ports, die Sie für RADIUS-Datenverkehr.

### Vorgehensweise für Windows PowerShell:

Wenn Sie dieses Verfahren mithilfe von Windows PowerShell ausführen möchten, führen Sie Windows PowerShell als Administrator aus, und geben Sie das folgende Cmdlet ein:

```
Install-WindowsFeature NPAS -IncludeManagementTools
```

### Prozedur für Server-Manager:

1. Klicken Sie in Server-Manager auf **Verwalten**, und wählen Sie dann **Rollen und Features hinzufügen** aus. Der Assistent zum Hinzufügen von Rollen und Features wird geöffnet.
2. Wählen Sie unter Vorbereitung die Option **weiter** aus.

#### NOTE

Die Seite **Vorbemerkungen** des Assistenten zum Hinzufügen von Rollen und Features wird nicht angezeigt, wenn Sie zuvor die Option **Diese Seite beim Ausführen des Assistenten zum Hinzufügen von Rollen und Features standardmäßig überspringen** ausgewählt haben.

3. Vergewissern Sie sich, dass unter Installationstyp auswählen die Option **rollenbasierte oder featurebasierte Installation** ausgewählt ist, und klicken Sie auf **weiter**.
4. Stellen Sie sicher, dass unter Zielserver auswählen die Option **einen Server aus dem Server Pool auswählen** ausgewählt ist.
5. Stellen Sie sicher, dass unter Server Pool die Option Lokaler Computer ausgewählt ist, und klicken Sie auf **weiter**.
6. Wählen Sie unter Server Rollen auswählen unter **Rollen** die Option **Netzwerk Richtlinien-und Zugriffs Dienste** aus. Es wird ein Dialogfeld mit der Frage angezeigt, ob für Netzwerk Richtlinien-und Zugriffs Dienste erforderliche Features hinzugefügt werden sollen.
7. Wählen Sie **Features hinzufügen** und dann **weiter** aus.
8. Wählen Sie unter Features auswählen die Option **weiter** aus, und überprüfen Sie unter Netzwerk Richtlinien-und Zugriffs Dienste die angegebenen Informationen, und klicken Sie dann auf **weiter**.
9. Wählen Sie unter Rollen Dienste auswählen die Option **Netzwerk Richtlinien Server** aus.
10. Klicken Sie für die für den Netzwerk Richtlinien Server erforderlichen Features auf **Features hinzufügen**, und wählen Sie **weiter** aus.
11. Wählen Sie unter Installations Auswahl bestätigen die Option **Zielserver bei Bedarf automatisch neu starten** aus.
12. Wählen Sie **Ja** aus, um die Auswahl zu bestätigen, und wählen Sie dann **Installieren** aus.

Auf der Seite Installationsfortschritt wird der Status während des Installationsvorgangs angezeigt. Wenn der Vorgang abgeschlossen ist, wird die Meldung "Installation erfolgreich auf *Computername*" angezeigt, wobei *Computername* der Name des Computers ist, auf dem Sie den Netzwerk Richtlinien Server installiert haben.

13. Wählen Sie Schließen aus.

## Konfigurieren von NPS

Nach der Installation von NPS konfigurieren Sie NPS so, dass alle Authentifizierungs-, Autorisierungs- und Buchhaltungsaufgaben für die Verbindungsanforderung, die Sie vom VPN-Server empfängt, verarbeitet werden.

### Registrieren des NPS-Servers in Active Directory

In diesem Verfahren registrieren Sie den Server in Active Directory, damit er beim Verarbeiten von Verbindungsanforderungen über die Berechtigung zum Zugreifen auf Benutzerkontoinformationen verfügt.

#### Dringlichkeit

1. Klicken Sie in Server-Manager auf Extras, und wählen Sie dann Netzwerk Richtlinien Server aus. Die NPS-Konsole wird geöffnet.
2. Klicken Sie in der NPS-Konsole mit der rechten Maustaste auf NPS (lokal), und wählen Sie dann Server in Active Directory registrieren aus.  
Das Dialogfeld Netzwerkrichtlinienserver wird geöffnet.
3. Klicken Sie im Dialogfeld Netzwerk Richtlinien Server zweimal auf OK .

Alternative Methoden zum Registrieren von NPS finden Sie unter [Registrieren eines NPS-Servers in einem Active Directory-Domäne](#).

### Konfigurieren der Kontoführung für den Netzwerkrichtlinienserver

In diesem Verfahren konfigurieren Sie die Netzwerk Richtlinien Server-Kontoführung mithilfe eines der folgenden Protokollierungstypen:

- **Ereignisprotokollierung.** Wird hauptsächlich für die Überwachung und Problembehandlung von Verbindungsversuchen verwendet. Sie können die NPS-Ereignisprotokollierung konfigurieren, indem Sie die NPS-Server Eigenschaften in der NPS-Konsole abrufen.
- **Protokollieren von Benutzeroauthentifizierung und Buchhaltungs Anforderungen in einer lokalen Datei.** Wird hauptsächlich für Verbindungs Analyse und Abrechnungszwecke verwendet. Wird auch als Sicherheitsuntersuchung verwendet, da Sie eine Methode zum Nachverfolgen der Aktivität eines böswilligen Benutzers nach einem Angriff bereitstellen. Sie können die lokale Datei Protokollierung mit dem Konfigurations-Assistenten für die Buchhaltung konfigurieren.
- **Protokollieren von Benutzer Authentifizierungs- und Buchhaltungs Anforderungen in einer Microsoft SQL Server XML-kompatiblen Datenbank.** Wird verwendet, um mehreren Servern, auf denen NPS ausgeführt wird, eine Datenquelle zu ermöglichen. Bietet außerdem die Vorteile der Verwendung einer relationalen Datenbank. Sie können SQL Server Protokollierung mit dem Konfigurations-Assistenten für die Buchhaltung konfigurieren.

Informationen zum Konfigurieren der Erfassung von Netzwerk Richtlinien Servern finden Sie unter [Konfigurieren der Netzwerk Richtlinien Server-Kontoführung](#)

### Hinzufügen des VPN-Servers als RADIUS-Client

Im Abschnitt [configure the Remote Access Server for Always on VPN](#) haben Sie den VPN-Server installiert und konfiguriert. Während der VPN-Serverkonfiguration haben Sie auf dem VPN-Server einen gemeinsamen RADIUS-Schlüssel hinzugefügt.

In diesem Verfahren verwenden Sie die gleiche gemeinsame geheime Text Zeichenfolge, um den VPN-Server als RADIUS-Client in NPS zu konfigurieren. Verwenden Sie dieselbe Text Zeichenfolge, die Sie auf dem VPN-Server verwendet haben, oder die Kommunikation zwischen dem NPS-Server und dem VPN-Server schlägt fehl

#### **IMPORTANT**

Wenn Sie einen neuen Netzwerk Zugriffs Server (VPN-Server, drahtlosen Zugriffspunkt, authentifizier enden Switch oder DFÜ-Server) in Ihrem Netzwerk hinzufügen, müssen Sie den Server als RADIUS-Client in NPS hinzufügen, damit NPS die Verbindung mit dem Netzwerk Zugriffs Server kennt und mit ihm kommunizieren kann.

#### **Dringlichkeit**

1. Doppelklicken Sie auf dem NPS-Server in der NPS-Konsole auf **RADIUS-Clients und -Server**.
2. Klicken Sie mit der rechten Maustaste auf **RADIUS-Clients** und wählen Sie **neu**. Das Dialogfeld Neuer RADIUS-Client wird geöffnet.
3. Vergewissern Sie sich, dass das Kontrollkästchen **diesen RADIUS-Client aktivieren** aktiviert ist.
4. Geben Sie unter Anzeige **Name** einen Namen für den VPN-Server ein.
5. Geben Sie unter **Adresse (IP oder DNS)** die NAS-IP-Adresse oder den voll qualifizierten Namen ein.  
Wenn Sie den FQDN eingeben, wählen Sie **überprüfen** aus, um zu überprüfen, ob der Name richtig ist und einer gültigen IP-Adresse zugeordnet ist.
6. Unter **gemeinsamer geheimer Schlüssel**:
  - a. Stellen Sie sicher, dass **manuell** ausgewählt ist.
  - b. Geben Sie die starke Text Zeichenfolge ein, die auch auf dem VPN-Server eingegeben wurde.
  - c. Geben Sie den gemeinsamen geheimen Schlüssel in **Confirm Shared Secret** wieder ein.
7. Wählen Sie **OK**. Der VPN-Server wird in der Liste der auf dem NPS-Server konfigurierten RADIUS-Clients angezeigt.

## Konfigurieren von NPS als RADIUS für VPN-Verbindungen

In diesem Verfahren konfigurieren Sie NPS als RADIUS-Server in Ihrem Organisations Netzwerk. Auf dem NPS müssen Sie eine Richtlinie definieren, die nur Benutzern in einer bestimmten Gruppe den Zugriff auf die Organisation/das Unternehmensnetzwerk über den VPN-Server ermöglicht. Dies gilt nur, wenn Sie ein gültiges Benutzerzertifikat in einer Anforderung für die Peer-Authentifizierung verwenden.

#### **Dringlichkeit**

1. Stellen Sie in der NPS-Konsole unter Standard Konfiguration sicher, dass **RADIUS-Server für DFÜ-oder VPN-Verbindungen** ausgewählt ist.
2. Wählen Sie **VPN oder Einwahl konfigurieren** aus.  
Der Assistent zum Konfigurieren von VPN oder DFÜ wird geöffnet.
3. Wählen Sie **VPN-Verbindungen (virtuelles privates Netzwerk)** aus, und klicken Sie auf **weiter**.
4. Wählen Sie unter DFÜ-oder VPN-Server angeben in RADIUS-Clients den Namen des VPN-Servers aus, den Sie im vorherigen Schritt hinzugefügt haben. Wenn der NetBIOS-Name des VPN-Servers beispielsweise RAS1 lautet, wählen Sie **RAS1** aus.

5. Klicken Sie auf **Weiter**.
6. Führen Sie unter Konfigurieren von Authentifizierungsmethoden die folgenden Schritte aus:
  - a. Deaktivieren Sie das Kontrollkästchen **Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAPv2)**.
  - b. Aktivieren Sie das Kontrollkästchen **Extensible Authentication-Protokoll**, um es auszuwählen.
  - c. Wählen Sie in Typ (basierend auf der Zugriffs- und Netzwerkkonfiguration) die Option **Microsoft: geschütztes EAP (PEAP)**, und klicken Sie dann auf **Konfigurieren**.

Das Dialogfeld geschützte EAP-Eigenschaften bearbeiten wird geöffnet.
  - d. Wählen Sie **Entfernen** aus, um den EAP-Typ des gesicherten Kennworts (EAP-MSCHAP v2) zu entfernen.
  - e. Wählen Sie **Hinzufügen**. Das Dialogfeld EAP hinzufügen wird geöffnet.
  - f. Wählen Sie **Smartcard oder anderes Zertifikataus**, und klicken Sie dann auf **OK**.
  - g. Wählen Sie **OK** aus, um geschützte EAP-Eigenschaften bearbeiten zu schließen.
7. Klicken Sie auf **Weiter**.

8. Führen Sie unter Benutzergruppen angeben die folgenden Schritte aus:
  - a. Wählen Sie **Hinzufügen**. Das Dialogfeld Benutzer, Computer, Dienstkonten oder Gruppen auswählen wird geöffnet.
  - b. Geben Sie **VPN-Benutzerein**, und wählen Sie dann **OK**
  - c. Klicken Sie auf **Weiter**.
9. Wählen Sie unter IP-Filter angeben die Option **weiteraus**.
10. Wählen Sie unter Verschlüsselungseinstellungen angeben die Option **weiteraus**. Nehmen Sie keine Änderungen vor.

Diese Einstellungen gelten nur für MPPE-Verbindungen (Point-to-Point Encryption) von Microsoft, die in diesem Szenario nicht unterstützt werden.
11. Wählen Sie unter Bereichs Namen angeben die Option **weiteraus**.
12. Wählen Sie **Fertig stellen** aus, um den Assistenten zu schließen.

## Automatische Registrierung des NPS-Server Zertifikats

In diesem Verfahren aktualisieren Sie Gruppenrichtlinie auf dem lokalen NPS-Server manuell. Wenn die automatische Registrierung von Zertifikaten konfiguriert ist und ordnungsgemäß funktioniert, wird der lokale Computer von der Zertifizierungsstelle automatisch registriert, wenn Gruppenrichtlinie aktualisiert wird.

### NOTE

Gruppenrichtlinie automatisch aktualisiert, wenn Sie den Domänen Mitglieds Computer neu starten oder wenn sich ein Benutzer an einem Domänen Mitglieds Computer anmeldet. Außerdem Gruppenrichtlinie in regelmäßigen Abständen aktualisiert. Standardmäßig erfolgt diese regelmäßige Aktualisierung alle 90 Minuten mit einem zufälligen Offset von bis zu 30 Minuten.

Sie müssen mindestens Mitglied der Gruppe **Administratoren** oder einer entsprechenden Gruppe sein, damit Sie dieses Verfahren durchführen können.

## Dringlichkeit

1. Öffnen Sie Windows PowerShell auf dem NPS.
2. Geben Sie an der Windows PowerShell-Eingabeaufforderung **gpupdate** ein, und drücken Sie dann die EINGABETASTE.

## Nächste Schritte

[Schritt 5: Konfigurieren von DNS-und Firewalleinstellungen für Always on-VPN](#): in diesem Schritt installieren Sie den Netzwerk Richtlinien Server (Network Policy Server, NPS) mithilfe von Windows PowerShell oder dem Assistenten zum Hinzufügen von Rollen und Features Server-Manager. Außerdem können Sie NPS so konfigurieren, dass alle Authentifizierungs-, Autorisierungs- und Buchhaltungsaufgaben für Verbindungsanforderungen verarbeitet werden, die vom VPN-Server empfangen werden.

# Schritt 5 Konfigurieren von DNS-und Firewalleinstellungen

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 4: Installieren und Konfigurieren des NPS-Servers](#)
- [Weiter: Schritt 6: Konfigurieren von Windows 10-Client Always on-VPN-Verbindungen](#)

In diesem Schritt konfigurieren Sie DNS- und Firewalleinstellungen für VPN-Konnektivität.

## Konfigurieren der DNS-Namensauflösung

Wenn Remote-VPN-Clients eine Verbindung herstellen, verwenden Sie die gleichen DNS-Server, die von den internen Clients verwendet werden. Auf diese Weise können Namen auf die gleiche Weise wie die übrigen internen Arbeitsstationen aufgelöst werden.

Aus diesem Grund müssen Sie sicherstellen, dass der Computername, den externe Clients zum Herstellen einer Verbindung mit dem VPN-Server verwenden, dem alternativen Antragsteller Namen entspricht, der in den für den VPN-Server ausgestellten Zertifikaten definiert ist.

Um sicherzustellen, dass Remote Clients eine Verbindung mit dem VPN-Server herstellen können, können Sie einen DNS A-Datensatz (Host) in der externen DNS-Zone erstellen. Der A-Datensatz sollte den alternativen Antragsteller Namen des Zertifikats für den VPN-Server verwenden.

### So fügen Sie einer Zone einen Host Ressourcen Daten Satz (A oder AAAA) hinzu

1. Wählen Sie auf einem DNS-Server in Server-Manager Extras aus, und **Wählen Sie dann DNS** aus. Der DNS-Manager wird geöffnet.
2. Wählen Sie in der Konsolen Struktur des DNS-Managers den Server aus, den Sie verwalten möchten.
3. Doppelklicken Sie im Detailbereich unter **Name** auf Forward-Lookupzonen, um die Ansicht zu erweitern.
4. Klicken Sie in Details der **Forward-Lookupzonen** mit der rechten Maustaste auf die Forward-Lookupzone, der Sie einen Datensatz hinzufügen möchten, und wählen Sie dann **neuer Host (A oder AAAA)** aus. Das Dialogfeld **neuer Host** wird geöffnet.
5. Geben Sie im Feld **neuer Host** unter **Name** den alternativen Antragsteller Namen des Zertifikats für den VPN-Server ein.
6. Geben Sie unter **IP-Adresse** die IP-Adresse für den VPN-Server ein. Sie können die Adresse im IPv4-Format (IP Version 4) eingeben, um einen Host-(A) Ressourcen Daten Satz oder ein IPv6-Format (IP Version 6) zum Hinzufügen eines Host Ressourceneinsatzes (AAAA) hinzuzufügen.
7. Wenn Sie für einen Bereich von IP-Adressen eine Reverse-Lookupzone erstellt haben, einschließlich der eingegebenen IP-Adresse, aktivieren Sie das Kontrollkästchen **zugeordneten Zeiger erstellen (PTR-Datensatz)**. Wenn Sie diese Option auswählen, wird ein zusätzlicher Zeiger (PTR)-Ressourcen Daten Satz in einer umgekehrten Zone für diesen Host erstellt, basierend auf den Informationen, die Sie unter **Name** und **IP-Adresse** eingegeben haben.
8. Wählen Sie **Host hinzufügen** aus.

## Konfigurieren der Edge-Firewall

Die Edge-Firewall trennt das externe Umkreis Netzwerk vom öffentlichen Internet. Eine visuelle Darstellung dieser Trennung finden Sie in der Abbildung im Thema [Always on VPN-Technologie Übersicht](#).

Ihre Edge-Firewall muss bestimmte Ports an Ihren VPN-Server zulassen und weiterleiten. Wenn Sie die Netzwerk Adressübersetzung (Network Address Translation, NAT) in ihrer Edge-Firewall verwenden, müssen Sie möglicherweise die Port Weiterleitung für UDP (User Datagram Protocol)-Ports 500 und 4500 aktivieren. Leiten Sie diese Ports an die IP-Adresse weiter, die der externen Schnittstelle des VPN-Servers zugewiesen ist.

Wenn Sie eingehenden Datenverkehr weiterleiten und NAT auf dem VPN-Server ausführen, müssen Sie die Firewallregeln öffnen, damit die UDP-Ports 500 und 4500 in der externen IP-Adresse eingehenden können, die auf die öffentliche Schnittstelle auf dem VPN-Server angewendet wird.

Wenn Ihre Firewall eine umfassende Paket Untersuchung unterstützt und Probleme beim Einrichten von Clientverbindungen auftreten, sollten Sie versuchen, die umfassende Paketüberprüfung für IKE-Sitzungen zu lockern oder zu deaktivieren.

Informationen dazu, wie Sie diese Konfigurationsänderungen vornehmen, finden Sie in der Firewalldokumentation.

## Konfigurieren der Firewall für das interne Umkreis Netzwerk

Die interne Umkreis Netzwerk Firewall trennt die Organisation/das Unternehmensnetzwerk vom internen Umkreis Netzwerk. Eine visuelle Darstellung dieser Trennung finden Sie in der Abbildung im Thema [Always on VPN-Technologie Übersicht](#).

In dieser Bereitstellung wird der RAS-VPN-Server im Umkreis Netzwerk als RADIUS-Client konfiguriert. Der VPN-Server sendet RADIUS-Datenverkehr an den NPS im Unternehmensnetzwerk und empfängt RADIUS-Datenverkehr aus dem NPS.

Konfigurieren Sie die Firewall so, dass RADIUS-Datenverkehr in beide Richtungen fließen kann.

### NOTE

Der NPS-Server im Organisations-/Unternehmensnetzwerk fungiert als RADIUS-Server für den VPN-Server, bei dem es sich um einen RADIUS-Client handelt. Weitere Informationen zur RADIUS-Infrastruktur finden Sie unter [Netzwerk Richtlinien Server \(Network Policy Server, NPS\)](#).

### RADIUS-datenverkehrsports auf dem VPN-Server und dem NPS-Server

Standardmäßig lauschen NPS und VPN auf den Ports 1812, 1813, 1645 und 1646 auf den RADIUS-Datenverkehr auf allen installierten Netzwerkadaptersn. Wenn Sie die Windows-Firewall mit erweiterter Sicherheit bei der Installation von NPS aktivieren, werden Firewallausnahmen für diese Ports während des Installationsvorgangs für IPv6-und IPv4-Datenverkehr automatisch erstellt.

### IMPORTANT

Wenn Ihre Netzwerk Zugriffs Server für das Senden von RADIUS-Datenverkehr über andere Ports als diese Standardeinstellungen konfiguriert sind, entfernen Sie die Ausnahmen, die bei der NPS-Installation unter Windows-Firewall mit erweiterter Sicherheit erstellt wurden, und erstellen Sie Ausnahmen für die Ports, die Sie für RADIUS-Datenverkehr.

### Verwenden Sie die gleichen RADIUS-Ports für die Firewallkonfiguration des internen Umkreis Netzwerks.

Wenn Sie die Standardkonfiguration des RADIUS-Ports auf dem VPN-Server und dem NPS-Server verwenden, stellen Sie sicher, dass Sie die folgenden Ports in der internen Umkreis Netzwerk Firewall öffnen:

- Ports UDP1812, UDP1813, UDP1645 und UDP1646

Wenn Sie nicht die Standardradius-Ports in der NPS-Bereitstellung verwenden, müssen Sie die Firewall so konfigurieren, dass RADIUS-Datenverkehr für die von Ihnen verwendeten Ports zugelassen wird. Weitere Informationen finden Sie unter [Konfigurieren von Firewalls für RADIUS-Datenverkehr](#).

## Nächste Schritte

**Schritt 6: Konfigurieren von Windows 10-Client-Always on-VPN-Verbindungen:** in diesem Schritt konfigurieren Sie die Windows 10-Client Computer für die Kommunikation mit dieser Infrastruktur über eine VPN-Verbindung. Sie können verschiedene Technologien zum Konfigurieren von Windows 10-VPN-Clients verwenden, einschließlich Windows PowerShell, Microsoft Endpoint Configuration Manager und InTune. Alle drei erfordern ein XML-VPN-Profil, um die entsprechenden VPN-Einstellungen zu konfigurieren.

# Schritt 6: Konfigurieren von Always On VPN-Verbindungen für den Windows 10-Client

22.05.2020 • 48 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 5: Konfigurieren von DNS- und Firewalleinstellungen](#)
- [Weiter: Schritt 7: Optionale Bedingter Zugriff für VPN-Konnektivität mithilfe von Azure AD](#)

In diesem Schritt erfahren Sie mehr über die profileXML-Optionen und das Schema und konfigurieren die Windows 10-Client Computer für die Kommunikation mit dieser Infrastruktur über eine VPN-Verbindung.

Sie können den Always on VPN-Client über PowerShell, Microsoft Endpoint Configuration Manager oder InTune konfigurieren. Alle drei erfordern ein XML-VPN-Profil, um die entsprechenden VPN-Einstellungen zu konfigurieren. Die Automatisierung der PowerShell-Registrierung für Organisationen ohne Configuration Manager oder InTune ist möglich.

## NOTE

Gruppenrichtlinie enthält keine administrativen Vorlagen zum Konfigurieren des Windows 10-Remote Zugriffs Always on VPN-Clients. Sie können jedoch Anmelde Skripts verwenden.

## Übersicht über profileXML

ProfileXML ist ein URI-Knoten innerhalb des VPnv2-CSP. Anstatt jeden VPnv2 CSP-Knoten einzeln zu konfigurieren – beispielsweise Trigger, Routenlisten und Authentifizierungsprotokolle – verwenden Sie diesen Knoten, um einen Windows 10-VPN-Client zu konfigurieren, indem Sie alle Einstellungen als einen einzelnen XML-Block an einen einzelnen CSP-Knoten überführen. Das Schema "profileXML" gleicht das Schema der VPnv2-CSP-Knoten nahezu identisch ab, aber einige Begriffe unterscheiden sich geringfügig.

Sie verwenden profileXML in allen von dieser Bereitstellung beschriebenen Übermittlungs Methoden, einschließlich Windows PowerShell, Microsoft Endpoint Configuration Manager und InTune. Es gibt zwei Möglichkeiten, den profileXML VPnv2 CSP-Knoten in dieser Bereitstellung zu konfigurieren:

- **OMA-DM.** Eine Möglichkeit ist die Verwendung eines MDM-Anbieters mithilfe von OMA-DM, wie bereits im Abschnitt [VPnv2 CSP-Knotenerläutert](#). Mit dieser Methode können Sie das XML-Markup für die VPN-Profil Konfiguration bei Verwendung von InTune problemlos in den profileXML-CSP-Knoten einfügen.
- **Windows-Verwaltungsinstrumentation (WMI)-zu-CSP-Bridge.** Die zweite Methode zum Konfigurieren des profileXML-CSP-Knotens ist die Verwendung der WMI-zu-CSP-Bridge – eine WMI-Klasse mit dem Namen **MDM\_VPnv2\_01**–, die auf den VPnv2-CSP und den profileXML-Knoten zugreifen kann. Wenn Sie eine neue Instanz dieser WMI-Klasse erstellen, verwendet WMI den CSP, um das VPN-Profil zu erstellen, wenn Windows PowerShell und Configuration Manager verwendet werden.

Obwohl sich diese Konfigurations Methoden unterscheiden, benötigen beide ein ordnungsgemäß formatiertes XML-VPN-Profil. Um die profileXML VPnv2 CSP-Einstellung zu verwenden, erstellen Sie XML, indem Sie das profileXML-Schema verwenden, um die für das einfache Bereitstellungs Szenario erforderlichen Tags zu konfigurieren. Weitere Informationen finden Sie unter [profileXML XSD](#).

Unten finden Sie alle erforderlichen Einstellungen und das zugehörige profileXML-Tag. Sie konfigurieren jede Einstellung in einem bestimmten Tag im profileXML-Schema, und nicht alle werden im nativen Profil gefunden. Weitere tagplatzierung finden Sie unter dem profileXML-Schema.

#### IMPORTANT

Eine beliebige andere Kombination aus Groß- oder Kleinbuchstaben für "True" in der folgenden Tags führt eine partielle Konfiguration von VPN-Profil:

```
<AlwaysOn>true</AlwaysOn>
<RememberCredentials>true</RememberCredentials>
```

### Verbindungstyp: Native IKEv2

ProfileXML-Element:

```
<NativeProtocolType>IKEv2</NativeProtocolType>
```

### Routing: Tunnelung aufteilen

ProfileXML-Element:

```
<RoutingPolicyType>SplitTunnel</RoutingPolicyType>
```

### Namensauflösung: Domänen Namen-Informationsliste und DNS-Suffix

ProfileXML-Elemente:

```
<DomainNameInformation>
<DomainName>.corp.contoso.com</DomainName>
<DnsServers>10.10.1.10,10.10.1.50</DnsServers>
</DomainNameInformation>

<DnsSuffix>corp.contoso.com</DnsSuffix>
```

### Auslösen: Erkennung von Always on und vertrauenswürdigen Netzwerken

ProfileXML-Elemente:

```
<AlwaysOn>true</AlwaysOn>
<TrustedNetworkDetection>corp.contoso.com</TrustedNetworkDetection>
```

### Authentifizierung: Peer-TLS mit TPM-geschützten Benutzer Zertifikaten

ProfileXML-Elemente:

```
<Authentication>
<UserMethod>Eap</UserMethod>
<Eap>
<Configuration>...</Configuration>
</Eap>
</Authentication>
```

Sie können einfache Tags verwenden, um einige VPN-Authentifizierungsmechanismen zu konfigurieren. EAP und PEAP sind jedoch mehr beteiligt. Die einfachste Möglichkeit, das XML-Markup zu erstellen, besteht darin, einen

VPN-Client mit seinen EAP-Einstellungen zu konfigurieren und diese Konfiguration anschließend in XML zu exportieren.

Weitere Informationen zu EAP-Einstellungen finden Sie unter [EAP-Konfiguration](#).

## Manuelles Erstellen eines Vorlagen Verbindungs Profils

In diesem Schritt verwenden Sie das Protected Extensible Authentication Protocol (Peer) zum Sichern der Kommunikation zwischen dem Client und dem Server. Anders als bei einem einfachen Benutzernamen und einem Kennwort muss für diese Verbindung ein eindeutiger eapconfiguration-Abschnitt im VPN-Profil verwendet werden.

Anstatt zu beschreiben, wie das XML-Markup von Grund auf neu erstellt wird, verwenden Sie Einstellungen in Windows, um ein VPN-Vorlagen Profil zu erstellen. Nachdem Sie das Vorlagen-VPN-Profil erstellt haben, verwenden Sie Windows PowerShell, um den eapconfiguration-Teil aus dieser Vorlage zu verwenden, um die endgültige profileXML zu erstellen, die Sie später in der Bereitstellung bereitstellen.

### NPS-Zertifikat Einstellungen aufzeichnen

Notieren Sie sich vor dem Erstellen der Vorlage den Hostnamen oder den voll qualifizierten Domänen Namen (Fully Qualified Domain Name, FQDN) des NPS-Servers aus dem Zertifikat des Servers und den Namen der Zertifizierungsstelle, die das Zertifikat ausgestellt hat.

### Dringlichkeit

1. Öffnen Sie auf dem NPS-Server den Netzwerk Richtlinien Server.
2. Klicken Sie in der NPS-Konsole unter Richtlinien auf **Netzwerk Richtlinien**.
3. Klicken Sie mit der rechten Maustaste auf **VPN-Verbindungen (virtuelles privates Netzwerk)**, und klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Einschränkungen**, und klicken Sie auf **Authentifizierungsmethoden**.
5. Klicken Sie in EAP-Typen auf **Microsoft: geschütztes EAP (PEAP)**, und klicken Sie dann auf **Bearbeiten**.
6. Notieren Sie die Werte für das **Zertifikat, das für den Aussteller ausgestellt wurde**

Diese Werte werden in der bevorstehenden Konfiguration der VPN-Vorlage verwendet. Wenn z. B. der voll qualifizierte Name des Servers nps01.Corp.contoso.com und der Hostname nps01 lautet, basiert der Zertifikat Name auf dem voll qualifizierten Namen oder DNS-Namen des Servers, z. –. nps01.Corp.contoso.com.

7. Beenden Sie das Dialogfeld geschützte EAP-Eigenschaften bearbeiten.
8. Beenden Sie das Dialogfeld Eigenschaften für virtuelles privates Netzwerk (VPN).
9. Schließen Sie den Netzwerk Richtlinien Server.

#### NOTE

Wenn Sie über mehrere NPS-Server verfügen, führen Sie diese Schritte nacheinander aus, damit das VPN-Profil überprüfen kann, ob die einzelnen Server verwendet werden sollen.

### Konfigurieren des VPN-Vorlagen Profils auf einem in die Domäne eingebundenen Client Computer

Nachdem Sie nun über die erforderlichen Informationen verfügen, konfigurieren Sie das Vorlagen-VPN-Profil auf einem in die Domäne eingebundenen Client Computer. Der von Ihnen verwendete Benutzer Kontotyp (d. h. Standardbenutzer oder Administrator) ist für diesen Teil des Prozesses nicht von Bedeutung.

Wenn Sie den Computer jedoch seit dem Konfigurieren der automatischen Zertifikat Registrierung nicht neu gestartet haben, sollten Sie dies vor dem Konfigurieren der VPN-Vorlagen Verbindung tun, um sicherzustellen, dass ein verwendbares Zertifikat für das Zertifikat registriert ist.

**NOTE**

Es gibt keine Möglichkeit, erweiterte Eigenschaften von VPN manuell hinzuzufügen, z. b. NRPT-Regeln, Always on, Erkennung vertrauenswürdiger Netzwerke usw. Im nächsten Schritt erstellen Sie eine VPN-Testverbindung, um die Konfiguration des VPN-Servers zu überprüfen und eine VPN-Verbindung mit dem Server herzustellen.

### Manuelles Erstellen einer einzelnen Test-VPN-Verbindung

1. Melden Sie sich bei einem in die Domäne eingebundenen Client Computer als Mitglied der Gruppe "**VPN-Benutzer**" an.
2. Geben Sie im Startmenü **VPN** ein, und drücken Sie die EINGABETASTE.
3. Klicken Sie im Detailbereich auf **VPN-Verbindung hinzufügen**.
4. Klicken Sie in der Liste VPN-Anbieter auf **Windows (integriert)**.
5. Geben Sie unter Verbindungs Name die Bezeichnung **Vorlage** ein.
6. Geben Sie unter Server Name oder Adresse den **externen** voll qualifizierten Namen des VPN-Servers ein (z. b. **VPN.contoso.com**).
7. Klicken Sie auf **Speichern**.
8. Klicken Sie unter Verwandte Einstellungen auf **Adapter Optionen ändern**.
9. Klicken Sie mit der rechten Maustaste auf **Vorlage**, und klicken Sie auf **Eigenschaften**
10. Klicken Sie auf der Registerkarte **Sicherheit** unter **Typ des VPN** auf **IKEv2**.
11. Klicken Sie unter Datenverschlüsselung auf **Verschlüsselung der maximalen Stärke**.
12. Klicken Sie auf **Extensible Authentication Protocol (EAP) verwenden**. Klicken Sie dann unter **Extensible Authentication Protocol (EAP) verwenden** auf Microsoft: **geschütztes EAP (PEAP) (Verschlüsselung aktiviert)**.
13. Klicken Sie auf **Eigenschaften**, um das Dialogfeld Eigenschaften für geschütztes EAP zu öffnen, und führen Sie die folgenden Schritte aus:
  - a. Geben Sie im Feld **Verbindung mit diesen Servern herstellen** den Namen des NPS-Servers ein, den Sie aus den NPS-Server-Authentifizierungs Einstellungen weiter oben in diesem Abschnitt abgerufen haben (z. b. **NPS01**).

**NOTE**

Der Servername, den Sie eingeben, muss mit dem Namen im Zertifikat identisch sein. Diesen Namen haben Sie zuvor in diesem Abschnitt wieder hergestellt. Wenn der Name nicht stimmt, schlägt die Verbindung fehl, und es wird angegeben, dass die Verbindung aufgrund einer Richtlinie, die auf Ihrem RAS/VPN-Server konfiguriert wurde, verhindert wurde.

- b. Wählen Sie unter **Vertrauenswürdige Stamm Zertifizierungsstellen** die Stamm Zertifizierungsstelle aus, die das Zertifikat des NPS-Servers ausgestellt hat (z. b. "Configuration Manager").
- c. Klicken Sie in Benachrichtigungen vor dem Herstellen einer Verbindung auf **Benutzer nicht zur Autorisierung neuer Server oder vertrauenswürdiger Zertifizierungsstellen**.

d. Wählen Sie unter Authentifizierungsmethode auswählen die Option **Smartcard oder anderes Zertifikataus**, und klicken Sie dann auf **Konfigurieren**. Das Dialogfeld Smartcard-oder andere Zertifikat Eigenschaften wird geöffnet.

e. Klicken Sie auf **Zertifikat auf diesem Computer verwenden**.

f. Geben Sie im Feld Verbindung mit diesen Servern herstellen den Namen des NPS-Servers ein, den Sie in den vorherigen Schritten aus den NPS-Server Authentifizierungs Einstellungen abgerufen haben.

g. Wählen Sie unter Vertrauenswürdige Stamm Zertifizierungsstellen die Stamm Zertifizierungsstelle aus, von der das Zertifikat des NPS-Servers ausgestellt wurde.

h. Aktivieren Sie das Kontrollkästchen **Benutzer nicht zur Autorisierung neuer Server oder vertrauenswürdiger Zertifizierungsstellen auffordern**.

i. Klicken Sie auf **OK**, um das Dialogfeld Smartcard-oder andere Zertifikat Eigenschaften zu schließen.

j. Klicken Sie auf **OK**, um das Dialogfeld Eigenschaften für geschütztes EAP zu schließen.

14. Klicken Sie auf **OK**, um das Dialogfeld Vorlagen Eigenschaften zu schließen.

15. Schließen Sie das Fenster Netzwerkverbindungen.

16. Testen Sie das VPN in den Einstellungen, indem Sie auf **Vorlage** und dann auf **verbinden** klicken.

#### **IMPORTANT**

Stellen Sie sicher, dass die VPN-Vorlagen Verbindung mit Ihrem VPN-Server erfolgreich ist. Dadurch wird sichergestellt, dass die EAP-Einstellungen korrekt sind, bevor Sie im nächsten Beispiel verwendet werden. Sie müssen mindestens einmal eine Verbindung herstellen, bevor Sie fortfahren. Andernfalls enthält das Profil nicht alle Informationen, die erforderlich sind, um eine Verbindung mit dem VPN herzustellen.

## Erstellen der profileXML-Konfigurationsdateien

Vergewissern Sie sich vor dem Abschließen dieses Abschnitts, dass Sie die VPN-Vorlagen Verbindung erstellt und getestet haben, die im Abschnitt [Manuelles Erstellen eines Vorlagen Verbindungs Profils](#) beschrieben wird. Das Testen der VPN-Verbindung ist erforderlich, um sicherzustellen, dass das Profil alle für die Verbindung mit dem VPN erforderlichen Informationen enthält.

Mit dem Windows PowerShell-Skript in der Liste 1 werden zwei Dateien auf dem Desktop erstellt, von denen beide **eaxconfiguration** -Tags enthalten, die auf dem zuvor erstellten Vorlagen Verbindungsprofil basieren:

- **VPN\_Profile.Xml**. Diese Datei enthält das XML-Markup, das erforderlich ist, um den profileXML-Knoten im VPNV2-CSP zu konfigurieren. Verwenden Sie diese Datei mit OMA-DM – kompatiblen MDM-Diensten wie InTune.
- **VPN\_Profile.ps1**. Bei dieser Datei handelt es sich um ein Windows PowerShell-Skript, das Sie auf Client Computern ausführen können, um den profileXML-Knoten im VPNV2-CSP zu konfigurieren. Sie können den CSP auch konfigurieren, indem Sie dieses Skript über Configuration Manager bereitstellen. Sie können dieses Skript nicht in einer Remotedesktop Sitzung ausführen, einschließlich einer erweiterten Hyper-V-Sitzung.

#### **IMPORTANT**

Die folgenden Beispiel Befehle erfordern Windows 10 Build 1607 oder höher.

### Create VPN\_Profile.XML und VPN\_Profile.ps1

1. Melden Sie sich bei dem in die Domäne eingebundenen Client Computer an, auf dem das VPN-Vorlagen Profil mit dem gleichen Benutzerkonto enthalten ist, und [Erstellen Sie manuell ein Vorlagen Verbindungsprofil](#).
2. Fügen Sie die Liste 1 in Windows PowerShell Integrated Scripting Environment (ISE) ein, und passen Sie die Parameter an, die in den Kommentaren beschrieben werden. Dabei handelt es sich um \$Template, \$ProfileName, \$Servers, \$DnsSuffix, \$Domainname, \$TrustedNetwork und \$DnsServers. Eine vollständige Beschreibung der einzelnen Einstellungen finden Sie in den Kommentaren.
3. Führen Sie das Skript aus, um **VPN\_Profile.XML** und **VPN\_Profile.ps1** auf dem Desktop zu generieren.

#### Auflistung 1: Grundlegendes zu makeprofile.ps1

In diesem Abschnitt wird der Beispielcode erläutert, den Sie verwenden können, um ein Verständnis für die Erstellung eines VPN-Profil zu erhalten, insbesondere für die Konfiguration von profileXML im VPNV2-CSP.

Nachdem Sie ein Skript aus diesem Beispielcode assembled und das Skript ausgeführt haben, generiert das Skript zwei Dateien: **VPN\_Profile.XML** und **VPN\_Profile.ps1**. Verwenden Sie **VPN\_Profile.XML**, um profileXML in OMA-DM-kompatiblen MDM-Diensten wie Microsoft InTune zu konfigurieren.

Verwenden Sie das Skript **VPN\_Profile.ps1** in Windows PowerShell oder Microsoft Endpoint Configuration Manager, um profileXML auf dem Windows 10-Desktop zu konfigurieren.

#### NOTE

Das vollständige Beispielskript finden Sie im Abschnitt [makeprofile.ps1 Full Script](#).

#### Parameter

Konfigurieren Sie die folgenden Parameter:

**\$Template.** Der Name der Vorlage, aus der die EAP-Konfiguration abgerufen werden soll.

**\$ProfileName.** Eindeutiger alphanumerischer Bezeichner für das Profil. Der Profilename darf keinen Schrägstrich (/) enthalten. Wenn der Profilename ein Leerzeichen oder ein anderes nicht alphanumerisches Zeichen enthält, muss er gemäß dem URL-Codierungsstandard ordnungsgemäß mit Escapezeichen versehen werden.

**\$Servers.** Öffentliche oder Routing fähige IP-Adresse oder DNS-Name für das VPN-Gateway. Sie kann auf die externe IP-Adresse eines Gateways oder auf eine virtuelle IP-Adresse für eine Serverfarm zeigen. Beispiele, 208.147.66.130 oder VPN.contoso.com.

**\$DnsSuffix.** Gibt ein oder mehrere durch Kommas getrennte DNS-Suffixe an. Der erste in der Liste wird auch als primäres Verbindungs spezifisches DNS-Suffix für die VPN-Schnittstelle verwendet. Die gesamte Liste wird auch der suffixsearchlist hinzugefügt.

**\$Domainname.** Wird verwendet, um den Namespace anzugeben, auf den die Richtlinie angewendet wird. Wenn eine Namensabfrage ausgegeben wird, vergleicht der DNS-Client den Namen in der Abfrage mit allen Namespaces unter domainnameinformationlist, um eine Übereinstimmung zu finden. Dieser Parameter kann einen der folgenden Typen aufweisen:

- FQDN-vollständig qualifizierter Domänen Name
- Suffix: ein Domänen Suffix, das an die Kurznamen-Abfrage für die DNS-Auflösung angefügt wird. Um ein Suffix anzugeben, fügen Sie dem DNS-Suffix einen Zeitraum (.) vorangestellt.

**\$DnsServers.** Liste der durch Trennzeichen getrennten DNS-Server-IP-Adressen, die für den Namespace verwendet werden sollen.

**\$TrustedNetwork.** Durch Trennzeichen getrennte Zeichenfolge zum Identifizieren des vertrauenswürdigen Netzwerks. VPN stellt keine automatische Verbindung her, wenn sich der Benutzer in seinem Unternehmens-Drahtlos Netzwerk befindet, in dem geschützte Ressourcen direkt für das Gerät zugänglich sind.

Im folgenden finden Sie Beispiel Werte für Parameter, die in den folgenden Befehlen verwendet werden. Stellen Sie sicher, dass Sie diese Werte für Ihre Umgebung ändern.

```
$TemplateName = 'Template'
$ProfileName = 'Contoso%20AlwaysOn%20VPN'
$Servers = 'vpn.contoso.com'
$DnsSuffix = 'corp.contoso.com'
$DomainName = '.corp.contoso.com'
$DNServers = '10.10.0.2,10.10.0.3'
$TrustedNetwork = 'corp.contoso.com'
```

## Vorbereiten und Erstellen der Profil-XML

Mit den folgenden Beispiel Befehlen werden EAP-Einstellungen aus dem Vorlagen Profil angezeigt:

```
$Connection = Get-VpnConnection -Name $TemplateName
if(!$Connection)
{
    $Message = "Unable to get $TemplateName connection profile: $_"
    Write-Host "$Message"
    exit
}
$EAPSettings= $Connection.EapConfigXmlStream.InnerXml
```

## Erstellen der Profil-XML

### IMPORTANT

Eine beliebige andere Kombination aus Groß- oder Kleinbuchstaben für "True" in der folgenden Tags führt eine partielle Konfiguration von VPN-Profil:

```
<AlwaysOn>true</AlwaysOn>
<RememberCredentials>true</RememberCredentials>
```

```
$ProfileXML = @(
    <VPNProfile>
        <DnsSuffix>$DnsSuffix</DnsSuffix>
        <NativeProfile>
            <Servers>$Servers</Servers>
            <NativeProtocolType>IKEv2</NativeProtocolType>
            <Authentication>
                <UserMethod>Eap</UserMethod>
                <Eap>
                    <Configuration>
                        $EAPSettings
                    </Configuration>
                </Eap>
            </Authentication>
            <RoutingPolicyType>SplitTunnel</RoutingPolicyType>
            </NativeProfile>
            <AlwaysOn>true</AlwaysOn>
            <RememberCredentials>true</RememberCredentials>
            <TrustedNetworkDetection>$TrustedNetwork</TrustedNetworkDetection>
            <DomainNameInformation>
                <DomainName>$DomainName</DomainName>
                <DnsServers>$DNServers</DnsServers>
            </DomainNameInformation>
        </VPNProfile>
    )
```

## Ausgabe VPN\_Profile. XML für InTune

Sie können den folgenden Beispiel Befehl verwenden, um die XML-Profil Datei zu speichern:

```
$ProfileXML | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.xml')
```

### Ausgabe von "VPN\_Profile.ps1" für den Desktop und Configuration Manager

Der folgende Beispielcode konfiguriert eine AlwaysOn-IKEv2-VPN-Verbindung mit dem profileXML-Knoten im VPNV2-CSP.

Sie können dieses Skript auf dem Windows 10-Desktop oder in Configuration Manager verwenden.

### Definieren von Schlüssel-VPN-Profil Parametern

```
$Script = '$ProfileName = ''' + $ProfileName + '''  
$ProfileNameEscaped = $ProfileName -replace ' ', '%20'
```

### Sonderzeichen im Profil mit Escapezeichen versehen

```
$ProfileXML = $ProfileXML -replace '<', '&lt;'  
$ProfileXML = $ProfileXML -replace '>', '&gt;'  
$ProfileXML = $ProfileXML -replace '''', '&quot;'
```

### Definieren von WMI-zu-CSP-Brücken Eigenschaften

```
$nodeCSPURI = ".\Vendor/MSFT/VPNV2"  
$namespaceName = "root\cimv2\mdm\dmmap"  
$className = "MDM_VPNv2_01"
```

### Bestimmen Sie die Benutzer-SID für das VPN-Profil:

```
try  
{  
    $username = Get-WmiObject Win32_ComputerSystem | select username  
    $objuser = New-Object System.Security.Principal.NTAccount($username.username)  
    $sid = $objuser.Translate([System.Security.Principal.SecurityIdentifier])  
    $SidValue = $sid.Value  
    $Message = "User SID is $SidValue."  
    Write-Host "$Message"  
}  
catch [Exception]  
{  
    $Message = "Unable to get user SID. User may be logged on over Remote Desktop: $_"  
    Write-Host "$Message"  
    exit  
}
```

### Definieren einer WMI-Sitzung:

```
$session = New-CimSession  
$options = New-Object Microsoft.Management.Infrastructure.Options.CimOperationOptions  
$options.SetCustomOption("PolicyPlatformContext_PrincipalContext_Type", "PolicyPlatform_UserContext", $false)  
$options.SetCustomOption("PolicyPlatformContext_PrincipalContext_Id", "$SidValue", $false)
```

### Vorheriges VPN-Profil erkennen und löschen:

```

try
{
    $deleteInstances = $session.EnumerateInstances($namespaceName, $className, $options)
    foreach ($deleteInstance in $deleteInstances)
    {
        $InstanceId = $deleteInstance.InstanceID
        if ("$InstanceId" -eq "$ProfileNameEscaped")
        {
            $session.DeleteInstance($namespaceName, $deleteInstance, $options)
            $Message = "Removed $ProfileName profile $InstanceId"
            Write-Host "$Message"
        } else {
            $Message = "Ignoring existing VPN profile $InstanceId"
            Write-Host "$Message"
        }
    }
}
catch [Exception]
{
    $Message = "Unable to remove existing outdated instance(s) of $ProfileName profile: $_"
    Write-Host "$Message"
    exit
}

```

### **Erstellen Sie das VPN-Profil:**

```

try
{
    $newInstance = New-Object Microsoft.Management.Infrastructure.CimInstance $className, $namespaceName
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ParentID", "$nodeCSPURI", "String",
    "Key")
    $newInstance.CimInstanceProperties.Add($property)
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("InstanceID", "$ProfileNameEscaped",
    "String", "Key")
    $newInstance.CimInstanceProperties.Add($property)
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ProfileXML", "$ProfileXML",
    "String", "Property")
    $newInstance.CimInstanceProperties.Add($property)
    $session.CreateInstance($namespaceName, $newInstance, $options)
    $Message = "Created $ProfileName profile."
    Write-Host "$Message"
}
catch [Exception]
{
    $Message = "Unable to create $ProfileName profile: $_"
    Write-Host "$Message"
    exit
}

$Message = "Script Complete"
Write-Host "$Message"

```

### **Speichern der XML-Profil Datei**

```

$Script | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.ps1')

$Message = "Successfully created VPN_Profile.xml and VPN_Profile.ps1 on the desktop."
Write-Host "$Message"

```

## **Vollständiges Skript für makeprofile.ps1**

In den meisten Beispielen wird das Windows PowerShell-Cmdlet Set-wmiinstance verwendet, um profileXML in eine neue Instanz der WMI-Klasse MDM\_VPNv2\_01 einzufügen.

Dies funktioniert jedoch nicht in Configuration Manager, da das Paket nicht im Kontext des Endbenutzers ausgeführt werden kann. Daher verwendet dieses Skript das Common Information Model, um eine WMI-Sitzung im Kontext des Benutzers zu erstellen. Anschließend wird eine neue Instanz der MDM\_VPNv2\_01 WMI-Klasse in dieser Sitzung erstellt. Diese WMI-Klasse verwendet die WMI-zu-CSP-Bridge, um den VPNv2-CSP zu konfigurieren. Daher konfigurieren Sie den CSP durch Hinzufügen der Klasseninstanz.

#### IMPORTANT

Die WMI-zu-CSP-Bridge erfordert die lokalen Administratorrechte. Zum Bereitstellen von pro-Benutzer-VPN-Profilen sollten Sie Configuration Manager oder MDM verwenden.

#### NOTE

Das Skript VPN\_Profile.ps1 verwendet die SID des aktuellen Benutzers, um den Kontext des Benutzers zu identifizieren. Da keine SID in einer Remotedesktop Sitzung verfügbar ist, funktioniert das Skript nicht in einer Remotedesktop Sitzung. Ebenso funktioniert es nicht in einer erweiterten Hyper-V-Sitzung. Wenn Sie einen Remote Zugriff Always on-VPN auf virtuellen Computern testen, deaktivieren Sie die erweiterte Sitzung auf Ihren Client-VMS, bevor Sie dieses Skript ausführen.

Das folgende Beispieldokument enthält alle Codebeispiele aus den vorherigen Abschnitten. Stellen Sie sicher, dass Sie Beispiel Werte in Werte ändern, die für Ihre Umgebung geeignet sind.

```
$TemplateName = 'Template'
$ProfileName = 'Contoso AlwaysOn VPN'
$Servers = 'vpn.contoso.com'
$DnsSuffix = 'corp.contoso.com'
$DomainName = '.corp.contoso.com'
$DNSServers = '10.10.0.2,10.10.0.3'
$TrustedNetwork = 'corp.contoso.com'

$Connection = Get-VpnConnection -Name $TemplateName
if (!$Connection)
{
    $Message = "Unable to get $TemplateName connection profile: $_"
    Write-Host "$Message"
    exit
}
$EAPSettings= $Connection.EapConfigXmlStream.InnerXml

$ProfileXML = @"
<VPNProfile>
    <DnsSuffix>$DnsSuffix</DnsSuffix>
    <NativeProfile>
        <Servers>$Servers</Servers>
        <NativeProtocolType>IKEv2</NativeProtocolType>
        <Authentication>
            <UserMethod>Eap</UserMethod>
            <Eap>
                <Configuration>
                    $EAPSettings
                </Configuration>
            </Eap>
        </Authentication>
        <RoutingPolicyType>SplitTunnel</RoutingPolicyType>
        </NativeProfile>
    <AlwaysOn>true</AlwaysOn>
    <RememberCredentials>true</RememberCredentials>
</VPNProfile>
"@
```

```

<!--Member Credentials/ or dev/ -->
<TrustedNetworkDetection>$TrustedNetwork</TrustedNetworkDetection>
<DomainNameInformation>
<DomainName>$DomainName</DomainName>
<DnsServers>$DNSServers</DnsServers>
</DomainNameInformation>
</VPNProfile>
")

$ProfileXML | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.xml')

$Script = @(
    `$ProfileName = '$ProfileName'
    `$ProfileNameEscaped = `$ProfileName -replace ' ', '%20'

    `$ProfileXML = '$ProfileXML'

    `$ProfileXML = `$ProfileXML -replace '<', '&lt;'
    `$ProfileXML = `$ProfileXML -replace '>', '&gt;'
    `$ProfileXML = `$ProfileXML -replace '``', '&quot;'

    `$nodeCSPURI = `".\Vendor/MSFT/VPNv2`"
    `$namespaceName = `"root\cimv2\mdm\dmmap`"
    `$className = `"$MDM_VPNv2_01`"

    try
    {
        `$username = Gwmi -Class Win32_ComputerSystem | select username
        `$objuser = New-Object System.Security.Principal.NTAccount(`$username.username)
        `$sid = `$objuser.Translate([System.Security.Principal.SecurityIdentifier])
        `$SidValue = `$sid.Value
        `$Message = `'"User SID is `$SidValue.`"
        Write-Host ``$Message``
    }
    catch [Exception]
    {
        `$Message = `'"Unable to get user SID. User may be logged on over Remote Desktop: `$_`"
        Write-Host ``$Message``
        exit
    }

    `$session = New-CimSession
    `$options = New-Object Microsoft.Management.Infrastructure.Options.CimOperationOptions
    `$options.SetCustomOption(`"PolicyPlatformContext_PrincipalContext_Type`", `"PolicyPlatform_UserContext`",
    `$false)
    `$options.SetCustomOption(`"PolicyPlatformContext_PrincipalContext_Id`", `"`$SidValue`, `$false)

    try
    {
        `$deleteInstances = `$session.EnumerateInstances(`$namespaceName, `$className, `$options)
        foreach (`$deleteInstance in `$deleteInstances)
        {
            `$InstanceId = `$deleteInstance.InstanceID
            if ("`$InstanceId`" -eq `"$ProfileNameEscaped`")
            {
                `$session.DeleteInstance(`$namespaceName, `$deleteInstance, `$options)
                `$Message = `'"Removed `$ProfileName profile `$InstanceId`"
                Write-Host ``$Message``
            } else {
                `$Message = `'"Ignoring existing VPN profile `$InstanceId`"
                Write-Host ``$Message``
            }
        }
    }
    catch [Exception]
    {
        `$Message = `'"Unable to remove existing outdated instance(s) of `$ProfileName profile: `$_`"
        Write-Host ``$Message``
        exit
    }
)

```

```

}

try
{
    $newInstance = New-Object Microsoft.Management.Infrastructure.CimInstance '$className', '$namespaceName'
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create(`"ParentID`", `"$nodeCSPURI`",
    `String`, `"Key`")
    $newInstance.CimInstanceProperties.Add($property)
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create(`"InstanceID`",
    `"$ProfileNameEscaped`", `String`, `"Key`")
    $newInstance.CimInstanceProperties.Add($property)
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create(`"ProfileXML`", `"$ProfileXML`",
    `String`, `"Property`")
    $newInstance.CimInstanceProperties.Add($property)
    $session.CreateInstance($namespaceName, $newInstance, $options)
    $Message = "Created `$ProfileName profile.`"

    Write-Host "`$Message"
}
catch [Exception]
{
    $Message = "Unable to create `$ProfileName profile: `$_`"
    Write-Host "`$Message"
    exit
}

`$Message = "Script Complete"
Write-Host "`$Message"
")

$Script | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.ps1')

$Message = "Successfully created VPN_Profile.xml and VPN_Profile.ps1 on the desktop."
Write-Host "$Message"

```

## Konfigurieren des VPN-Clients mithilfe von Windows PowerShell

Um den VPnv2-CSP auf einem Windows 10-Client Computer zu konfigurieren, führen Sie das Windows PowerShell-Skript VPN\_Profile.ps1 aus, das Sie im Abschnitt [Erstellen des Profils "XML"](#) erstellt haben. Öffnen Sie Windows PowerShell als Administrator. Andernfalls erhalten Sie die Fehlermeldung "Zugriff verweigert".

Nachdem Sie VPN\_Profile.ps1 ausgeführt haben, um das VPN-Profil zu konfigurieren, können Sie jederzeit überprüfen, ob es erfolgreich war, indem Sie den folgenden Befehl in der Windows PowerShell ISE ausführen:

```
Get-WmiObject -Namespace root\cimv2\mdm\dmmmap -Class MDM_VPNv2_01
```

### Erfolgreiche Ergebnisse des Cmdlets "Get-WmiObject"

```

__GENUS : 2
__CLASS : MDM_VPNv2_01
__SUPERCLASS:
__DYNASTY   : MDM_VPNv2_01
__RELPATH   : MDM_VPNv2_01.InstanceID="Contoso%20AlwaysOn%20VPN",ParentID
               ="./Vendor/MSFT/VPNV2"
__PROPERTY_COUNT: 10
__DERIVATION: {}
__SERVER: WIN01
__NAMESPACE : root\cimv2\mdm\dmmmap
__PATH   : \\WIN01\root\cimv2\mdm\dmmmap:MDM_VPNv2_01.InstanceID="Conto
               so%20AlwaysOn%20VPN",ParentID="./Vendor/MSFT/VPNV2"
AlwaysOn: True
ByPassForLocal :
DnsSuffix   : corp.contoso.com
FdnModeTd   :

```

```


    .
    InstanceID : Contoso%20AlwaysOn%20VPN
    LockDown:
    ParentID: ./Vendor/MSFT/VPNv2
    ProfileXML : <VPNProfile><RememberCredentials>true</RememberCredentials>
        <AlwaysOn>true</AlwaysOn><DnsSuffix>corp.contoso.com</DnsSu
        ffix><TrustedNetworkDetection>corp.contoso.com</TrustedNetw
        orkDetection><NativeProfile><Servers>vpn.contoso.com;vpn.co
        ntoso.com</Servers><RoutingPolicyType>SplitTunnel</RoutingP
        olicyType><NativeProtocolType>Ikev2</NativeProtocolType><Au
        thentication><UserMethod>Eap</UserMethod><MachineMethod>Eap
        </MachineMethod><Eap><Configuration><EapHostConfig xmlns="h
        ttp://www.microsoft.com/provisioning/EapHostConfig"><EapMet
        hod><Type xmlns="https://www.microsoft.com/provisioning/EapC
        ommon">25</Type><VendorId xmlns="https://www.microsoft.com/p
        rovisioning/EapCommon">0</VendorId><VendorType xmlns="http:
        //www.microsoft.com/provisioning/EapCommon">0</VendorType><
        AuthorId xmlns="https://www.microsoft.com/provisioning/EapCo
        mmon">0</AuthorId></EapMethod><Config xmlns="https://www.mic
        rosoft.com/provisioning/EapHostConfig"><Eap xmlns="https://w
        ww.microsoft.com/provisioning/BaseEapConnectionPropertiesV1
        "><Type>25</Type><EapType xmlns="https://www.microsoft.com/p
        rovisioning/MsPeapConnectionPropertiesV1"><ServerValidation
        ><DisableUserPromptForServerValidation>true</DisableUserPro
        mptForServerValidation><ServerNames>NPS</ServerNames><Trust
        edRootCA>3f 07 88 e8 ac 00 32 e4 06 3f 30 f8 db 74 25 e1
        2e 5b 84 d1 </TrustedRootCA></ServerValidation><FastReconne
        ct>true</FastReconnect><InnerEapOptional>false</InnerEapOpt
        ional><Eap xmlns="https://www.microsoft.com/provisioning/Bas
        eEapConnectionPropertiesV1"><Type>13</Type><EapType xmlns="
        https://www.microsoft.com/provisioning/EapTlsConnectionPrope
        rtiesV1"><CredentialsSource><CertificateStore><SimpleCertSe
        lection>true</SimpleCertSelection></CertificateStore></Cred
        entialsSource><ServerValidation><DisableUserPromptForServer
        Validation>true</DisableUserPromptForServerValidation><Serv
        erNames>NPS</ServerNames><TrustedRootCA>3f 07 88 e8 ac 00
        32 e4 06 3f 30 f8 db 74 25 e1 2e 5b 84 d1 </TrustedRootCA><
        /ServerValidation><DifferentUsername>false</DifferentUserna
        me><PerformServerValidation xmlns="https://www.microsoft.com/
        provisioning/EapTlsConnectionPropertiesV2">true</PerformSe
        rverValidation><AcceptServerName xmlns="https://www.microsof
        t.com/provisioning/EapTlsConnectionPropertiesV2">true</Acce
        ptServerName></EapType></Eap><EnableQuarantineChecks>false<
        /EnableQuarantineChecks><RequireCryptoBinding>false</Requir
        eCryptoBinding><PeapExtensions><PerformServerValidation xml
        ns="https://www.microsoft.com/provisioning/MsPeapConnec
        tionPropertiesV2">true</PerformServerValidation><AcceptServerNam
        e xmlns="https://www.microsoft.com/provisioning/MsPeapConnec
        tionPropertiesV2">true</AcceptServerName></PeapExtensions><
        /EapType></Eap></Config></EapHostConfig></Configuration></E
        ap></Authentication></NativeProfile><DomainNameInformation>
        <DomainName>corp.contoso.com</DomainName><DnsServers>10.10.
        0.2,10.10.0.3</DnsServers><AutoTrigger>true</AutoTrigger><
        /DomainNameInformation></VPNProfile>
```

RememberCredentials : True  
 TrustedNetworkDetection : corp.contoso.com  
 PSComputerName : WIN01

Die profileXML-Konfiguration muss in der Struktur, in der Rechtschreibung, in der Konfiguration und in manchen Fällen recht groß sein. Wenn Sie in der Struktur etwas anderes als das Auflisten 1 sehen, enthält das profileXML-Markup wahrscheinlich einen Fehler.

Wenn Sie eine Problembehandlung für das Markup durchsetzen müssen, ist es einfacher, es in einem XML-Editor zu platzieren, als es in der Windows PowerShell ISE behandeln zu müssen. Beginnen Sie in jedem Fall mit der einfachsten Version des Profils, und fügen Sie Komponenten nacheinander hinzu, bis das Problem erneut auftritt.

# Konfigurieren des VPN-Clients mithilfe von Configuration Manager

In Configuration Manager können Sie VPN-profile bereitstellen, indem Sie den profileXML-CSP-Knoten genau wie in Windows PowerShell verwenden. Hier verwenden Sie das Windows PowerShell-Skript VPN\_Profile.ps1, das Sie im Abschnitt [Erstellen der profileXML-Konfigurationsdateien](#) erstellt haben.

Wenn Sie Configuration Manager für die Bereitstellung eines Remote Zugriffs Always on VPN-Profs für Windows 10-Client Computer verwenden möchten, müssen Sie zunächst eine Gruppe von Computern oder Benutzern erstellen, für die Sie das Profil bereitstellen. Erstellen Sie in diesem Szenario eine Benutzergruppe, um das Konfigurationsskript bereitzustellen.

## Erstellen einer Benutzergruppe

1. Öffnen Sie in der Configuration Manager Konsole Assets und Konformität \ Benutzer Sammlungen.
2. Klicken Sie auf dem Menüband **Start** in der Gruppe **Erstellen** auf **Benutzer Sammlung erstellen**.
3. Führen Sie auf der Seite Allgemein die folgenden Schritte aus:
  - a. Geben Sie unter **Name** den Namen **VPN-Benutzerein**.
  - b. Klicken Sie auf **Durchsuchen**, dann auf **alle Benutzer** und dann auf **OK**.
  - c. Klicken Sie auf **Weiter**.
4. Führen Sie auf der Seite Mitgliedschafts Regeln die folgenden Schritte aus:
  - a. Klicken Sie unter **Mitgliedschafts Regeln** auf **Regel hinzufügen**, und klicken Sie auf **direkt Regel**. In diesem Beispiel fügen Sie einzelne Benutzer zur Benutzer Sammlung hinzu. Sie können jedoch eine Abfrage Regel verwenden, um dieser Sammlung für eine größere Bereitstellung dynamisch Benutzer hinzuzufügen.
  - b. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
  - c. Geben Sie auf der Seite Ressourcen suchen unter **Wert** den Namen des Benutzers ein, den Sie hinzufügen möchten. Der Ressourcen Name enthält die Domäne des Benutzers. Um Ergebnisse auf der Grundlage einer Teil Übereinstimmung einzuschließen, fügen % Sie das Zeichen an beiden Enden des Such Kriteriums ein. Wenn Sie z. b. alle Benutzer suchen möchten, die die Zeichenfolge "Lori" enthalten, geben Sie % Lori% ein. Klicken Sie auf **Weiter**.
  - d. Wählen Sie auf der Seite Ressourcen auswählen die Benutzer aus, die Sie der Gruppe hinzufügen möchten, und klicken Sie auf **weiter**.
  - e. Klicken Sie auf der Seite Zusammenfassung auf **Weiter**.
  - f. Klicken Sie auf der Seite Abschluss auf **Schließen**.
5. Klicken Sie im Assistenten zum Erstellen von Benutzer Sammlungen auf der Seite **Mitgliedschafts Regeln** auf **weiter**.
6. Klicken Sie auf der Seite Zusammenfassung auf **Weiter**.
7. Klicken Sie auf der Seite Abschluss auf **Schließen**.

Nachdem Sie die Benutzergruppe für den Empfang des VPN-Profs erstellt haben, können Sie ein Paket und ein Programm erstellen, um das Windows PowerShell-Konfigurationsskript bereitzustellen, das Sie im Abschnitt [Erstellen der profileXML-Konfigurationsdateien](#) erstellt haben.

## Erstellen eines Pakets, das das profileXML-Konfigurationsskript enthält

1. Hosten Sie das Skript VPN\_Profile.ps1 auf einer Netzwerkfreigabe, auf die das Computer Konto des Standort Servers zugreifen kann.

2. Öffnen Sie in der Configuration Manager-Konsole **Software Bibliothek \ Anwendungs Verwaltung \ Pakete**.
3. Klicken Sie auf dem Menüband **Start** in der Gruppe **Erstellen** auf **Paket erstellen**, um den Assistenten zum Erstellen von Paketen und Programmen zu starten.
4. Führen Sie auf der Seite **Paket** die folgenden Schritte aus:
  - a. Geben Sie unter **Name** den Namen **Windows 10 Always on VPN-Profilein**.
  - b. Aktivieren Sie das Kontrollkästchen **Dieses Paket enthält Quelldateien**, und klicken Sie auf **Durchsuchen**.
  - c. Klicken Sie im Dialogfeld Quellordner festlegen auf **Durchsuchen**, wählen Sie die Dateifreigabe mit **VPN\_Profile.ps1** aus, und klicken Sie auf **OK**. Stellen Sie sicher, dass Sie einen Netzwerkpfad und keinen lokalen Pfad auswählen. Anders ausgedrückt: der Pfad sollte in etwa wie folgt aussehen: \* \ File Server \ vpnscrip\*, nicht c: \ vpnscrip.
5. Klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite **Programmtyp** auf **weiter**.
7. Führen Sie auf der Seite **Standard Programm** die folgenden Schritte aus:
  - a. Geben Sie unter **Name** den Namen **VPN-Profil Skriptein**.
  - b. Geben Sie in der **Befehlszeile PowerShell** **exe-ExecutionPolicy Bypass-file "VPN\_Profile.ps1"** ein.
  - c. Klicken Sie im **Lauf Modus** auf mit **Administratorrechten ausführen**.
  - d. Klicken Sie auf **Weiter**.
8. Führen Sie auf der Seite **Anforderungen** die folgenden Schritte aus:
  - a. Wählen Sie **dieses Programm kann nur auf bestimmten Plattformen ausgeführt werden aus**.
  - b. Aktivieren Sie die Kontrollkästchen **alle Windows 10 (32-Bit)** und **alle Windows 10 (64 Bit)**.
  - c. Geben Sie im Feld **Geschätzter Speicherplatz 1** ein.
  - d. Geben Sie unter **maximal zulässige Laufzeit (Minuten)** **15** ein.
  - e. Klicken Sie auf **Weiter**.
9. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.
10. Klicken Sie auf der Seite **Abschluss** auf **Schließen**.

Nachdem Sie das Paket und das Programm erstellt haben, müssen Sie es für die **VPN-Benutzer** Gruppe bereitstellen.

#### **Bereitstellen des profileXML-Konfigurations Skripts**

1. Öffnen Sie in der Configuration Manager-Konsole **Software Bibliothek \ Anwendungs Verwaltung \ Pakete**.
2. Klicken Sie unter **Pakete** auf **Windows 10 Always on VPN-Profil**.
3. Klicken Sie auf der Registerkarte **Programme** unten im Detailbereich mit der rechten Maustaste auf **VPN-Profil Skript**, klicken Sie auf **Eigenschaften**, und führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf der Registerkarte **erweitert** in **Wenn dieses Programm einem Computer zugewiesen ist, auf einmal für jeden Benutzer, der sich anmeldet**.

- b. Klicken Sie auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf **VPN- Profil Skript** , und klicken Sie auf bereitstellen, um den Assistenten zum
5. Führen Sie auf der Seite Allgemein die folgenden Schritte aus:
  - a. Klicken Sie neben **Sammlung** auf **Durchsuchen**.
  - b. Klicken Sie in der Liste **Sammlungs Typen** (oben links) auf **Benutzer Sammlungen**.
  - c. Klicken Sie auf **VPN-Benutzer** und dann auf **OK**.
  - d. Klicken Sie auf **Weiter**.
6. Führen Sie auf der Seite Inhalt die folgenden Schritte aus:
  - a. Klicken Sie auf **Hinzufügen** und dann auf **Verteilungs Punkt**.
  - b. Wählen Sie unter **Verfügbare Verteilungs Punkte** die Verteilungs Punkte aus, an die Sie das profileXML-Konfigurationsskript verteilen möchten, und klicken Sie auf **OK**.
  - c. Klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite Bereitstellungs Einstellungen auf **weiter**.
8. Führen Sie auf der Seite Zeitplanung die folgenden Schritte aus:
  - a. Klicken Sie auf **neu** , um das Dialogfeld Zuweisungs Zeitplan zu öffnen.
  - b. Klicken Sie auf **direkt nach diesem Ereignis zuweisen**, und klicken Sie auf **OK**.
  - c. Klicken Sie auf **Weiter**.
9. Führen Sie auf der Seite Benutzer Darstellung die folgenden Schritte aus:
  - a. Aktivieren Sie das Kontrollkästchen **Software Installation** .
  - b. Klicken Sie auf **Übersicht**.
10. Klicken Sie auf der Seite Zusammenfassung auf **Weiter**.
11. Klicken Sie auf der Seite Abschluss auf **Schließen**.

Melden Sie sich bei der Bereitstellung des profilxml-Konfigurations Skripts bei einem Windows 10-Client Computer mit dem Benutzerkonto an, das Sie beim Erstellen der Benutzer Sammlung ausgewählt haben. Überprüfen Sie die Konfiguration des VPN-Clients.

#### **NOTE**

Das Skript **VPN\_Profile.ps1** funktioniert nicht in einer Remotedesktop Sitzung. Ebenso funktioniert es nicht in einer erweiterten Hyper-V-Sitzung. Wenn Sie einen Remote Zugriff Always on-VPN auf virtuellen Computern testen, deaktivieren Sie die erweiterte Sitzung auf Ihren Client-VMS, bevor Sie fortfahren.

### **Überprüfen der Konfiguration des VPN-Clients**

1. Klicken Sie in der Systemsteuerung unter **System \ Sicherheit** auf **Configuration Manager**.
2. Führen Sie im Dialogfeld Configuration Manager Eigenschaften auf der Registerkarte **Aktionen** die folgenden Schritte aus:
  - a. Klicken Sie auf **Computer Richtlinien Abruf & Evaluierungs Zyklus**, klicken Sie auf **jetzt ausführen**, und klicken Sie auf **OK**.

b. Klicken Sie auf **Benutzerrichtlinien Abruf & Evaluierungs Zyklen**, klicken Sie auf **jetzt ausführen**, und klicken Sie auf **OK**.

c. Klicken Sie auf **OK**.

3. Schließen Sie die Systemsteuerung.

Das neue VPN-Profil sollte in Kürze angezeigt werden.

## Konfigurieren des VPN-Clients mithilfe von InTune

Wenn Sie InTune zum Bereitstellen von Windows 10-Remote Zugriff Always on VPN-Profilen verwenden möchten, können Sie den profileXML-CSP-Knoten mithilfe des VPN-Profil konfigurieren, das Sie im Abschnitt [Erstellen der profileXML-Konfigurationsdateien](#) erstellt haben, oder Sie können das unten angegebene Basis-EAP-XML-Beispiel verwenden.

### NOTE

InTune verwendet nun Azure Ad Gruppen. Wenn Azure AD Connect die Gruppe "VPN-Benutzer" vom lokalen Standort aus mit Azure AD synchronisiert haben und Benutzer der Gruppe "VPN-Benutzer" zugewiesen sind, können Sie den Vorgang fortsetzen.

Erstellen Sie die VPN-Geräte Konfigurationsrichtlinie, um die Windows 10-Client Computer für alle Benutzer zu konfigurieren, die der Gruppe hinzugefügt wurden. Da die Intune-Vorlage VPN-Parameter bereitstellt, kopieren Sie nur den < eaphostconfig> < /EapHostConfig> Teil der VPN\_ProfileXML Datei.

### Erstellen der Always on VPN-Konfigurationsrichtlinie

1. Melden Sie sich beim [Azure-Portal](#) an.
2. Wechseln Sie zu **InTune > Geräte Konfigurations > profile**.
3. Klicken Sie zum Starten des Assistenten zum Erstellen von Profilen auf **Profil erstellen**.
4. Geben Sie einen **Namen** für das VPN-Profil und (optional) eine Beschreibung ein.
5. Wählen Sie unter **Plattform** die Option **Windows 10 oder höher**, und wählen Sie in der Dropdown-Dropdown-Dropdown-Dropdown-

### TIP

Wenn Sie ein benutzerdefiniertes VPN-Profil erstellen, finden Sie entsprechende Anweisungen unter [Anwenden von profileXML mithilfe von InTune](#).

6. Überprüfen oder legen Sie auf der Registerkarte **Basis-VPN** die folgenden Einstellungen fest:

- **Verbindungs Name:** Geben Sie den Namen der VPN-Verbindung ein, wie er auf dem Client Computer auf der Registerkarte "VPN" unter "Einstellungen" angezeigt wird, z. B. "Configuration autovpn".
- **Server:** Fügen Sie einen oder mehrere VPN-Server hinzu, indem Sie auf **Hinzufügen**
- **Beschreibung** und **IP-Adresse oder** voll qualifizierten Namen: Geben Sie die Beschreibung und die IP-Adresse oder den voll qualifizierten Namen des VPN-Servers ein. Diese Werte müssen mit dem Antragsteller Namen im Authentifizierungszertifikat des VPN-Servers übereinstimmen.
- **Standard Server:** Wenn dies der VPN-Standard Server ist, legen Sie auf **true** fest. Dadurch kann dieser Server als Standard Server verwendet werden, der von Geräten zum Herstellen der

Verbindung verwendet wird.

- **Verbindungstyp:** Legen Sie auf **IKEv2fest**.
- **Always on:** Legen Sie so fest, dass bei der Anmeldung automatisch eine Verbindung mit dem VPN hergestellt und die Verbindung **bleibt, bis** der Benutzer die Verbindung manuell trennt.
- **Anmelde Informationen bei jeder Anmeldung speichern:** Boolescher Wert (true oder false) zum Zwischenspeichern von Anmelde Informationen. Wenn der Wert auf true festgelegt ist, werden Anmelde Informationen nach Möglichkeit zwischengespeichert

7. Kopieren Sie die folgende XML-Zeichenfolge in einen Text-Editor:

#### IMPORTANT

Eine beliebige andere Kombination aus Groß- oder Kleinbuchstaben für "True" in der folgenden Tags führt eine partielle Konfiguration von VPN-Profil:

```
<AlwaysOn>true</AlwaysOn>
<RememberCredentials>true</RememberCredentials>
```

```
<EapHostConfig xmlns="https://www.microsoft.com/provisioning/EapHostConfig"><EapMethod><Type
xmlns="https://www.microsoft.com/provisioning/EapCommon">25</Type><VendorId
xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorId><VendorType
xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorType><AuthorId
xmlns="https://www.microsoft.com/provisioning/EapCommon">0</AuthorId></EapMethod><Config
xmlns="https://www.microsoft.com/provisioning/EapHostConfig"><Eap
xmlns="https://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"><Type>25</Type><EapType
xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV1"><ServerValidation>
<DisableUserPromptForServerValidation>true</DisableUserPromptForServerValidation>
<ServerNames>NPS.contoso.com</ServerNames><TrustedRootCA>5a 89 fe cb 5b 49 a7 0b 1a 52 63 b7 35 ee d7
1c c2 68 be 4b </TrustedRootCA></ServerValidation><FastReconnect>true</FastReconnect>
<InnerEapOptional>false</InnerEapOptional><Eap
xmlns="https://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"><Type>13</Type><EapType
xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV1"><CredentialsSource>
<CertificateStore><SimpleCertSelection>true</SimpleCertSelection></CertificateStore>
</CredentialsSource><ServerValidation>
<DisableUserPromptForServerValidation>true</DisableUserPromptForServerValidation>
<ServerNames>NPS.contoso.com</ServerNames><TrustedRootCA>5a 89 fe cb 5b 49 a7 0b 1a 52 63 b7 35 ee d7
1c c2 68 be 4b </TrustedRootCA></ServerValidation><DifferentUsername>false</DifferentUsername>
<PerformServerValidation
xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">true</PerformServerValidation>
<AcceptServerName
xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">true</AcceptServerName>
</EapType></Eap><EnableQuarantineChecks>false</EnableQuarantineChecks>
<RequireCryptoBinding>false</RequireCryptoBinding><PeapExtensions><PerformServerValidation
xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2">true</PerformServerValidation>
<AcceptServerName
xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2">true</AcceptServerName>
</PeapExtensions></EapType></Eap></Config></EapHostConfig>
```

8. Ersetzen Sie die Datei " \*\* < treuhändrootca>5A 89 FE CB 5B 49 A7 0B 1a 52 63 B7 35 EE T7 1C C2 68 be  
4B</ treudrootca>\*\* im Beispiel mit dem Zertifikat Fingerabdruck Ihrer lokalen Stamm  
Zertifizierungsstelle an beiden stellen.

#### **IMPORTANT**

Verwenden Sie den Beispiel Fingerabdruck nicht im < Abschnitt "thumbrootca" < /TrustedRootCA> weiter unten. Der Treuhänder muss der Zertifikat Fingerabdruck der lokalen Stamm Zertifizierungsstelle sein, von der das Server Authentifizierungszertifikat für RRAS-und NPS-Server ausgestellt wurde. **Dabei darf es sich nicht um das Cloud-Stamm Zertifikat oder um den Fingerabdruck der zwischen ausstellenden Zertifizierungsstelle handeln.**

9. Ersetzen Sie die \*\* < Server Ames>NPS.contoso.com < /ServerNames>\*\* in der XML-Beispieldatei durch den voll qualifizierten Domänen Namen der in die Domäne eingebundenen NPS, bei der die Authentifizierung stattfindet.
10. Kopieren Sie die überarbeitete XML-Zeichenfolge, und fügen Sie Sie in das Feld **EAP XML auf der Registerkarte Basis-VPN** ein. Eine Always on VPN-Geräte Konfigurationsrichtlinie, die EAP verwendet, wird in InTune erstellt.

#### **Synchronisieren der Always on-VPN-Konfigurationsrichtlinie mit InTune**

Um die Konfigurationsrichtlinie zu testen, melden Sie sich bei einem Windows 10-Client Computer als Benutzer an, den Sie der Gruppe **Always on-VPN-Benutzer** hinzugefügt haben, und synchronisieren Sie dann mit InTune.

1. Klicken Sie im Menü Start auf **Einstellungen**.
2. Klicken Sie unter Einstellungen auf Konten und dann auf **Arbeits-oder Schul Kontozugreifen**.
3. Klicken Sie auf das MDM-Profil, und klicken Sie auf **Info**.
4. Klicken Sie auf **Synchronisieren**, um die Bewertung und den Abruf einer InTune-Richtlinie zu
5. Schließen Sie die Einstellungen. Nach der Synchronisierung sehen Sie, dass das VPN-Profil auf dem Computer verfügbar ist.

## Nächste Schritte

Sie haben die Bereitstellung Always on VPN abgeschlossen. Weitere Funktionen, die Sie konfigurieren können, finden Sie in der folgenden Tabelle:

ZWECK	WEITERE INFORMATIONEN FINDEN SIE UNTER...
Konfigurieren des bedingten Zugriffs für VPN	<a href="#">Schritt 7: Optionale Konfigurieren des bedingten Zugriffs für VPN-Konnektivität mithilfe von Azure AD</a> : in diesem Schritt können Sie optimieren, wie autorisierte VPN-Benutzer mithilfe des <a href="#">bedingten Zugriffs von Azure Active Directory (Azure AD)</a> auf Ihre Ressourcen zugreifen. Mit Azure AD bedingten Zugriff für VPN-Konnektivität (virtuelles privates Netzwerk) können Sie die VPN-Verbindungen schützen. Beim bedingten Zugriff handelt es sich um ein richtlinienbasiertes Auswertungsmodul, mit dem Sie Zugriffsregeln für alle mit Azure Active Directory (Azure AD) verknüpften Anwendungen erstellen können.
Weitere Informationen zu den erweiterten VPN-Features	<a href="#">Erweiterte VPN-Features</a> : auf dieser Seite finden Sie Anleitungen zum Aktivieren von VPN-Datenverkehrs filtern, zum Konfigurieren automatischer VPN-Verbindungen mithilfe von App-Triggern und zum Konfigurieren von NPS für das Zulassen von VPN-Verbindungen von Clients mithilfe von Zertifikaten, die von Azure AD ausgestellt wurden.

# Schritt 7. Optionale Bedingter Zugriff für VPN-Konnektivität mithilfe von Azure AD

09.04.2020 • 8 minutes to read • [Edit Online](#)

- [Vorheriges: Schritt 6: Konfigurieren von Windows 10-Client Always on-VPN-Verbindungen](#)
- [Weiter: Schritt 7,1. Konfigurieren von EAP-TLS zum Ignorieren der CRL-Überprüfung \(Zertifikat Sperr Liste\)](#)

In diesem optionalen Schritt können Sie optimieren, wie VPN-Benutzer mit dem [bedingten Zugriff von Azure Active Directory \(Azure AD\)](#) auf Ihre Ressourcen zugreifen. Mit Azure AD bedingten Zugriff für VPN-Konnektivität (virtuelles privates Netzwerk) können Sie die VPN-Verbindungen schützen. Beim bedingten Zugriff handelt es sich um einrichtlinienbasiertes Auswertungsmodul, mit dem Sie Zugriffsregeln für alle mit Azure Active Directory (Azure AD) verknüpften Anwendungen erstellen können.

## Erforderliche Komponenten

Sie sind mit den folgenden Themen vertraut:

- [Bedingter Zugriff in Azure Active Directory](#)
- [VPN und bedingter Zugriff](#)

Zum Konfigurieren Azure Active Directory bedingten Zugriffs für VPN-Konnektivität muss Folgendes konfiguriert sein:

- [Server Infrastruktur](#)
- [RAS-Server für Always on-VPN](#)
- [Netzwerk Richtlinien Server](#)
- [DNS-und Firewalleinstellungen](#)
- [Windows 10-Client Always on-VPN-Verbindungen](#)

## Schritt 7,1. Konfigurieren von EAP-TLS zum Ignorieren der CRL-Überprüfung (Zertifikat Sperr Liste)

In diesem Schritt können Sie **IgnoreNoRevocationCheck** hinzufügen und festlegen, dass die Authentifizierung von Clients zulässig ist, wenn das Zertifikat keine CRL-Verteilungs Punkte enthält. Standardmäßig ist **IgnoreNoRevocationCheck** auf 0 (deaktiviert) festgelegt.

Ein EAP-TLS-Client kann keine Verbindung herstellen, es sei denn, der NPS-Server schließt eine Sperr Überprüfung der Zertifikat Kette (einschließlich des Stamm Zertifikats) ab. Cloud-Zertifikate, die von Azure AD an den Benutzer ausgegeben werden, verfügen nicht über eine Zertifikat Sperr Liste, da es sich um kurzlebige Zertifikate mit einer Lebensdauer von einer Stunde handelt. EAP auf NPS muss so konfiguriert werden, dass das Fehlen einer CRL ignoriert wird. Da die Authentifizierungsmethode EAP-TLS ist, wird dieser Registrierungs Wert nur unter **eap\13** benötigt. Wenn andere EAP-Authentifizierungsmethoden verwendet werden, sollte der Registrierungs Wert ebenfalls hinzugefügt werden.

## Schritt 7,2. Stamm Zertifikate für die VPN-Authentifizierung mit Azure AD erstellen

In diesem Schritt konfigurieren Sie Stamm Zertifikate für die VPN-Authentifizierung mit Azure AD, wodurch automatisch eine VPN-Server-Cloud-App im Mandanten erstellt wird.

Zum Konfigurieren des bedingten Zugriffs für VPN-Konnektivität müssen Sie folgende Schritte ausführen:

1. Erstellen Sie ein VPN-Zertifikat in der Azure-Portal.
2. Laden Sie das VPN-Zertifikat herunter.
3. Stellen Sie das Zertifikat auf Ihrem VPN-Server bereit.

#### IMPORTANT

Sobald ein VPN-Zertifikat in der Azure-Portal erstellt wurde, wird es von Azure AD sofort verwendet, um dem VPN-Client kurzlebige Zertifikate auszustellen. Es ist wichtig, dass das VPN-Zertifikat sofort auf dem VPN-Server bereitgestellt wird, um Probleme mit der Überprüfung der Anmelde Informationen des VPN-Clients zu vermeiden.

## Schritt 7.3. Konfigurieren der Richtlinie für bedingten Zugriff

In diesem Schritt konfigurieren Sie die Richtlinie für bedingten Zugriff für VPN-Konnektivität.

Zum Konfigurieren der Richtlinie für bedingten Zugriff müssen Sie folgende Schritte ausführen:

1. Erstellen Sie eine Richtlinie für bedingten Zugriff, die VPN-Benutzern zugewiesen wird.
2. Legen Sie die Cloud-App auf **VPN-Serverfest**.
3. Legen Sie für Grant (Zugriffs Steuerung) die **Multi-Factor Authentication** fest. Sie können bei Bedarf andere Steuerelemente verwenden.

## Schritt 7.4. Bereitstellen von Stamm Zertifikaten für den bedingten Zugriff im lokalen AD

In diesem Schritt stellen Sie ein vertrauenswürdiges Stamm Zertifikat für die VPN-Authentifizierung für das lokale Ad bereit.

Zum Bereitstellen des vertrauenswürdigen Stamm Zertifikats müssen Sie folgende Schritte ausführen:

1. Fügen Sie das heruntergeladene Zertifikat als *Vertrauenswürdige* Stamm Zertifizierungsstelle für die VPN-Authentifizierung hinzu.
2. Importieren Sie das Stamm Zertifikat auf den VPN-Server und den VPN-Client.
3. Vergewissern Sie sich, dass die Zertifikate vorhanden sind und als vertrauenswürdig angezeigt werden.

## Schritt 7.5. Erstellen von OMA-DM-basierten VPNV2-Profilen für Windows 10-Geräte

In diesem Schritt können Sie OMA-DM-basierte VPNV2-Profile mithilfe von Intune erstellen, um eine VPN-Geräte Konfigurationsrichtlinie bereitzustellen. Wenn Sie zum Erstellen von VPNV2-Profilen Configuration Manager oder PowerShell-Skript verwenden möchten, finden Sie weitere Informationen unter [VPNV2 CSP Settings](#).

## Nächste Schritte

[Schritt 7.1. Konfigurieren von EAP-TLS zum Ignorieren der CRL-Überprüfung \(Zertifikat Sperr Liste\)](#): in diesem Schritt müssen Sie **IgnoreNoRevocationCheck** hinzufügen und festlegen, dass die Authentifizierung von Clients zugelassen wird, wenn das Zertifikat keine CRL-Verteilungs Punkte enthält. Standardmäßig ist IgnoreNoRevocationCheck auf 0 (deaktiviert) festgelegt.

## Verwandte Themen

- [Konfigurieren von VPNV2-Profilen](#): der VPN-Client ist nun in der Lage, die cloudbasierte Plattform für den

bedingten Zugriff zu integrieren, um eine Geräte Kompatibilitäts Option für Remote Clients bereitzustellen. In diesem Schritt konfigurieren Sie die VPnv2-Profile mit <devicecompliance> <aktiviert> true</Enabled> .

- **Verbessern des Remote Zugriffs in Windows 10 mit einem automatischen VPN-Profil:** erfahren Sie, wie Microsoft den bedingten Zugriff für VPN-Konnektivität implementiert. VPN-Profile enthalten alle Informationen, die ein Gerät für die Verbindung mit dem Unternehmensnetzwerk benötigt, einschließlich der unterstützten Authentifizierungsmethoden und des VPN-Servers, mit dem das Gerät eine Verbindung herstellen soll. Änderungen in Windows 10 Anniversary Update, einschließlich bedingtem Zugriff und Single Sign-on, ermöglichen es uns, unser Always-on-VPN-Verbindungsprofil zu erstellen.
- **Bedingter Zugriff in Azure Active Directory:** Sicherheit ist bei Organisationen, die die Cloud nutzen, ein Hauptanliegen. Ein wichtiger Aspekt der cloudsicherheit ist die Identität und der Zugriff bei der Verwaltung Ihrer cloudressourcen. In einer mobilen, cloudbasierten Welt können Benutzer über eine Vielzahl von Geräten und apps von überall aus auf die Ressourcen Ihrer Organisation zugreifen. Daher reicht es nicht aus, sich auf eine Ressource zu konzentrieren, die auf eine Ressource zugreifen kann. Um das Gleichgewicht zwischen Sicherheit und Produktivität zu meistern, müssen IT-Experten auch berücksichtigen, wie auf eine Ressource über eine Zugriffs Steuerungs Entscheidung zugegriffen wird.
- **VPN und bedingter Zugriff:** der VPN-Client ist jetzt in der Lage, die cloudbasierte Plattform für den bedingten Zugriff zu integrieren, um eine Geräte Kompatibilitäts Option für Remote Clients bereitzustellen. Beim bedingten Zugriff handelt es sich um ein richtlinienbasiertes Auswertungsmodul, mit dem Sie Zugriffsregeln für alle mit Azure Active Directory (Azure AD) verknüpften Anwendungen erstellen können.

# Schritt 7.1. Konfigurieren von EAP-TLS, um ignorieren (Certificate Revocation List, CRL) überprüfen

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 7: Optionale Bedingter Zugriff für VPN-Konnektivität mithilfe von Azure AD](#)
- [Weiter: Schritt 7,2. Stamm Zertifikate für die VPN-Authentifizierung mit Azure AD erstellen](#)

## IMPORTANT

Wenn diese Registrierungs Änderung nicht implementiert wird, treten bei IKEv2-Verbindungen mit cloudzertifikaten mit PEAP Fehler auf, aber IKEv2-Verbindungen mit Client Authentifizierungs Zertifikaten, die von der lokalen Zertifizierungsstelle ausgestellt werden, funktionieren weiterhin.

In diesem Schritt können Sie **IgnoreNoRevocationCheck** hinzufügen und festlegen, dass die Authentifizierung von Clients zulässig ist, wenn das Zertifikat keine CRL-Verteilungs Punkte enthält. Standardmäßig ist IgnoreNoRevocationCheck auf 0 (deaktiviert) festgelegt.

## NOTE

Wenn ein Windows-Routing-und Remote Zugriffs Server (RRAS) NPS zum Proxy von RADIUS-Aufrufen an einen zweiten NPS verwendet, müssen Sie auf beiden Servern **IgnoreNoRevocationCheck = 1** festlegen.

Ein EAP-TLS-Client kann keine Verbindung herstellen, es sei denn, der NPS-Server schließt eine Sperr Überprüfung der Zertifikat Kette (einschließlich des Stamm Zertifikats) ab. Cloud-Zertifikate, die von Azure AD an den Benutzer ausgegeben werden, verfügen nicht über eine Zertifikat Sperr Liste, da es sich um kurzlebige Zertifikate mit einer Lebensdauer von einer Stunde handelt. EAP auf NPS muss so konfiguriert werden, dass das Fehlen einer CRL ignoriert wird. Standardmäßig ist IgnoreNoRevocationCheck auf 0 (deaktiviert) festgelegt. Fügen Sie IgnoreNoRevocationCheck hinzu, und legen Sie es auf 1 fest, um die Authentifizierung von Clients zuzulassen, wenn das Zertifikat keine CRL-Verteilungs Punkte enthält.

Da die Authentifizierungsmethode EAP-TLS ist, wird dieser Registrierungs Wert nur unter eap\13. benötigt. Wenn andere EAP-Authentifizierungsmethoden verwendet werden, sollte der Registrierungs Wert ebenfalls hinzugefügt werden.

## Dringlichkeit

1. Öffnen Sie " **Regedit. exe** " auf dem NPS-Server.
2. Navigieren Sie zu **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\rasman\PPP\EAP\13**.
3. Wählen Sie **Edit > New** , und wählen Sie **DWORD-Wert (32-Bit)** aus, und geben Sie **IgnoreNoRevocationCheck** ein.
4. Doppelklicken Sie auf **IgnoreNoRevocationCheck** , und legen Sie die Wertdaten auf **1** fest.
5. Wählen Sie **OK** aus, und starten Sie den Server neu. Das Neustarten der RRAS-und NPS-Dienste genügt

nicht.

Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren der Zertifikat Sperr Überprüfung \(CRL\) auf Clients](#).

REGISTRIERUNGSPFAD	EAP-ERWEITERUNG
Hklm\system\currentcontrolset\services\rasman\ppp\ead\13	EAP-TLS
Hklm\system\currentcontrolset\services\rasman\ppp\ead\25	PEAP
Hklm\system\currentcontrolset\services\rasman\ppp\ead\26	EAP-MSCHAP V2

## Nächste Schritte

[Schritt 7.2. Erstellen von Stamm Zertifikaten für die VPN-Authentifizierung mit Azure AD:](#) in diesem Schritt konfigurieren Sie Stamm Zertifikate für den bedingten Zugriff für die VPN-Authentifizierung mit Azure AD, bei der automatisch eine VPN-Server-Cloud-App im Mandanten erstellt wird.

# Schritt 7.2: Erstellen von Stamm Zertifikaten für den bedingten Zugriff für die VPN-Authentifizierung mit Azure AD

27.05.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 7.1. Konfigurieren von EAP-TLS zum Ignorieren der CRL-Überprüfung \(Zertifikat Sperr Liste\)](#)
- [Weiter: Schritt 7.3. Konfigurieren der Richtlinie für bedingten Zugriff](#)

In diesem Schritt konfigurieren Sie die Stamm Zertifikate für den bedingten Zugriff für die VPN-Authentifizierung mit Azure AD, wodurch automatisch eine Cloud-App mit dem Namen VPN-Server im Mandanten erstellt wird. Erforderliche Schritte zum Konfigurieren des bedingten Zugriffs für VPN-Verbindungen:

1. Erstellen eines VPN-Zertifikats über das Azure-Portal
2. Herunterladen des VPN-Zertifikats
3. Stellen Sie das Zertifikat für Ihre VPN-und NPS-Server bereit.

## IMPORTANT

Sobald ein VPN-Zertifikat in der Azure-Portal erstellt wurde, wird es von Azure AD sofort verwendet, um dem VPN-Client kurzlebige Zertifikate auszustellen. Es ist wichtig, dass das VPN-Zertifikat sofort auf dem VPN-Server bereitgestellt wird, um Probleme mit der Überprüfung der Anmelde Informationen des VPN-Clients zu vermeiden.

Wenn ein Benutzer versucht, eine VPN-Verbindung herzustellen, ruft der VPN-Client den Webkonto-Manager (WAM) auf dem Windows 10-Client auf. WAM Ruft die VPN-Server-Cloud-App auf. Wenn die Bedingungen und Steuerelemente in der Richtlinie für bedingten Zugriff erfüllt sind, stellt Azure AD ein Token in Form eines kurzlebigen Zertifikats (1 Stunde) für das WAM aus. Das Zertifikat wird vom WAM in den Zertifikat Speicher des Benutzers eingefügt, und die Steuerung wird an den VPN-Client weitergeleitet.

Der VPN-Client sendet die Zertifikat Probleme dann an das VPN, um die Überprüfung der Anmelde Informationen durch Azure AD.

## NOTE

Azure AD verwendet das zuletzt erstellte Zertifikat auf dem Blatt VPN-Konnektivität als Aussteller.

## Dringlichkeit

1. Melden Sie sich als globaler Administrator beim [Azure-Portal](#) an.
2. Klicken Sie im linken Menü auf **Azure Active Directory**.
3. Klicken Sie auf der Seite **Azure Active Directory** im Abschnitt **Verwalten** auf **Sicherheit**.
4. Klicken Sie auf der Seite **Sicherheit** im Abschnitt **Schutz** auf **bedingter Zugriff**.
5. Bei **\*\*bedingtem Zugriff | \*\*Auf der Seite Richtlinien im Abschnitt **Verwalten** auf **VPN-Konnektivität**.**
6. Klicken Sie auf der Seite **VPN-Konnektivität** auf **Neues Zertifikat**.

7. Führen Sie auf der Seite **neu** die folgenden Schritte aus: a. Wählen Sie für **Select Duration** entweder 1, 2 oder 3 Jahre aus. b. Klicken Sie auf **Erstellen**.

## Nächste Schritte

[Schritt 7,3. Konfigurieren der Richtlinie für bedingten Zugriff:](#) in diesem Schritt konfigurieren Sie die Richtlinie für den bedingten Zugriff für VPN-Konnektivität.

# Schritt 7.3. Konfigurieren der Richtlinie für bedingten Zugriff

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 7.2. Stamm Zertifikate für die VPN-Authentifizierung mit Azure AD erstellen](#)
- [Weiter: Schritt 7.4. Bereitstellen von Stamm Zertifikaten für den bedingten Zugriff im lokalen AD](#)

In diesem Schritt konfigurieren Sie die Richtlinie für bedingten Zugriff für VPN-Konnektivität. Wenn das erste Stamm Zertifikat auf dem Blatt "VPN-Konnektivität" erstellt wird, wird automatisch eine "VPN Server"-cloudanwendung im Mandanten erstellt.

Erstellen Sie eine Richtlinie für bedingten Zugriff, die der Gruppe "VPN-Benutzer" zugewiesen ist, und legen Sie den Bereich der Cloud-App

- **Benutzer:** VPN-Benutzer
- **Cloud-App:** VPN-Server
- **Grant (Zugriffs Steuerung) :** "Multi-Factor Authentication erforderlich". Andere Steuerelemente können bei Bedarf verwendet werden.

**Prozedur:** In diesem Schritt wird die Erstellung der grundlegendsten Richtlinie für den bedingten Zugriff behandelt. Wenn gewünscht, können zusätzliche Bedingungen und Steuerelemente verwendet werden.

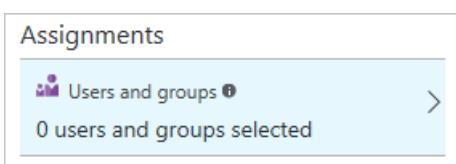
1. Wählen Sie auf der Seite **bedingter Zugriff** auf der Symbolleiste am oberen Rand die Option **Hinzufügen**.



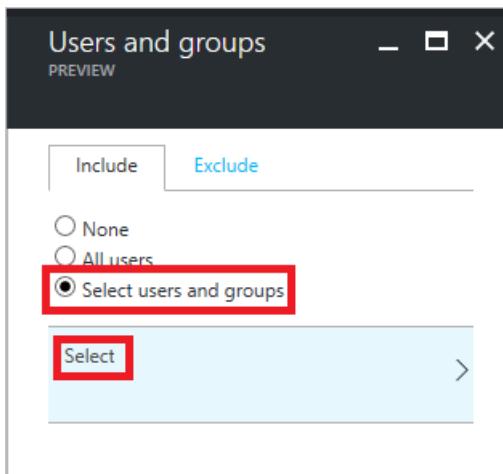
2. Geben Sie auf der Seite **neu** im Feld **Name** einen Namen für die Richtlinie ein. Geben Sie z. b. **VPN-Richtlinie** ein.



3. Wählen Sie im Abschnitt **Zuweisung** die Option **Benutzer und Gruppen**.



4. Führen Sie auf der Seite **Benutzer und Gruppen** die folgenden Schritte aus:



a. Wählen Sie **Benutzer und Gruppen auswählen** aus.

b. Wählen Sie **auswählen** aus.

c. Wählen Sie auf der Seite **auswählen** die Gruppe **VPN-Benutzer** aus, und wählen Sie dann **auswählen** aus.

d. Wählen Sie auf der Seite **Benutzer und Gruppen** die Option **abgeschlossen** aus.

5. Führen Sie auf der Seite **neu** die folgenden Schritte aus:

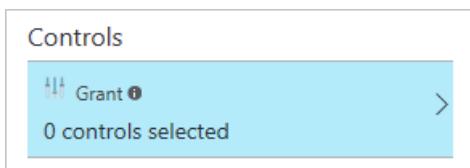
The screenshot displays three sequential configuration steps. The first step, 'New', includes fields for 'Name' (set to 'VPN policy') and 'Assignments' (with a 'Cloud apps' section). The second step, 'Cloud apps', allows selecting cloud applications, with 'Select apps' chosen and 'Select None' highlighted. The third step, 'Select Cloud apps', lists available applications like 'vpn' and 'VS VPN Server'.

a. Wählen Sie im Abschnitt **Zuweisungen** die Option **Cloud-apps** aus.

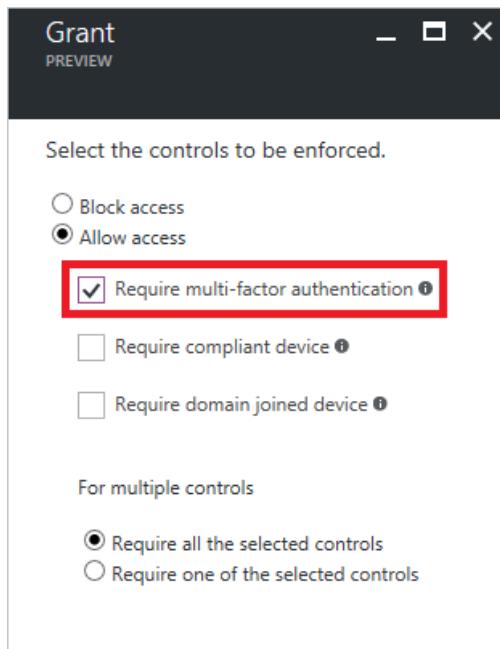
b. Wählen Sie auf der Seite **Cloud-apps** die Option **apps auswählen** aus.

d. Wählen Sie **VPN-Server** aus.

6. Wählen Sie auf der Seite **neu** im Abschnitt **Steuer Elemente** die Option **erteilen aus**, um die Seite **erteilen** zu öffnen.



7. Führen Sie auf der Seite **Grant** die folgenden Schritte aus:



a. Wählen Sie Multi-Factor Authentication erforderlich aus.

b. Wählen Sie auswählen aus.

8. Wählen Sie auf der Seite neu unter Richtlinie aktivierend die Option ein aus.



9. Wählen Sie auf der Seite neu die Option Erstellen aus.

## Nächste Schritte

**Schritt 7.4.** Bereitstellen von Stamm Zertifikaten für den bedingten Zugriff im lokalen AD: in diesem Schritt stellen Sie das Stamm Zertifikat für den bedingten Zugriff als vertrauenswürdiges Stamm Zertifikat für die VPN-Authentifizierung in Ihrem lokalen AD bereit.

# Schritt 7.4. Bereitstellen von Stamm Zertifikaten für den bedingten Zugriff im lokalen AD

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

In diesem Schritt stellen Sie das Stamm Zertifikat für den bedingten Zugriff als vertrauenswürdiges Stamm Zertifikat für die VPN-Authentifizierung in Ihrem lokalen AD bereit.

- [Vorheriges: Schritt 7.3. Konfigurieren der Richtlinie für bedingten Zugriff](#)
- [Weiter: Schritt 7.5. Erstellen von OMA-DM-basierten VPnv2-Profilen für Windows 10-Geräte](#)

1. Wählen Sie auf der Seite **VPN-Konnektivität** die Option **Zertifikat herunterladen** aus.

#### NOTE

Die Option **Base64-Zertifikat herunterladen** ist für einige Konfigurationen verfügbar, die für die Bereitstellung Base64-Zertifikate erfordern.

2. Melden Sie sich bei einem in die Domäne eingebundenen Computer mit Unternehmens Administratorrechten an, und führen Sie diese Befehle an einer Administrator Eingabeaufforderung aus, um die Cloud-Stamm Zertifikate dem *Enterprise NTAuth*-Speicher hinzuzufügen:

#### NOTE

Für Umgebungen, in denen der VPN-Server nicht mit der Active Directory Domäne verknüpft ist, müssen die Stamm Zertifikate der Cloud manuell zum Speicher der *vertrauenswürdigen Stamm Zertifizierungsstellen* hinzugefügt werden.

BEFEHL	BESCHREIBUNG
<code>certutil -dspublish -f VpnCert.cer RootCA</code>	Erstellt zwei Container der Generation 1 der <b>Microsoft-VPN</b> -Stamm Zertifizierungsstellen unter den Containern <b>CN = AIA</b> und <b>CN = Certification Autoritäten</b> und veröffentlicht jedes Stamm Zertifikat als Wert für das Attribut <i>cACertificate</i> der beiden Container der Microsoft-VPN-Stamm Zertifizierungsstelle Gen 1 .
<code>certutil -dspublish -f VpnCert.cer NTAuthCA</code>	Erstellt einen <b>CN = ntauthcertificate</b> -Container unter den Containern <b>CN = AIA</b> und <b>CN = Certification Autoritäten</b> und veröffentlicht jedes Stamm Zertifikat als Wert für das <i>cACertificate</i> -Attribut des <b>CN = ntauthcertificate</b> -Containers.
<code>gpupdate /force</code>	Hiermit wird das Hinzufügen der Stamm Zertifikate zu den Windows Server- und Client Computern beschleunigt.

3. Vergewissern Sie sich, dass die Stamm Zertifikate im Enterprise NTAuth-Speicher vorhanden sind und als vertrauenswürdig angezeigt werden:

- a. Melden Sie sich bei einem Server mit Unternehmens Administratorrechten an, auf dem die **Verwaltungs Tools** für die Zertifizierungsstelle installiert sind.

**NOTE**

Die Zertifizierungsstellen- **Verwaltungs Tools** werden standardmäßig als Zertifizierungsstellen Server installiert. Sie können auf anderen Mitglieds Servern als Teil der Rollen **Verwaltungs Tools** in Server-Manager installiert werden.

- a. Geben Sie auf dem VPN-Server im Startmenü **PKIView. msc** ein, um das Dialogfeld Unternehmens-PKI zu öffnen.
- b. Geben Sie im Startmenü **PKIView. msc** ein, um das Dialogfeld Unternehmens-PKI zu öffnen.
- c. Klicken Sie mit der rechten Maustaste auf **Enterprise PKI**, und wählen Sie die Option **Verwalten**
- d. Stellen Sie sicher, dass jedes Zertifikat der Microsoft-VPN-Stamm Zertifizierungsstelle Gen 1 unter:
  - NTAuthCertificates
  - AIA-Container
  - Zertifizierungsstellen Container

## Nächste Schritte

[Schritt 7.5. Erstellen von OMA-DM-basierten VPnv2-Profilen für Windows 10-Geräte](#): in diesem Schritt können Sie OMA-DM-basierte VPnv2-Profile mithilfe von InTune erstellen, um eine VPN-Geräte Konfigurationsrichtlinie bereitzustellen. Wenn Sie zum Erstellen von VPnv2-Profilen Microsoft-Endpunkt Configuration Manager oder PowerShell-Skript verwenden möchten, finden Sie weitere Informationen unter [VPnv2 CSP Settings](#).

# Schritt 7.5: Erstellen von OMA-DM-basierten VPNV2-Profilen für Windows 10-Geräte

21.05.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

- [Vorheriges: Schritt 7.4. Bereitstellen von Stamm Zertifikaten für den bedingten Zugriff im lokalen AD](#)
- [Weiter: Erfahren Sie, wie der bedingte Zugriff für VPN funktioniert.](#)

In diesem Schritt können Sie OMA-DM-basierte VPNV2-Profilen mithilfe von InTune erstellen, um eine VPN-Geräte Konfigurationsrichtlinie bereitzustellen. Wenn Sie zum Erstellen von VPNV2-Profilen Microsoft-Endpunkt Configuration Manager oder PowerShell-Skript verwenden möchten, finden Sie weitere Informationen unter [VPNV2 CSP Settings](#).

## Verwaltete Bereitstellung mit InTune

Alles, was in diesem Abschnitt erläutert wird, ist die Mindestanforderung, um VPN mit bedingtem Zugriff zu arbeiten. Das Aufteilen von Tunneln, das Verwenden von WIP, das Erstellen von benutzerdefinierten InTune-Geräte Konfigurations Profilen zum Herstellen von autovpn oder das einmalige Anmelden (SSO) wird nicht behandelt. Integrieren Sie die folgenden Einstellungen in das VPN-Profil, das Sie zuvor in [Schritt 5 erstellt haben](#).

[Konfigurieren Sie Windows 10-Client Always on-VPN-Verbindungen](#). In diesem Beispiel integrieren wir Sie in das [Konfigurieren des VPN-Clients mithilfe der InTune -Richtlinie](#).

### Setzung

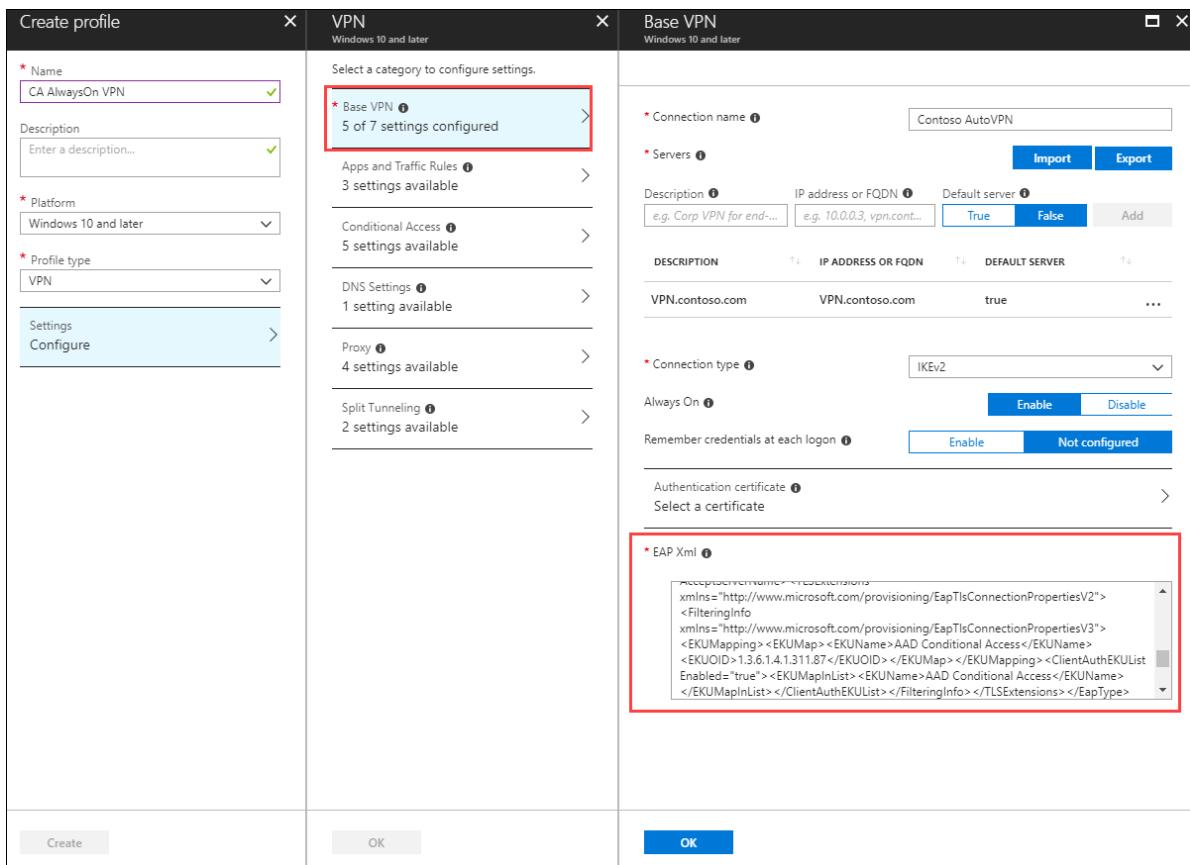
Der Windows 10-Client Computer wurde bereits mit einer VPN-Verbindung mithilfe von InTune konfiguriert.

### Dringlichkeit

1. Wählen Sie im Azure-Portal die Option **InTune > -Geräte Konfigurations > profile** aus, und wählen Sie das VPN-Profil aus, das Sie zuvor unter [Konfigurieren des VPN-Clients mit InTune](#) erstellt haben.
2. Wählen Sie im Richtlinien-Editor die Option **Eigenschaften > Einstellungen > Basis-VPN** aus. Erweitern Sie den vorhandenen **EAP-XML** -Code so, dass er einen Filter enthält, der dem VPN-Client die erforderliche Logik zum Abrufen des Aad-bedingten Zugriffs Zertifikats aus dem Zertifikat Speicher des Benutzers bietet, anstatt es zu erlauben, das erste erkannte Zertifikat zu verwenden.

### NOTE

Ohne diesen Fehler könnte der VPN-Client das von der lokalen Zertifizierungsstelle ausgegebene Benutzerzertifikat abrufen, was zu einer fehlgeschlagenen VPN-Verbindung führt.

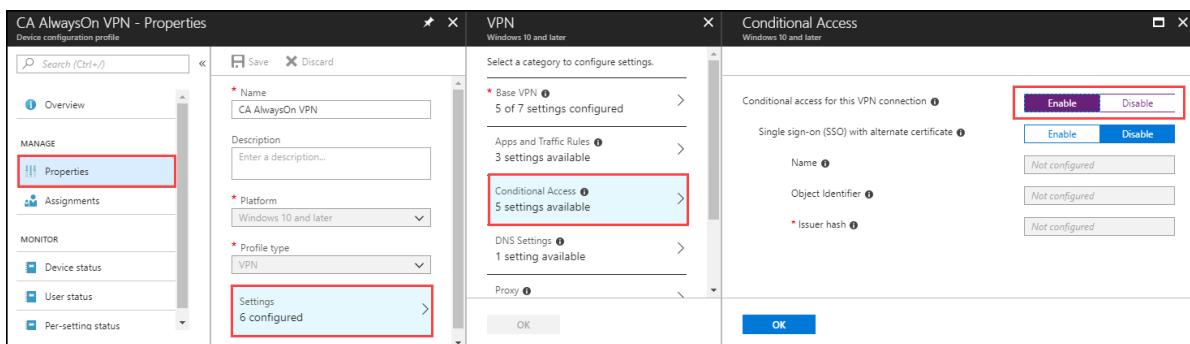


3. Suchen Sie den Abschnitt, der mit \*\* < /AcceptServerName> < /EapType>\*\* endet, und fügen Sie die folgende Zeichenfolge zwischen diesen beiden Werten ein, um dem VPN-Client die Logik zur Auswahl des Aad-bedingten Zugriffs Zertifikats bereitzustellen:

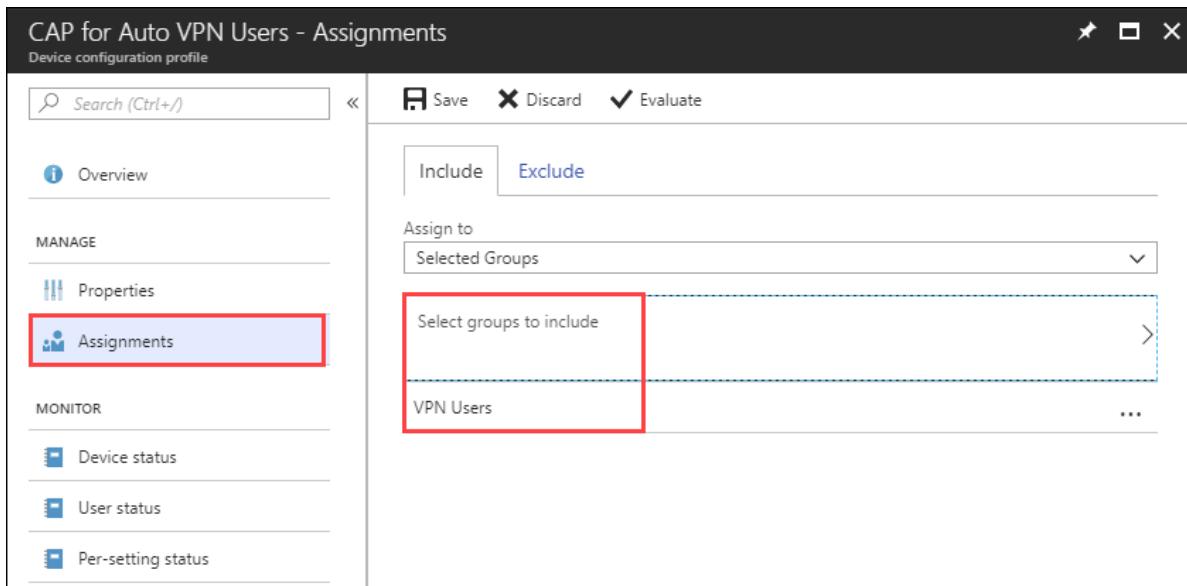
```
<TLSExtensions xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">
<FilteringInfo xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV3"><EKUMapping>
<EKUMap><EKUName>AAD Conditional Access</EKUName><EKUID>1.3.6.1.4.1.311.87</EKUID></EKUMap>
</EKUMapping><ClientAuthEKUList Enabled="true"><EKUMapInList><EKUName>AAD Conditional Access</EKUName>
</EKUMapInList></ClientAuthEKUList></FilteringInfo></TLSExtensions>
```

4. Wählen Sie das Blatt für den bedingten Zugriff aus, und schalten Sie den bedingten Zugriff für diese VPN-Verbindung auf **aktiviert**um.

Wenn Sie diese Einstellung aktivieren, wird die Einstellung \*\* < devicecompliance> < aktiviert>true < /Enabled #d2\*\* in der VPNv2-Profil-XML geändert.



5. Wählen Sie **OK** aus.
6. Wählen Sie **Zuweisungen** unter **einbeziehen** aus, und wählen Sie **Gruppen auswählen**, die eingeschlossen werden sollen.
7. Wählen Sie die Gruppe **VPN-Benutzer** aus, die diese Richtlinie empfängt, und wählen Sie **Speichern**



## Erzwingen der MDM-Richtlinien Synchronisierung auf dem Client

Wenn das VPN-Profil auf dem Client Gerät nicht angezeigt wird, \ können Sie unter Einstellungen Netzwerk & Internet- \ VPN erzwingen, dass die MDM-Richtlinie synchronisiert wird.

1. Melden Sie sich bei einem in die Domäne eingebundenen Client Computer als Mitglied der Gruppe "VPN-Benutzer" an.
2. Geben Sie im Startmenü Accountein, und drücken Sie die EINGABETASTE.
3. Klicken Sie im linken Navigationsbereich auf Arbeits- oder Schul Konto zugreifen.
4. Wählen Sie unter Arbeitsplatz oder Schule zugreifen die Option verbunden mit < \domäne> MDMAus, und wählen Sie dann Infoaus.
5. Wählen Sie Synchronisieren aus, und vergewissern Sie sich, dass das VPN-Profil unter Einstellungen \ Netzwerk & Internet- \ VPN

## Nächste Schritte

Sie haben die Konfiguration des VPN-Profs für die Verwendung Azure AD bedingten Zugriffs abgeschlossen.

ZWECK	WEITERE INFORMATIONEN FINDEN SIE UNTER...
Weitere Informationen zur Funktionsweise des bedingten Zugriffs mit VPNs	<a href="#">VPN und bedingter Zugriff</a> : auf dieser Seite finden Sie weitere Informationen dazu, wie der bedingte Zugriff mit VPNs funktioniert.
Weitere Informationen zu den erweiterten VPN-Features	<a href="#">Erweiterte VPN-Features</a> : auf dieser Seite finden Sie Anleitungen zum Aktivieren von VPN-Datenverkehrs filtern, zum Konfigurieren automatischer VPN-Verbindungen mithilfe von App-Triggern und zum Konfigurieren von NPS für das Zulassen von VPN-Verbindungen von Clients mithilfe von Zertifikaten, die von Azure AD ausgestellt wurden.

## Zugehörige Themen

- [VPnv2 CSP](#): in diesem Thema erhalten Sie einen Überblick über VPnv2 CSP. Der VPnv2-Konfigurations Dienstanbieter ermöglicht dem MDM-Server, das VPN-Profil des Geräts zu konfigurieren.

- [Konfigurieren von Windows 10-Client-Always on-VPN-Verbindungen](#): dieses Thema enthält Informationen zu den profileXML-Optionen und-Schemas sowie zum Erstellen des profileXML-VPN. Nachdem Sie die Serverinfrastruktur eingerichtet haben, müssen Sie die Windows 10-Client Computer für die Kommunikation mit dieser Infrastruktur über eine VPN-Verbindung konfigurieren.
- [Konfigurieren des VPN-Clients mithilfe von InTune](#): dieses Thema enthält Informationen zum Bereitstellen von Windows 10-RAS-Always on VPN-Profilen. InTune verwendet nun Azure Ad Gruppen. Wenn Azure AD Connect die Gruppe "VPN-Benutzer" vom lokalen Standort zu "Azure AD" synchronisieren, ist es nicht erforderlich, den VPN-Client mit InTune zu konfigurieren.

# Problembehandlung bei Always On VPN

09.04.2020 • 20 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal), Windows Server 2016, Windows Server 2012 R2, Windows 10

Wenn Ihr Always on VPN-Setup keine Verbindung zwischen Clients und Ihrem internen Netzwerk herstellt, ist wahrscheinlich ein ungültiges VPN-Zertifikat, falsche NPS-Richtlinien oder Probleme mit den Client Bereitstellungs Skripts oder dem Routing-und RAS-Zugriff aufgetreten. Der erste Schritt bei der Problembehandlung und dem Testen Ihrer VPN-Verbindung ist das Verständnis der Kernkomponenten der Always on-VPN-Infrastruktur.

Sie können Verbindungsprobleme auf verschiedene Arten beheben. Bei Client seitigen Problemen und der allgemeinen Problembehandlung sind die Anwendungsprotokolle auf Client Computern von großer Bedeutung. Bei Authentifizierungs spezifischen Problemen kann das NPS-Protokoll auf dem NPS-Server Ihnen helfen, die Ursache des Problems zu bestimmen.

## Fehlercodes

### Fehlercode: 800

- **Fehlerbeschreibung:** Die Remote Verbindung wurde nicht hergestellt, weil bei den versuchten VPN-Tunneln ein Fehler aufgetreten ist. Der VPN-Server ist möglicherweise nicht erreichbar. Wenn diese Verbindung versucht, einen L2TP/IPSec-Tunnel zu verwenden, sind die für die IPsec-Aushandlung erforderlichen Sicherheitsparameter möglicherweise nicht ordnungsgemäß konfiguriert.
- **Mögliche Ursache:** Dieser Fehler tritt auf, wenn der VPN-Tunneltyp **automatisch** ist und der Verbindungsversuch für alle VPN-Tunnel fehlschlägt.
- **Mögliche Lösungen:**
  - Wenn Sie wissen, welcher Tunnel für Ihre Bereitstellung verwendet werden soll, legen Sie den Typ des VPN auf den jeweiligen Tunneltyp auf der VPN-Clientseite fest.
  - Wenn Sie eine VPN-Verbindung mit einem bestimmten Tunneltyp herstellen, schlägt die Verbindung weiterhin fehl, dies führt jedoch zu einem fehlerhaften Tunnel spezifischen Fehler (z. b. "GRE blockiert für PPTP").
  - Dieser Fehler tritt auch auf, wenn der VPN-Server nicht erreicht werden kann oder die Tunnelverbindung nicht hergestellt werden kann.
- **Stelle sicher:**
  - IKE-Ports (UDP-Ports 500 und 4500) sind nicht blockiert.
  - Die richtigen Zertifikate für IKE sind sowohl auf dem Client als auch auf dem Server vorhanden.

### Fehlercode: 809

- **Fehlerbeschreibung:** Die Netzwerkverbindung zwischen Ihrem Computer und dem VPN-Server konnte nicht hergestellt werden, da der Remote Server nicht antwortet. Dies liegt möglicherweise daran, dass eines der Netzwerkgeräte (z. b. Firewalls, NAT, Router) zwischen Ihrem Computer und dem Remote Server nicht für das Zulassen von VPN-Verbindungen konfiguriert ist. Wenden Sie sich an Ihren Administrator oder an Ihren Dienstanbieter, um zu ermitteln, welches Gerät das Problem möglicherweise verursacht.
- **Mögliche Ursache:** Dieser Fehler wird durch blockierte UDP 500-oder 4500-Ports auf dem VPN-Server oder der Firewall verursacht.

- **Mögliche Lösung.** Stellen Sie sicher, dass die UDP-Ports 500 und 4500 durch alle Firewalls zwischen dem Client und dem RRAS-Server zulässig sind.

#### **Fehlercode: 812**

- **Fehlerbeschreibung.** Es kann keine Verbindung mit Always on VPN hergestellt werden. Die Verbindung wurde aufgrund einer Richtlinie, die auf Ihrem RAS/VPN-Server konfiguriert wurde, verhindert. Die Authentifizierungsmethode, die der Server zum Überprüfen Ihres Benutzernamens und Kennworts verwendet hat, stimmt möglicherweise nicht mit der Authentifizierungsmethode, die in Ihrem Verbindungsprofil konfiguriert wurde. Wenden Sie sich an den Administrator des RAS-Servers, und Benachrichtigen Sie ihn über diesen Fehler.
- **Mögliche Ursachen:**
  - Die typische Ursache für diesen Fehler ist, dass der NPS eine Authentifizierungs Bedingung angegeben hat, die der Client nicht erfüllen kann. Beispielsweise kann der NPS die Verwendung eines Zertifikats zum Sichern der PEAP-Verbindung angeben, aber der Client versucht, EAP-MSCHAPv2 zu verwenden.
  - Das Ereignisprotokoll 20276 wird in der Ereignisanzeige protokolliert, wenn die Einstellung RRAS-basiertes VPN-Server-Authentifizierungsprotokoll nicht mit der des VPN-Client Computers identisch ist.
- **Mögliche Lösung.** Stellen Sie sicher, dass Ihre Client Konfiguration mit den Bedingungen übereinstimmt, die auf dem NPS-Server angegeben sind.

#### **Fehlercode: 13806**

- **Fehlerbeschreibung.** Ein gültiges Computer Zertifikat konnte von IKE nicht gefunden werden. Wenden Sie sich an den Netzwerk Sicherheitsadministrator, um ein gültiges Zertifikat im entsprechenden Zertifikat Speicher zu installieren.
- **Mögliche Ursache:** Dieser Fehler tritt normalerweise auf, wenn auf dem VPN-Server kein Computer Zertifikat oder Stamm Computer Zertifikat vorhanden ist.
- **Mögliche Lösung.** Stellen Sie sicher, dass die in dieser Bereitstellung beschriebenen Zertifikate sowohl auf dem Client Computer als auch auf dem VPN-Server installiert sind.

#### **Fehlercode: 13801**

- **Fehlerbeschreibung.** Die Anmelde Informationen für die IKE-Authentifizierung sind unzulässig.
- **Mögliche Ursachen.** Dieser Fehler tritt in der Regel in einem der folgenden Fälle auf:
  - Das Computer Zertifikat, das für die IKEv2-Überprüfung auf dem RAS-Server verwendet wird, verfügt über keine **Server Authentifizierung mit Verbesserter Schlüssel Verwendung**
  - Das Computer Zertifikat auf dem RAS-Server ist abgelaufen.
  - Das Stamm Zertifikat zum Überprüfen des RAS-Serverzertifikats ist auf dem Client Computer nicht vorhanden.
  - Der auf dem Client Computer verwendete VPN-Servername stimmt nicht mit dem **subjectname** des Serverzertifikats identisch.
- **Mögliche Lösung.** Stellen Sie sicher, dass das Serverzertifikat unter **Erweiterte Schlüssel Verwendung** eine **Server Authentifizierung** enthält. Vergewissern Sie sich, dass das Serverzertifikat noch gültig ist. Vergewissern Sie sich, dass die verwendete Zertifizierungsstelle unter **Vertrauenswürdige Stamm Zertifizierungsstellen** auf dem RRAS-Server aufgeführt ist. Überprüfen Sie, ob der VPN-Client eine Verbindung mit dem voll qualifizierten Namen des VPN-Servers herstellt, wie im Zertifikat des VPN-Servers dargestellt.

### **Fehlercode: 0x80070040**

- **Fehlerbeschreibung.** Das Serverzertifikat verfügt nicht über eine **Server Authentifizierung** als eine seiner Zertifikat Verwendungs Einträge.
- **Mögliche Ursache:** Dieser Fehler kann auftreten, wenn auf dem RAS-Server kein Server Authentifizierungszertifikat installiert ist.
- **Mögliche Lösung.** Stellen Sie sicher, dass das Computer Zertifikat, das der RAS-Server für **IKEv2** verwendet, als eine der Zertifikat Verwendungs Einträge **Server Authentifizierung** verwendet.

### **Fehlercode: 0x800B0109**

Im Allgemeinen wird der VPN-Client Computer mit der Active Directory – basierten Domäne verknüpft. Wenn Sie Domänen Anmelde Informationen für die Anmeldung beim VPN-Server verwenden, wird das Zertifikat automatisch im Speicher Vertrauenswürdige Stamm Zertifizierungsstellen installiert. Wenn der Computer jedoch nicht der Domäne hinzugefügt wird oder wenn Sie eine Alternative Zertifikat Kette verwenden, kann dieses Problem auftreten.

- **Fehlerbeschreibung.** Eine Zertifikat Kette wurde verarbeitet, aber in einem Stamm Zertifikat beendet, dem der Vertrauens Anbieter nicht vertraut.
- **Mögliche Ursache:** Dieser Fehler kann auftreten, wenn das entsprechende Zertifikat der vertrauenswürdigen Stamm Zertifizierungsstelle nicht im Speicher für vertrauenswürdige Stamm Zertifizierungsstellen auf dem Client Computer installiert ist.
- **Mögliche Lösung.** Stellen Sie sicher, dass das Stamm Zertifikat auf dem Client Computer im Speicher vertrauenswürdiger Stamm Zertifizierungsstellen installiert ist.

## Protokolle

### **Anwendungsprotokolle**

In den Anwendungs Protokollen auf Client Computern wird der größte Teil der Details der VPN-Verbindungs Ereignisse auf höherer Ebene aufgezeichnet.

Suchen Sie nach Ereignissen aus der Quelle RasClient. Alle Fehlermeldungen geben den Fehlercode am Ende der Nachricht zurück. Einige der gängigeren Fehlercodes sind unten aufgeführt, aber eine vollständige Liste ist in den [Routing-und RAS-Fehlercodes](#) verfügbar.

### NPS-Protokolle

NPS erstellt und speichert die NPS-Buchhaltungs Protokolle. Standardmäßig werden diese in%  
SystemRoot%\System32\Logfiles\ in einer Datei namens inxxxx.txt gespeichert, wobei xxxx das Datum ist, an dem die Datei erstellt wurde.

Standardmäßig sind diese Protokolle im Format für durch Trennzeichen getrennte Werte enthalten, Sie enthalten jedoch keine Überschriften Zeile. Die Überschriften Zeile lautet:

```
ComputerName,ServiceName,Record-Date,Record-Time,Packet-Type,User-Name,Fully-Qualified-Distinguished-Name,Called-Station-ID,Calling-Station-ID,Callback-Number,Framed-IP-Address,NAS-Identifier,NAS-IP-Address,NAS-Port,Client-Vendor,Client-IP-Address,Client-Friendly-Name,Event-Timestamp,Port-Limit,NAS-Port-Type,Connect-Info,Framed-Protocol,Service-Type,Authentication-Type,Policy-Name,Reason-Code,Class,Session-Timeout,Idle-Timeout,Termination-Action,EAP-Friendly-Name,Acct-Status-Type,Acct-Delay-Time,Acct-Input-Octets,Acct-Output-Octets,Acct-Session-Id,Acct-Authentic,Acct-Session-Time,Acct-Input-Packets,Acct-Output-Packets,Acct-Terminate-Cause,Acct-Multi-Ssn-ID,Acct-Link-Count,Acct-Interim-Interval,Tunnel-Type,Tunnel-Medium-Type,Tunnel-Client-Endpt,Tunnel-Server-Endpt,Acct-Tunnel-Conn,Tunnel-Pvt-Group-ID,Tunnel-Assignment-ID,Tunnel-Preference,MS-Acct-Auth-Type,MS-Acct-EAP-Type,MS-RAS-Version,MS-RAS-Vendor,MS-CHAP-Error,MS-CHAP-Domain,MS-MPPE-Encryption-Types,MS-MPPE-Encryption-Policy,Proxy-Policy-Name,Provider-Type,Provider-Name,Remote-Server-Address,MS-RAS-Client-Name,MS-RAS-Client-Version
```

Wenn Sie diese Überschriften Zeile als erste Zeile der Protokolldatei einfügen und die Datei dann in Microsoft Excel importieren, werden die Spalten ordnungsgemäß bezeichnet.

Die NPS-Protokolle können bei der Diagnose von Richtlinien bezogenen Problemen hilfreich sein. Weitere Informationen zu NPS-Protokollen finden Sie unter [Interpretieren von NPS-Daten Bank Format-Protokolldateien](#).

## VPN\_Profile.ps1-Skript Probleme

Die häufigsten Probleme beim manuellen Ausführen des VPN\_Profile.ps1-Skripts umfassen Folgendes:

- Verwenden Sie ein Remote Verbindungs Tool? Stellen Sie sicher, dass Sie RDP oder eine andere Remote Verbindungsmethode nicht verwenden, da Sie mit der Erkennung von Benutzer Anmelde Informationen verwendet wird.
- Ist der Benutzer ein Administrator dieses lokalen Computers? Stellen Sie sicher, dass beim Ausführen des Skripts VPN\_Profile.ps1, dass der Benutzer über Administratorrechte verfügt.
- Verfügen Sie über zusätzliche aktivierte PowerShell-Sicherheitsfeatures? Stellen Sie sicher, dass die PowerShell-Ausführungs Richtlinie das Skript nicht blockiert. Vor dem Ausführen des Skripts sollten Sie ggf. den eingeschränkten Modus deaktivieren. Sie können den eingeschränkten Sprachmodus aktivieren, nachdem das Skript erfolgreich abgeschlossen wurde.

## VPN-Client Verbindungsprobleme Always on

Eine geringfügige Fehlkonfiguration kann dazu führen, dass die Client Verbindung fehlschlägt, und die Ursache ist möglicherweise schwierig zu ermitteln. Ein Always on-VPN-Client durchläuft mehrere Schritte, bevor eine Verbindung hergestellt wird. Gehen Sie bei der Problembehandlung von Client Verbindungsproblemen wie folgt vor:

1. Ist der Vorlagen Computer extern verbunden? Ein **whatismyip** -Scan sollte eine öffentliche IP-Adresse anzeigen, die nicht zu Ihnen gehört.
2. Können Sie den Remote Zugriff/VPN-Servernamen in eine IP-Adresse auflösen? Öffnen Sie in der **Systemsteuerung > Netzwerk -und Internet > Netzwerkverbindungen** die Eigenschaften für das VPN-Profil. Der Wert auf der Registerkarte **Allgemein** sollte durch DNS öffentlich aufgelöst werden können.
3. Können Sie über ein externes Netzwerk auf den VPN-Server zugreifen? Öffnen Sie das ICMP (Internet Control Message Protocol) für die externe Schnittstelle, und Pingen Sie den Namen vom Remote Client. Nachdem ein Ping erfolgreich war, können Sie die ICMP-Zulassungs Regel entfernen.
4. Haben Sie die internen und externen NICs auf dem VPN-Server ordnungsgemäß konfiguriert? Befinden sich diese in unterschiedlichen Subnetzen? Stellt die externe NIC eine Verbindung mit der richtigen Schnittstelle Ihrer Firewall her?
5. Werden UDP 500-und 4500-Ports vom Client für die externe Schnittstelle des VPN-Servers geöffnet? Überprüfen Sie die Client Firewall, die Server Firewall und alle Hardware Firewalls. IPSec verwendet den UDP-Port 500. Stellen Sie daher sicher, dass die IPEC nicht deaktiviert oder an einem beliebigen Speicherort blockiert ist.
6. Schlägt die Zertifikats Überprüfung fehl? Vergewissern Sie sich, dass der NPS-Server über ein Server Authentifizierungszertifikat verfügt, das IKE-Anforderungen bedienen kann. Stellen Sie sicher, dass Sie die richtige VPN-Server-IP-Adresse als NPS-Client angegeben haben. Stellen Sie sicher, dass Sie sich mit PEAP authentifizieren, und die geschützten EAP-Eigenschaften sollten nur die Authentifizierung mit einem Zertifikat zulassen. Sie können die NPS-Ereignisprotokolle auf Authentifizierungsfehler überprüfen. Weitere Informationen finden Sie unter [Installieren und Konfigurieren des NPS-Servers](#).
7. Stellen Sie eine Verbindung her, haben aber keinen Zugriff auf das Internet/lokales Netzwerk? Überprüfen

Sie die IP-Pools des DHCP/VPN-Servers auf Konfigurationsprobleme.

8. Stellen Sie eine Verbindung her und haben eine gültige interne IP-Adresse, haben aber keinen Zugriff auf lokale Ressourcen? Überprüfen Sie, ob Clients wissen, wie Sie zu diesen Ressourcen gelangen. Sie können den VPN-Server zum Weiterleiten von Anforderungen verwenden.

## Azure AD Verbindungsprobleme mit bedingtem Zugriff

**Oops: Sie können dies noch nicht erreichen.**

- **Fehlerbeschreibung.** Wenn die Richtlinie für bedingten Zugriff nicht erfüllt wird, wird die VPN-Verbindung blockiert, jedoch wird eine Verbindung hergestellt, nachdem der Benutzer X zum Schließen der Nachricht ausgewählt hat. Wenn Sie OK auswählen, wird ein anderer Authentifizierungs Versuch ausgelöst, der in einer anderen "Oops"-Meldung endet. Diese Ereignisse werden im Aad-Betriebs Ereignisprotokoll des Clients aufgezeichnet.

- **Mögliche Ursache**

- Der Benutzer verfügt über ein gültiges Client Authentifizierungszertifikat im persönlichen Zertifikat Speicher, das nicht von Azure AD ausgestellt wurde.
- Der Abschnitt VPN-Profil <tlsextensions> ist entweder nicht vorhanden oder enthält nicht den <ekuname> Aad Conditional Access </EKUName> <ekuoid> 1.3.6.1.4.1.311.87 </EKOID> <ekuname > Aad Conditional Access </EKUName> <ekuoid> 1.3.6.1.4.1.311.87 </EKOID> Einträge. Mit den <ekuname > und <ekuoid-> Einträgen wird dem VPN-Client mitgeteilt, welches Zertifikat aus dem Zertifikat Speicher des Benutzers abgerufen werden soll, wenn das Zertifikat an den VPN-Server übergeben wird. Ohne diesen Vorgang verwendet der VPN-Client ein gültiges Client Authentifizierungszertifikat, das sich im Zertifikat Speicher des Benutzers befindet, und die Authentifizierung ist erfolgreich.
- Der RADIUS-Server (NPS) wurde nicht so konfiguriert, dass nur Client Zertifikate akzeptiert werden, die die ID des **bedingten Aad-Zugriffs** enthalten.

- **Mögliche Lösung.** Gehen Sie folgendermaßen vor, um diese Schleife zu verwenden:

1. Führen Sie in Windows PowerShell das Cmdlet **Get-WMIObject** zum Sichern der VPN-Profil Konfiguration aus.
2. Vergewissern Sie sich, dass die Abschnitte <tlsextensions > , <ekuname > und <ekuoid > vorhanden sind, und zeigen Sie den richtigen Namen und die OID an.

```
PS C:\> Get-WmiObject -Class MDM_VPNv2_01 -Namespace root\cimv2\mdm\dmmmap

__GENUS          : 2
__CLASS         : MDM_VPNv2_01
__SUPERCLASS    :
__DYNASTY       : MDM_VPNv2_01
__RELPATH        : MDM_VPNv2_01.InstanceID="AlwaysOnVPN",ParentID=".Vendor/MSFT/VPNv2"
__PROPERTY_COUNT : 10
__DERIVATION     : {}
__SERVER         : DERS2
__NAMESPACE      : root\cimv2\mdm\dmmmap
__PATH           :
\\DERS2\root\cimv2\mdm\dmmmap:MDM_VPNv2_01.InstanceID="AlwaysOnVPN",ParentID=".Vendor/MSFT/VPNv2"
AlwaysOn        :
ByPassForLocal  :
DnsSuffix       :
EdpModeId       :
InstanceID      : AlwaysOnVPN
LockDown        :
```

```

ParentID          : ./Vendor/MsFTI/VPNv2
ProfileXML        : <VPNProfile><RememberCredentials>false</RememberCredentials>
<DeviceCompliance><Enabled>true</Enabled>
                           Enabled><Sso><Enabled>true</Enabled></Sso></DeviceCompliance>
<NativeProfile><Servers>derras2.
                           corp.deverett.info;derras2.corp.deverett.info</Servers>
<RoutingPolicyType>ForceTunnel</RoutingPolicyType>
                           gPolicyType><NativeProtocolType>Ikev2</NativeProtocolType>
<Authentication><UserMethod>Eap</UserMethod>
                           erMethod><MachineMethod>Eap</MachineMethod><Eap><Configuration>
<EapHostConfig
                           xmlns="https://www.microsoft.com/provisioning/EapHostConfig">
<EapMethod><Type
                           xmlns="https://www.microsoft.com/provisioning/EapCommon">25</Type>
<VendorId
                           xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorId>
<VendorType
                           xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorType>
<AuthorId
                           xmlns="https://www.microsoft.com/provisioning/EapCommon">0</AuthorId>
<EapMethod><Config
                           xmlns="https://www.microsoft.com/provisioning/EapHostConfig"><Eap
                           xmlns="https://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"><Type>25</Type>
<EapType xmlns="https://www.mic
                           rosoft.com/provisioning/MsPeapConnectionPropertiesV1">
<ServerValidation><DisableUserPromptFor
                           ServerValidation>true</DisableUserPromptForServerValidation>
<ServerNames></ServerNames><Serv
                           erValidation><FastReconnect>true</FastReconnect>
<InnerEapOptional>false</InnerEapOptional><Ea
                           p
                           xmlns="https://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"><Type>13</Type>
<EapType
                           xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV1"><Credenti
                           alsSource><CertificateStore>
<SimpleCertSelection>true</SimpleCertSelection><CertificateStore
                           ></CertificatesSource><ServerValidation>
<DisableUserPromptForServerValidation>true</DisableUser
                           PromptForServerValidation><ServerNames></ServerNames>
<TrustedRootCA>5a 89 fe cb 5b 49 a7 0b
                           1a 52 63 b7 35 ee d7 1c c2 68 be 4b </TrustedRootCA>
</ServerValidation><DifferentUsername>fa
                           se</DifferentUsername><PerformServerValidation
                           xmlns="https://www.microsoft.com/provisioning/E
                           apTlsConnectionPropertiesV2">true</PerformServerValidation>
<AcceptServerName
                           xmlns="https://ww
                           .microsoft.com/provisioning/EapTlsConnectionPropertiesV2">false</AcceptServerName><TLSExtens
                           ions
                           xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2"><FilteringInfo
                           xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV3"><EKUMapping><EKUMap><
                           EKUName>AAD Conditional
                           Access</EKUName><EKUOID>1.3.6.1.4.1.311.87</EKUOID></EKUMap>
</EKUMapping><ClientAuthEKUL
                           list
                           Enabled="true"><EKUMapInList><EKUName>AAD Conditional
                           Access</EKUName></EKUMapInList></Client
                           AuthEKUList></FilteringInfo></TLSExtensions></EapType></Eap>
<EnableQuarantineChecks>false</En
                           ableQuarantineChecks>
<RequireCryptoBinding>false</RequireCryptoBinding><PeapExtensions><Perfo
                           rmServerValidation
                           xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2"
                           >false</PerformServerValidation><AcceptServerName
                           xmlns="https://www.microsoft.com/provisionin
                           g/MsPeapConnectionPropertiesV2">false</AcceptServerName>
</PeapExtensions></EapType></Eap></Co

```

```
nfig></EapHostConfig></Configuration></Eap></Authentication>
</NativeProfile></VPNProfile>
RememberCredentials      : False
TrustedNetworkDetection :
PSComputerName          : DERS2
```

3. Führen Sie den **certutil** -Befehl aus, um zu bestimmen, ob gültige Zertifikate im Zertifikat Speicher des Benutzers vorhanden sind:

```
C:\>certutil -store -user My

My "Personal"
=====
Serial Number: 32000000265259d0069fa6f205000000000026
Issuer: CN=corp-DEDC0-CA, DC=corp, DC=deverett, DC=info
NotBefore: 12/8/2017 8:07 PM
NotAfter: 12/8/2018 8:07 PM
Subject: E=winfed@deverett.info, CN=WinFed, OU=Users, OU=Corp, DC=corp, DC=deverett, DC=info
Certificate Template Name (Certificate Type): User
Non-root Certificate
Template: User
Cert Hash(sha1): a50337ab015d5612b7dc4c1e759d201e74cc2a93
Key Container = a890fd7fbfc072f8fe045e680c501cf_5834bfa9-1c4a-44a8-a128-c2267f712336
Simple container name: te-User-c7bcc4bd-0498-4411-af44-da2257f54387
Provider = Microsoft Enhanced Cryptographic Provider v1.0
Encryption test passed

=====
Serial Number: 367fbdd7e6e4103dec9b91f93959ac56
Issuer: CN=Microsoft VPN root CA gen 1
NotBefore: 12/8/2017 6:24 PM
NotAfter: 12/8/2017 7:29 PM
Subject: CN=WinFed@deverett.info
Non-root Certificate
Cert Hash(sha1): 37378a1b06dcef1b4d4753f7d21e4f20b18fbfec
Key Container = 31685cae-af6f-48fb-ac37-845c69b4c097
Unique container name: bf4097e20d4480b8d6ebc139c9360f02_5834bfa9-1c4a-44a8-a128-c2267f712336
Provider = Microsoft Software Key Storage Provider
Private key is NOT exportable
Encryption test passed
```

#### NOTE

Wenn ein Zertifikat vom Aussteller **CN = Microsoft VPN Root CA Gen 1** im persönlichen Speicher des Benutzers vorhanden ist, der Benutzer aber durch Auswählen von **X** zum Schließen der oops-Nachricht Zugriff erhalten hat, erfassen Sie CAPI2-Ereignisprotokolle, um zu überprüfen, ob das Zertifikat, das für die Authentifizierung verwendet wurde, ein gültiges Client Authentifizierungszertifikat war, das von der Microsoft-VPN-Stamm Zertifizierungsstelle

4. Wenn ein gültiges Client Authentifizierungszertifikat im persönlichen Speicher des Benutzers vorhanden ist, tritt bei der Verbindung ein Fehler auf (wie), nachdem der Benutzer das **X** ausgewählt hat, und wenn die **<tlsextensions >**, **<ekuname >** und **<ekuoid >** Abschnitte vorhanden sind und die richtigen Informationen enthalten.

Es wird eine Fehlermeldung angezeigt, die besagt, dass ein Zertifikat nicht gefunden werden kann, das mit dem Extensible Authenticate-Protokoll verwendet werden kann.

#### Das Zertifikat kann nicht auf dem Blatt "VPN-Konnektivität" gelöscht werden.

- **Fehlerbeschreibung:** Zertifikate auf dem Blatt "VPN-Konnektivität" können nicht gelöscht werden.
- **Mögliche Ursache:** Das Zertifikat ist auf **primärfestgelegt**.

- Mögliche Lösung.

1. Wählen Sie auf dem Blatt VPN-Konnektivität das Zertifikat aus.
2. Wählen Sie unter **primär** die Option **Nein**, und wählen Sie dann **Speichern** aus.
3. Wählen Sie auf dem Blatt VPN-Konnektivität erneut das Zertifikat aus.
4. Klicken Sie auf **Löschen**.

# Border Gateway Protocol (BGP)

09.04.2020 • 21 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema erhalten Sie Informationen zum Verständnis des Border Gateway Protocol (BGP), einschließlich Bereitstellungstopologien mit BGP-Unterstützung und BGP-Features sowie -Funktionen.

## NOTE

Zusätzlich zu diesem Thema ist die folgende BGP-Dokumentation verfügbar.

- [BGP-Befehlsreferenz für Windows PowerShell](#)

Dieses Thema enthält folgende Abschnitte:

- [BGP-Unterstützte Bereitstellungstopologien](#)
- [BGP-Funktionen](#)

Wenn Sie auf einem Windows Server 2016-RAS-Dienst (RAS) Gateway im mehr Instanzen Modus konfiguriert werden, bietet Border Gateway Protocol (BGP) die Möglichkeit, das Routing von Netzwerk Datenverkehr zwischen den VM-Netzwerken Ihrer Mandanten und den zugehörigen Remote Standorten zu verwalten. Sie können BGP auch für RAS-Gateway-bereit Stellungen mit einem Mandanten verwenden und wenn Sie den Remote Zugriff als lokales Netzwerk (LAN-) Router bereitstellen.

BGP verringert den Bedarf an manueller Routingkonfiguration auf Routern, da es ein dynamisches Routingprotokoll ist, das automatisch Routen zwischen Standorten lernt, die über die Standort-zu-Standort-VPN-Verbindungen verbunden sind.

Wenn Sie das BGP-Routing verwenden möchten, müssen Sie den **RAS-Dienst (RAS-)** und/oder den **Routing** Rollen Dienst der RAS-Server Rolle auf einem Computer oder virtuellen Computer (VM-) installieren. abhängig davon, ob Sie über eine mehr Instanzen fähige Bereitstellung verfügen, ist die Verwendung des verwendeten Systems abhängig davon:

- Bei einer mehr Instanzen fähigen Bereitstellung wird empfohlen, das RAS-Gateway auf einem oder mehreren virtuellen Computern zu installieren. Die Verwendung mehrerer virtueller Computer bietet hohe Verfügbarkeit. Das RAS-Gateway kann mehrere Verbindungen von mehreren Mandanten verarbeiten und besteht aus einem Hyper-V-Host und einem virtuellen Computer, der tatsächlich als Gateway konfiguriert ist. Dieses Gateway ist mit Standort-zu-Standort-VPN-Verbindungen als mehr Instanzen fähiger BGP-Router für Exchange-Mandanten und clouddienstanbieter (CSP) Subnetzrouten konfiguriert.
- Für eine Bereitstellung eines Edge-Gateways mit einem einzelnen Mandanten oder eine LAN-routerbereitstellung können Sie das RAS-Gateway entweder auf einem physischen Computer oder auf einem virtuellen Computer installieren.

## IMPORTANT

Bei der Installation eines RAS-Gateways müssen Sie angeben, ob BGP für jeden Mandanten aktiviert ist, indem Sie den Windows PowerShell -Befehl **enable-remoteaccessroutingdomain** mit dem **Typeparameter** Wert **all** verwenden. Wenn Sie den Remote Zugriff als BGP-fähigen LAN-Router ohne mehr Instanzen fähige Funktionen installieren möchten, können Sie den Befehl **install-remoteaccess-vpntype routingonly** verwenden.

Der folgende Beispielcode veranschaulicht, wie Sie RAS im mehr Instanzen Modus mit allen RAS-Funktionen (Punkt-zu-Standort-VPN, Site-to-Site-VPN und BGP-Routing) installieren können, die für zwei Mandanten aktiviert sind: "mso" und "Fabrikam".

```
$Contoso_RoutingDomain = "ContosoTenant"  
$Fabrikam_RoutingDomain = "FabrikamTenant"  
  
Install-RemoteAccess -MultiTenancy  
  
Enable-RemoteAccessRoutingDomain -Name $Contoso_RoutingDomain -Type All -PassThru  
Enable-RemoteAccessRoutingDomain -Name $Fabrikam_RoutingDomain -Type All -PassThru
```

## BGP-Unterstützte Bereitstellungstopologien

Im Folgenden sind die unterstützten Bereitstellungstopologien aufgeführt, bei denen Unternehmensstandorte mit einem Cloud Service Provider (CSP)-Datencenter verbunden sind.

In allen Szenarien ist das CSP-Gateway ein Windows Server 2016-RAS-Gateway am Rand. Das RAS-Gateway, das mehrere Verbindungen von mehreren Mandanten verarbeiten kann, besteht aus einem Hyper-V-Host und einem virtuellen Computer, der tatsächlich als Gateway konfiguriert ist. Dieses Edgegateway wird als mehrinstanzenfähiger BGP-Router für den Austausch von Unternehmens- und CSP-Subnetzrouten mit Standort-zu-Standort-VPN-Verbindungen konfiguriert.

Mandanten stellen eine Verbindung mit ihren Ressourcen im CSP-Datencenter mithilfe einer Standort-zu-Standort (S2S)-VPN-Verbindung her. Darüber hinaus wird das BGP-Routingprotokoll für dynamischen Routinginformationsaustausch zwischen den Unternehmens- und den CSP-Gateways bereitgestellt.

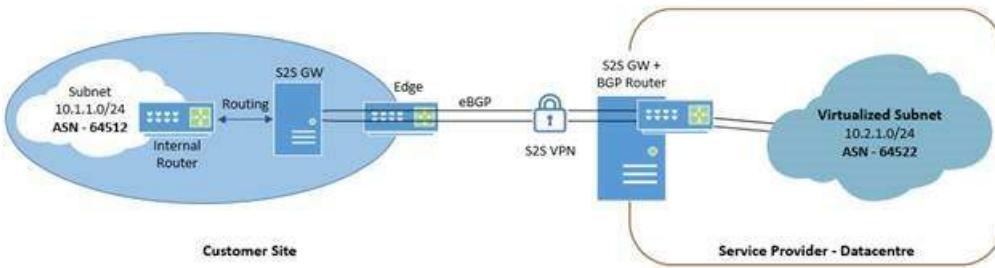
Die folgenden Bereitstellungstopologien werden unterstützt.

- [RAS-VPN-Standort-zu-Standort-Gateway mit BGP am Unternehmens Standort Edge](#)
- [Drittanbieter Gateway mit BGP am Unternehmens Standort Edge](#)
- [Mehrere Unternehmensstandorte mit Drittanbieter Gateways](#)
- [Separate Beendigungs Punkte für BGP und VPN](#)

Die folgenden Abschnitte enthalten weitere Informationen über die einzelnen unterstützten BGP-Topologien.

### RAS-VPN-Standort-zu-Standort-Gateway mit BGP am Unternehmens Standort Edge

Diese Topologie stellt einen mit einem CSP verbundene Unternehmensstandort dar. Die Unternehmens Routing Topologie enthält einen internen Router, ein Windows Server 2016-RAS-Gateway, das für VPN-Standort-zu-Standort-Verbindungen mit dem CSP konfiguriert ist, und ein edgefirewallgerät. Das RAS-Gateway beendet die S2S-VPN-und BGP-Verbindungen.



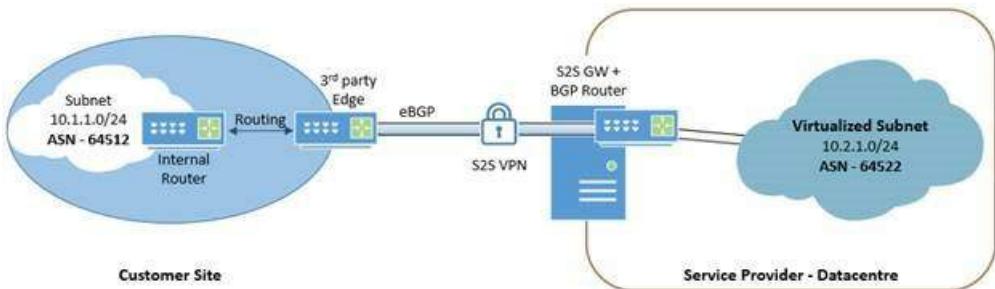
Beide Standorte sind mittels externem Border Gateway Protocol (eBGP) verbunden, das Informationen zwischen BGP-fähigen Routern in separaten autonomen Systemen (AS) übertragen kann. Dazu müssen sowohl das Unternehmen als auch der CSP unterschiedliche autonome Systemnummern (ASN) besitzen. Dies ist ein Parameter, der integraler Bestandteil des BGP-Protokolls ist.

In diesem Szenario funktioniert BGP auf folgende Weise.

- Das Edgegerät des Unternehmensstandorts erlernt mithilfe von BGP die virtualisierten Subnetzrouten (10.2.1.0/24), die in der Cloud gehostet werden. Dieses Gerät kündigt auch die lokalen Subnetzrouten (10.1.1.0/24) für das mehr Instanzen fähige CSP-RAS-Gateway an.
- Der Edgerouter des Kunden lernt lokale interne Routen über einen der folgenden Mechanismen:
  - Das Edgegerät führt BGP mit einem internen Router aus und lernt interne Routen (in diesem Beispiel 10.1.1.0/24). In der Zwischenzeit lernt der interne Router externe Routen (z. B. 10.2.1.0/24) vom Edgegerät, und der interne Router muss diese Routen an andere lokale Router über ein internes Gatewayprotokoll (IGP), wie z. B. OSPF (Open Shortest Path First) oder Routing Information-Protokoll (RIP), verteilen.
  - Das Edgegerät kann mit statischen Routen oder Schnittstellen zur Auswahl von Routen für die Ankündigung mithilfe von BGP konfiguriert werden. Das Edgegerät verteilt die externen Routen mit einem IGP auch an andere lokale Router.

#### Drittanbieter Gateway mit BGP am Unternehmens Standort Edge

Diese Topologie stellt einen Unternehmensstandort dar, der mit einem Edgerouter eines Drittanbieters eine Verbindung mit einem CSP herstellt. Der Edgerouter dient auch als Standort-zu-Standort-VPN-Gateway.

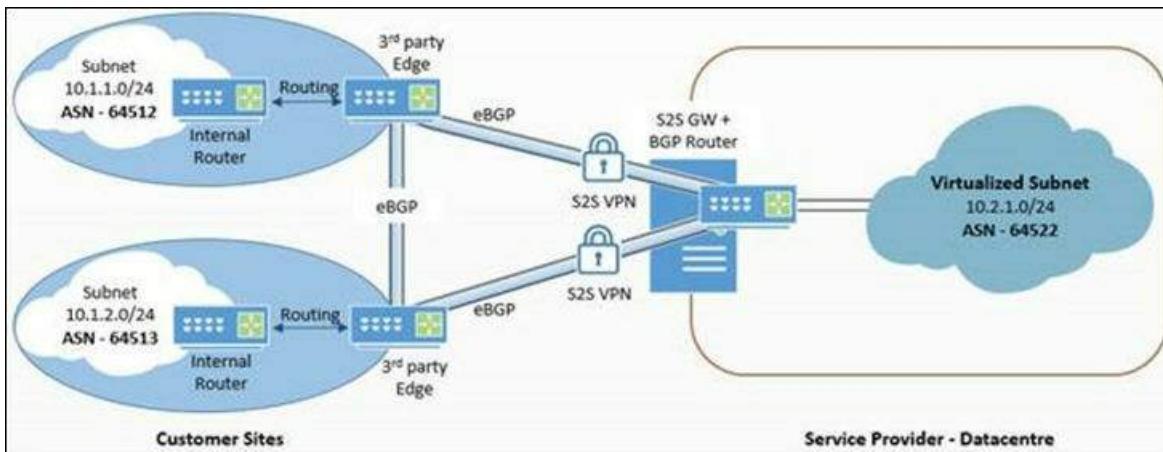


Der Unternehmensedgerouter lernt lokale interne Routen mit einem der folgenden Mechanismen:

- Das Edgegerät führt BGP mit einem internen Router aus und lernt interne Routen (in diesem Fall 10.1.1.0/24)
- Das Edgegerät implementiert ein internes Gatewayprotokoll (IGP) und ist direkt am internen Routing beteiligt.

#### Mehrere Unternehmensstandorte mit Verbindung zum CSP-clouddatencenter

Diese Topologie stellt mehrere Unternehmensstandorte dar, die mit einem Edgerouter eines Drittanbieters eine Verbindung mit einem CSP herstellen. Die Edgegeräte der Drittanbieter dienen als Standort-zu-Standort-VPN-Gateways und BGP-Router.



Die Edgerouter des Kunden lernen lokale interne Routen mit einem der folgenden Mechanismen:

- Das Edgegerät führt BGP mit einem internen Router aus und lernt interne Routen (in diesem Fall 10.1.1.0/24)
- Das Edgegerät implementiert ein internes Gatewayprotokoll (IGP) und ist direkt am internen Routing beteiligt.

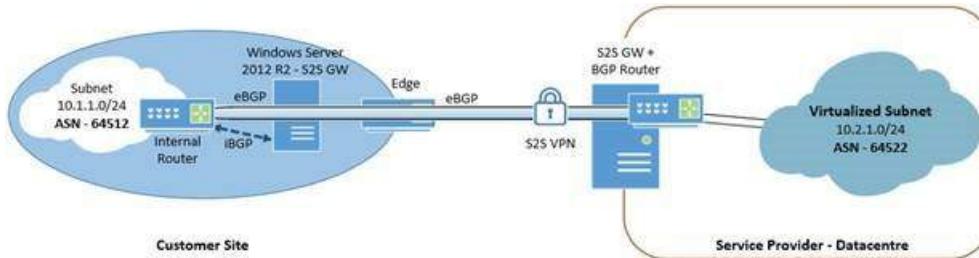
Jeder Unternehmensstandort lernt die Routen vom anderen Standort über die direkte eBGP-Verbindung.

Jeder Unternehmensstandort lernt die gehosteten Netzwerkrouten direkt und über den anderen Unternehmensstandort, wählt jedoch die optimale Route auf Grundlage der Kosten der Route aus.

Wenn der BGP-Router an Enterprise Site 1 keine Verbindung mit dem BGP-Router des Enterprise-Standorts 2 herstellen kann, weil die Konnektivität fehlgeschlagen ist, beginnt der BGP-Router von Standort 1 dynamisch, die Routen an das Netzwerk des Unternehmens Standorts 2 vom CSP-BGP-Router zu erlernen. die Umleitung von Standort 1 an Standort 2 über den Windows Server BGP-Router beim CSP.

### Separate Beendigungs Punkte für BGP und VPN

Diese Topologie stellt ein Unternehmen dar, das zwei verschiedene Router als BGP- und Standort-zu-Standort-VPN-Endpunkte verwendet. Die Site-to-Site-VPN-Verbindung wird auf dem Windows Server 2012 R2-S2S-Gateway beendet, während BGP auf einem internen Router beendet wird. Auf der CSP-Seite der Verbindungen beendet der CSP sowohl VPN-als auch BGP-Verbindungen mit dem RAS-Gateway. Bei dieser Konfiguration muss die interne Drittanbieter-Routerhardware die Umverteilung von IGP-Routen an BGP sowie von BGP-Routen an IGP unterstützen.



Der interne Router lernt Unternehmensrouten mit einem der folgenden Mechanismen:

- BGP
- Ein internes Gatewayprotokoll (IGP), wie z. B. OSPF oder RIP.
- Statische Routenkonfiguration

Wenn am Unternehmensstandort ein IGP verwendet wird, muss der interne Router IGP-Routen an BGP und BGP-Routen an IGP-Routen umverteilen, um die Subnetzverbindung zwischen den virtuellen CSP-Netzwerken und den lokalen Unternehmenssubnetzen aufrechtzuerhalten.

Bei dieser Bereitstellung verfügt das Enterprise RAS-Gateway über eine Standort-zu-Standort-VPN-Verbindung mit dem CSP-RAS-Gateway, das dem Enterprise RAS-Gateway die Routen zum CSP-Gateway bereitstellt. Der interne Unternehmens Router lernt dann diese Route zum CSP-Gateway, indem IBGP mit dem Enterprise RAS-Gateway verwendet wird. Aus diesem Grund kann der interne Unternehmens Router dann eine peeringsitzung mit dem BGP-Router für das CSP-Gateway erstellen.

Ab diesem Zeitpunkt tauschen der interne Unternehmens Router und das CSP-RAS-Gateway Routing Informationen aus. Und der Enterprise RAS-BGP-Router lernt die CSP-Routen und Unternehmens Routen, um Pakete physisch zwischen den Netzwerken weiterzuleiten.

## BGP-Funktionen

Im folgenden finden Sie die Features des RAS-Gateway-BGP-Routers.

**BGP-Routing als Rollen Dienst des Remote Zugriffs.** Sie können jetzt den **Routing Rollen Dienst** der Remote Zugriffs-Server Rolle installieren, ohne den RAS-Rollen Dienst (**Remote Access Service**) zu installieren, wenn Sie den Remote Zugriff als BGP-LAN-Router verwenden möchten. Dadurch wird der Speicherbedarf des BGP-Routers reduziert, und nur die für das dynamische BGP-Routing erforderlichen Komponenten werden installiert. Der **Routing Rollen Dienst** ist nützlich, wenn nur eine BGP-Router-VM erforderlich ist und Sie DirectAccess oder VPN nicht verwenden müssen. Außerdem bietet die Verwendung des Remote Zugriffs als LAN-Router mit BGP die dynamischen Routing Vorteile von BGP in Ihrem internen Netzwerk.

**BGP-Statistiken (Nachrichtenindikatoren, Routingindikatoren)**. Der BGP-Router unterstützt, falls erforderlich, die Anzeige von Nachrichten- und Routingstatistiken mit dem Windows PowerShell-Befehl **Get-BgpStatistics**.

**Equal Cost Multi Path Routing (ECMP)-Unterstützung.** Der BGP-Router unterstützt ECMP und kann über mehr als eine Route mit gleichen Kosten in BGP-Routingtabelle und -stapel verfügen. Die BGP-Routerauswahl der Route für die Übertragung von Datenpaketen ist bei aktiviertem ECMP zufällig.

**HoldTime-Konfiguration.** Der BGP-Router unterstützt die Konfiguration des HoldTimer-Werts entsprechend den Erfordernissen des Netzwerks. Dieser Zeitgeber kann dynamisch geändert werden, um Interoperabilität mit Geräten von Drittanbietern oder ein bestimmtes maximales Sitzungstimeout der BGP-Peeringsitzung zu gewährleisten.

**Interne BGP- und externe BGP-Unterstützung.** Der BGP-Router unterstützt iBGP- und eBGP-Peering. Um eines der beiden Protokolle zu konfigurieren, müssen Sie sicherstellen, dass die entsprechenden ASNs den lokalen und Remote-BGP-Routern zugewiesen sind. Alle vier BGP-Bereitstellungstopologien umfassen die Verwendung von eBGP-Peering, und die vierte Topologie verwendet zudem iBGP-Peering.

**Interoperabilität mit Drittanbieterlösungen.** Der BGP-Router basiert auf der neuesten BGP-Spezifikation in der Version 4 und wurde für die Interoperabilität mit den meisten wichtigen Drittanbieter-BGP-Routinggeräten getestet. Weitere Informationen finden Sie unter RFC 4271 (Request for Comments), [A Border Gateway Protocol 4 \(BGP-4\)](#).

**Unterstützung von IPv4- und IPv6-Transportpeering.** Der BGP-Router unterstützt IPv4- und IPv6-Peering. Sie müssen jedoch den BGP-Bezeichner als IPv4-Adresse des BGP-Routers konfigurieren. Für alle BGP-Routerbereitstellungstopologien kann einer der beiden Peeringtypen (IPV4/IPv6) verwendet werden.

**IPv4- und IPv6-Unicastrouten-Lern- und Ankündigungsfunctionen (Multiprotokoll-NRLI [Network Layer Reachability Information])**. Unabhängig von der verwendeten Transportart kann der BGP-Router IPv4- und IPv6-Routen austauschen, wenn die entsprechende Funktion beim Einrichten der Sitzung durch andere BGP-Router angekündigt wird. Zum Konfigurieren von IPv6-Routing, muss der Parameter **IPv6Routing** aktiviert sein, und eine lokale, globale IPv6-Adresse muss auf Routerebene konfiguriert sein.

**Peering im gemischten Modus und im passiven Modus.** Sie können BGP-peeringsitzungen im gemischten Modus konfigurieren. Dabei fungiert der BGP-Router sowohl als Initiator-als auch als Beantworter-oder Passiv-

Modus, wobei der BGP-Router kein Peering initiiert, aber auf eingehende Anforderungen antwortet. Der gemischte Modus ist die Standardeinstellung und wird für BGP-Peering empfohlen. Dies gilt, wenn Sie den passiven Modus nicht zum Debuggen und zur Diagnose verwenden möchten. Für alle BGP-Routerbereitstellungstopologien ist Peering im gemischten Modus erforderlich, um automatische Neustarts bei Fehlerereignissen zu aktivieren.

**Routenattribut-Umschreibefunktion.** Sie können die folgenden Attribute von den BGP-Routereingangs und -Ausgangsroutenkündigungen mithilfe der BGP-Routingrichtlinien Next-Hop, MED, Local-Pref und Community hinzufügen, ändern oder entfernen.

**Routenfilterung.** Der BGP-Router unterstützt Filterung von Eingangs und -Ausgangsroutenkündigungen basierend auf mehreren Routenattributen wie Präfix, ASN-Bereich, Community und Next-Hop.

**Routen Reflektor (RR) und RR-Client.** Der BGP-Router kann als Routen Reflektor und RR-Client fungieren. Dies ist bei komplexen Topologien nützlich, bei denen RR das Netzwerk durch die Bildung von RR-Clustern vereinfachen kann.

**Route-Refresh-Unterstützung.** Der BGP-Router unterstützt Route-Refresh und kündigt dies standardmäßig beim Peering an. Es ist in der Lage, einen neuen Satz von Routen Aktualisierungen zu senden, wenn er von einem Peer per Route-Refresh-Nachricht angefordert wird, und eine Route-Aktualisierung zu senden, um die Routing Tabelle in Ereignissen wie Routing Richtlinien Änderungen für einen Peer zu aktualisieren. Dies ermöglicht das ändern oder Aktualisieren der BGP-Routing Richtlinien in Windows Server 2016, ohne dass das Peering neu gestartet werden muss.

**Unterstützung für die Konfiguration von statischen Routen.** Sie können statische Routen oder Schnittstellen auf dem BGP-Router mit dem Windows PowerShell-Befehl `Add-BgpCustomRoute` konfigurieren. Die statischen Routen, die Sie konfigurieren, können die Präfixe oder Schnittstellennamen sein, von denen die Routen ausgewählt werden müssen. Allerdings werden nur die Routen mit auflösbaren Next-Hops in die BGP-Routingtabellen einbezogen und den Peers angekündigt.

**Transitroutingunterstützung.** Der BGP-Router unterstützt Transit Routing für IBGP-zu-IBGP-Verbindungen, IBGP-zu-EBGP-Verbindungen sowie EBGP-zu-EBGP-Verbindungen.

**Die Weiterleitungs Klappen Dämpfung.** Die Weiterleitung von Klappen für das BGP-Routing in Windows Server 2016 bietet Unterstützung für die Weiterleitungen von Routen dämpfen. Wenn z. b. eine Route ständig angekündigt und zurückgezogen wird, sodass die Routing Tabelle instabil wird, können Sie den BGP-Router so konfigurieren, dass er der Route eine Dämpfungs Gewichtung zuweist und ihn nach Bedarf zu unterdrücken oder zu unterdrücken. Dies hilft bei der Verwaltung einer stabilen Routing Tabelle und der geringeren Verarbeitung durch den BGP-Router.

**Routen Aggregation.** Durch die Weiterleitung von Aggregationen an den BGP-Router haben Sie die Möglichkeit, Aggregat Routen zu konfigurieren und die präziseren Routen Ankündigungen durch Zusammenfassungs-oder Aggregat Routen an Peers zu ersetzen. Dies führt zu einer geringeren Anzahl von Routen Ankündigungs Meldungen, die im Netzwerk übertragen werden.

#### NOTE

In System Center wird das RAS-Gateway als Windows Server-Gateway bezeichnet.

# BGP-Befehlsreferenz für Windows PowerShell

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Sie können dieses Thema als Referenz verwenden, wenn Sie Windows PowerShell-Skripts schreiben, um BGP-Funktionen über RAS-Gateway und RAS-LAN-Router (Local Area Network) hinzuzufügen, zu konfigurieren und zu entfernen.

Diese BGP-Befehle sind Teil des Windows PowerShell-Befehlssatzes für Remote Zugriff für Windows Server 2016. Dieses Thema hilft Ihnen dabei, die BGP-Befehle, die Sie in Skripts verwenden möchten, schnell zu finden.

Weitere Informationen zu allen Remote Zugriffs Befehlen finden Sie unter [Remote Access-Cmdlets](#).

## BGP-Befehlsreferenz

In den folgenden Abschnitten finden Sie einen Befehlsnamen, einen Zweck und eine Syntax für jeden BGP-Befehl sowie einen Link zum Befehl in der RAS-Referenz, der ausführlichere Informationen zu den einzelnen Befehlen enthält.

Diese Referenz umfasst folgende Abschnitte:

- [Befehle hinzufügen](#)
- [Befehle löschen](#)
- [Deaktivieren und Aktivieren von Befehlen](#)
- [Get-Befehle](#)
- [Installieren von Befehlen](#)
- [Befehle entfernen](#)
- [Befehle festlegen](#)
- [Starten und Abbrechen von Befehlen](#)
- [Deinstallations Befehle](#)

### **Befehle hinzufügen**

Die folgenden BGP-Befehle werden hinzugefügt.

#### [Add-bgpcustomroute](#)

Fügt der BGP-Routing Tabelle benutzerdefinierte Routen hinzu.

```
Add-BgpCustomRoute [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-Interface <String[]> ] [-Network <String[]> ] [-PassThru]
[-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

#### [Add-bgppeer](#)

Fügt einen neuen BGP-Peer hinzu.

```
Add-BgpPeer [-Name] <String> -LocalIPAddress <IPAddress> -PeerASN <UInt32> -PeerIPAddress <IPAddress> [-CimSession <CimSession[]> ] [-HoldTimeSec <UInt16> ] [-IdleHoldTimeSec <UInt16> ] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-LocalASN <UInt32> ] [-MaxAllowedPrefix <UInt32> ] [-OperationMode <OperationMode> {Mixed | Server} ] [-PassThru] [-PeeringMode <PeeringMode> {Automatic | Manual} ] [-RouteReflectorClient <Boolean> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Weight <UInt16> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Add-bgprouteaggregate

Fügt eine neue Aggregat Route für bestimmte BGP-Routen hinzu.

```
Add-BgpRouteAggregate -Prefix <String> [-AttributePolicy <String[]> ] [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-PassThru] [-PreserveASPath <PreserveASPath> ] [-RoutingDomain <String> ] [-SummaryOnly <SummaryOnly> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Add-bgprouter

Fügt einen BGP-Router für die angegebene Mandanten-ID hinzu.

```
Add-BgpRouter -BgpIdentifier <IPAddress> -LocalASN <UInt32> [-CimSession <CimSession[]> ] [-ClientToClientReflection <ClientToClientReflection> ] [-ClusterId <UInt32> ] [-CompareMEDAcrossASN <Boolean> ] [-DefaultGatewayRouting <Boolean> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-IPv6Routing <IPv6RoutingState> {Disabled | Enabled} ] [-LocalIPv6Address <IPAddress> ] [-PassThru] [-RouteReflector <RouteReflector> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-TransitRouting <TransitRouting> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Add-bgproutingpolicy

Fügt dem Richtlinien Speicher eine BGP-Routing Richtlinie hinzu.

```
Add-BgpRoutingPolicy [-Name] <String> [-PolicyType] <PolicyType> {Deny | Allow | ModifyAttribute} [-AddCommunity <String[]> ] [-CimSession <CimSession[]> ] [-ClearMED] [-Force] [-IgnorePrefix <String[]> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-MatchASNRange <UInt32[]> ] [-MatchCommunity <String[]> ] [-MatchNextHop <IPAddress[]> ] [-MatchPrefix <String[]> ] [-NewLocalPref <UInt32> ] [-NewMED <UInt32> ] [-NewNextHop <IPAddress> ] [-PassThru] [-RemoveAllCommunities] [-RemoveCommunity <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Add-bgproutingpolicyforpeer

Fügt BGP-Routing Richtlinien BGP-Peers hinzu.

```
Add-BgpRoutingPolicyForPeer -Direction <PolicyDirection> {Ingress | Egress} -PolicyName <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-PeerName <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Befehle löschen

Im folgenden finden Sie die unverschlüsselten Befehle für BGP.

## Clear-bgprouteflapdampening

Löscht die Weiterleitungs Klappen-Feuchtigkeits Informationen für den angegebenen Satz von BGP-Routen.

```
Clear-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-Prefix <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [<WorkflowParameters>]
```

## Deaktivieren und Aktivieren von Befehlen

Im folgenden finden Sie die Befehle zum Deaktivieren und aktivieren für BGP.

### Deaktivieren-bgprouteflapdampening

Deaktiviert die Routen Dämpfung für die Fluktuation BGP-Routen.

```
Disable-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [<WorkflowParameters>]
```

### Enable-bgprouteflapdampening

Aktiviert die Routen Dämpfung für die Fluktuation BGP-Routen.

```
Enable-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-PassThru] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [<WorkflowParameters>]
```

## Get-Befehle

Im folgenden finden Sie die Get-Befehle für BGP.

### Get-bgpcustomroute

Ruft benutzerdefinierte Routeninformationen vom BGP-Router ab.

```
Get-BgpCustomRoute [-CimSession <CimSession[]> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [<CommonParameters>] [ <WorkflowParameters>]
```

### Get-bgppeer

Ruft Konfigurationsinformationen für BGP-Peers ab.

```
Get-BgpPeer [[-Name] <String[]> ] [-CimSession <CimSession[]> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [<CommonParameters>] [ <WorkflowParameters>]
```

### Get-bgprouteaggregate

Ruft alle vom Administrator konfigurierten BGP-Aggregat Routen ab.

```
Get-BgpRouteAggregate [-CimSession <CimSession[]> ] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-Prefix <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [<WorkflowParameters>]
```

## Get-bgprouteflapdampening

Ruft die Konfiguration einer BGP-Weiterleitungs-däfungs-Engine ab.

```
Get-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-InformationAction <ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-
RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

## Get-bgprouteinformation

Ruft BGP-Routeninformationen für mindestens ein Netzwerk Präfix aus der BGP-Routing Tabelle ab.

```
Get-BgpRouteInformation [-CimSession <CimSession[]> ] [-InformationAction <ActionPreference> {SilentlyContinue
| Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-Network <String[]> ] [-
RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Type <RouteType> ] [ <CommonParameters>] [
<WorkflowParameters>]
```

## Get-bgprouter

Ruft Konfigurationsinformationen für BGP-Router ab.

```
Get-BgpRouter [-CimSession <CimSession[]> ] [-InformationAction <System.Management.Automation.ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-
RoutingDomain <String[]> ] [-ThrottleLimit <Int32> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Get-bgproutingpolicy

Ruft Konfigurationsinformationen der BGP-Routing Richtlinien ab.

```
Get-BgpRoutingPolicy [[-Name] <String[]> ] [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-PolicyType <PolicyType> {Deny | Allow | ModifyAttribute} ]
[-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Get-bgpstatistics

Abrufen von BGP-Peering-bezogenen Nachrichten-und Routen Ankündigungs Statistiken.

```
Get-BgpStatistics [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-PeerName <String[]> ] [-RoutingDomain <String> ] [-
ThrottleLimit <Int32> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Installieren von Befehlen

Im folgenden finden Sie die Installations Befehle für RAS-Gateway und BGP.

### Install-remoteaccess

Führt Voraussetzungs Prüfungen für DirectAccess (da) aus, um sicherzustellen, dass die Installation möglich ist, ob für den Remote Zugriff (einschließlich der Verwaltung von Remote Clients) installiert ist, und installiert VPN (sowohl RAS-VPN als auch Standort-zu-Standort-VPN), und installiert BGP-Routing.

```

Parameter Set: MultiTenant
Install-RemoteAccess [-MultiTenancy] [-CapacityKbps <UInt64> ] [-CimSession <CimSession[]> ] [-ComputerName
<String> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop |
Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-MsgAuthenticator <String>
{Enabled | Disabled} ] [-PassThru] [-RadiusPort <UInt16> ] [-RadiusScore <Byte> ] [-RadiusServer <String> ] [-
RadiusTimeout <UInt32> ] [-SharedSecret <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [
<CommonParameters>] [ <WorkflowParameters>]

Parameter Set: Vpn
Install-RemoteAccess [-VpnType] <String> {Vpn | VpnS2S | SstpProxy | RoutingOnly} [-CimSession <CimSession[]> ]
[-ComputerName <String> ] [-EntrypointName <String> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-IPAddressRange <String[]> ] [-IPv6Prefix <String> ] [-
Legacy] [-MsgAuthenticator <String> {Enabled | Disabled} ] [-PassThru] [-RadiusPort <UInt16> ] [-RadiusScore
<Byte> ] [-RadiusServer <String> ] [-RadiusTimeout <UInt32> ] [-SharedSecret <String> ] [-ThrottleLimit <Int32>
] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]

```

## IMPORTANT

Wenn Sie das RAS-Gateway im mehr Instanzen fähigen Modus installieren, müssen Sie angeben, ob BGP für jeden Mandanten aktiviert ist, indem Sie den Windows PowerShell-Befehl **enable-remoteaccessroutingdomain** mit dem -**Type**- Parameterwert **all** verwenden. Der folgende Beispielcode veranschaulicht, wie Sie RAS im mehr Instanzen Modus mit allen RAS-Funktionen (Punkt-zu-Standort-VPN, Site-to-Site-VPN und BGP-Routing) installieren können, die für zwei Mandanten aktiviert sind: "mso" und "Fabrikam".

```

$Contoso_RoutingDomain = "ContosoTenant"
$Fabrikam_RoutingDomain = "FabrikamTenant"

Install-RemoteAccess -MultiTenancy

Enable-RemoteAccessRoutingDomain -Name $Contoso_RoutingDomain -Type All -PassThru
Enable-RemoteAccessRoutingDomain -Name $Fabrikam_RoutingDomain -Type All -PassThru

```

Wenn Sie den Remote Zugriff als LAN-Router anstelle von als Gateway verwenden, können Sie weiterhin BGP verwenden, was den Vorteil bietet, dass Sie das dynamische Routing in Ihrem Intranet verwenden. Geben Sie den folgenden Befehl in einer Windows PowerShell-Eingabeaufforderung ein, und drücken Sie die EINGABETASTE, um den Remote Zugriff als BGP-LAN-Router zu installieren.

```
Install-RemoteAccess -VpnType RoutingOnly
```

## Befehle entfernen

Im folgenden finden Sie die Remove-Befehle für BGP.

### [Remove-bgpcustomroute](#)

Entfernt benutzerdefinierte Routen vom BGP-Router.

```

Remove-BgpCustomRoute [-CimSession <CimSession[]> ] [-Force] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-Interface <String[]> ] [-Network <String[]> ] [-
RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]

```

### [Remove-bgppeer](#)

Entfernt BGP-Peers von einem Router.

```
Remove-BgpPeer [-Name] <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Remove-bgprouteaggregate

Entfernt den Satz der angegebenen aggregierten BGP-Routen.

```
Remove-BgpRouteAggregate [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-Prefix <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Remove-bgprouter

Entfernt einen BGP-Router.

```
Remove-BgpRouter [-CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String[]> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Remove-bgproutingpolicy

Entfernt Routing Richtlinien aus dem Richtlinien Speicher.

```
Remove-BgpRoutingPolicy [-Name] <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Remove-bgproutingpolicyforpeer

Entfernt Routing Richtlinien von BGP-Peers.

```
Parameter Set: Remove1  
Remove-BgpRoutingPolicyForPeer [-CimSession <CimSession[]> ] [-Direction <PolicyDirection> {Ingress | Egress} ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-PeerName <String[]> ] [-PolicyName <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Befehle festlegen

Im folgenden finden Sie die SET-Befehle für BGP.

## Set-bgppeer

Aktualisiert die Konfiguration des angegebenen BGP-Peers.

```
Set-BgpPeer [-Name] <String> [-CimSession <CimSession[]> ] [-ClearPrefixLimit] [-Force] [-HoldTimeSec <UInt16> ] [-IdleHoldTimeSec <UInt16> ] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-LocalASN <UInt32> ] [-LocalIPAddress <IPAddress> ] [-MaxAllowedPrefix <UInt32> ] [-OperationMode <OperationMode> {Mixed | Server} ] [-PassThru] [-PeerASN <UInt32> ] [-PeeringMode <PeeringMode> {Automatic | Manual} ] [-PeerIPAddress <IPAddress> ] [-RouteReflectorClient <Boolean> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Weight <UInt16> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Set-bgprouteaggregate

Aktualisiert die Eigenschaften der angegebenen Aggregat-BGP-Route.

```
Set-BgpRouteAggregate -Prefix <String> [-AttributePolicy <String[]> ] [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-PassThru] [-PreserveASPath <PreserveASPath> ] [-RoutingDomain <String> ] [-SummaryOnly <SummaryOnly> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Set-bgprouteflapdampening

Konfiguriert die BGP-Weiterleitungs-Engine für die Routen Dämpfung.

```
Set-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-HalfLife <UInt32> ] [-HalfLifeUnreachable <UInt32> ] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-MaxSuppressTime <UInt32> ] [-PassThru] [-ReuseThreshold <UInt32> ] [-RoutingDomain <String> ] [-SuppressThreshold <UInt32> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Set-bgrouter

Aktualisiert die Konfiguration des lokalen BGP-Routers für die angegebene Mandanten-ID.

```
Set-BgpRouter [-BgpIdentifier <IPAddress> ] [-CimSession <CimSession[]> ] [-ClientToClientReflection <ClientToClientReflection> ] [-ClusterId <UInt32> ] [-CompareMEDAcrossASN <Boolean> ] [-DefaultGatewayRouting <Boolean> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-IPv6Routing <IPv6RoutingState> {Disabled | Enabled} ] [-LocalASN <UInt32> ] [-LocalIPv6Address <IPAddress> ] [-PassThru] [-RouteReflector <RouteReflector> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-TransitRouting <TransitRouting> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Set-bgproutingpolicy

Ändert eine Routing Richtlinien Konfiguration.

```
Set-BgpRoutingPolicy [-Name] <String> [-AddCommunity <String[]> ] [-CimSession <CimSession[]> ] [-ClearMED] [-Force] [-IgnorePrefix <String[]> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-MatchASNRange <UInt32[]> ] [-MatchCommunity <String[]> ] [-MatchNextHop <IPAddress[]> ] [-MatchPrefix <String[]> ] [-NewLocalPref <UInt32> ] [-NewMED <UInt32> ] [-NewNextHop <IPAddress> ] [-PassThru] [-PolicyType <PolicyType> {Deny | Allow | ModifyAttribute} ] [-RemoveAllCommunities] [-RemoveCommunity <String[]> ] [-RemovePolicyClause <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

## Set-bgproutingpolicyforpeer

Ändert BGP-Routing Richtlinien für BGP-Peers.

```
Set-BgpRoutingPolicyForPeer -Direction <PolicyDirection> {Ingress | Egress} -PolicyName <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-PeerName <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters> ] [ <WorkflowParameters> ]
```

## Starten und Abbrechen von Befehlen

Im folgenden finden Sie die Befehle zum Starten und Abbrechen für BGP.

### Start-bgppeer

Startet das Routing von Sitzungen für BGP-Peers.

```
Start-BgpPeer [-Name] <String[]> [-CimSession <CimSession[]> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [ <CommonParameters> ] [ <WorkflowParameters> ]
```

### "Beendigung-bgppeer"

Beendet das Routing von Sitzungen für BGP-Peers.

```
Stop-BgpPeer [-Name] <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters> ] [ <WorkflowParameters> ]
```

## Deinstallations Befehle

Im folgenden finden Sie die Deinstallations Befehle für RAS-Gateway und BGP.

### Deinstallieren-remoteaccess

Deinstalliert den Remote Zugriff vom Computer, einschließlich aller Remote Zugriffs Features und-Funktionen (RAS-Gateway, BGP usw.).

```
Uninstall-RemoteAccess [-CimSession <CimSession[]> ] [-ComputerName <String> ] [-EntryPointName <String> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-ThrottleLimit <Int32> ] [-VpnType <String> {Vpn | VpnS2S} ] [-Confirm] [-WhatIf] [ <CommonParameters> ] [ <WorkflowParameters> ]
```

# RAS-Gateway

27.03.2020 • 19 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

RAS-Gateway ist ein Software Router und ein Gateway, das Sie im Einzel Mandanten Modus oder im mehr Instanzen fähigen Modus verwenden können.

- Der **Modus mit nur einem Mandanten** ermöglicht Organisationen beliebiger Größe das Bereitstellen des Gateways als Außendienst (virtuelles privates Netzwerk, VPN) und DirectAccess-Server mit Internet Zugriff. Im Einzel Mandanten Modus können Sie das RAS-Gateway auf einem physischen Server oder virtuellen Computer (VM) bereitstellen, auf dem Windows Server 2016 ausgeführt wird.
- Der mehr Instanzen fähige **Modus** ermöglicht clouddienstanbietern (Cloud Service Providers, CSPs) und Unternehmen die Verwendung des RAS-Gateways, um das Routing von Daten Center-und cloudnetzwerkdatenverkehr zwischen virtuellen und physischen Netzwerken, Bei einem mehr Instanzen fähigen Modus empfiehlt es sich, das RAS-Gateway auf virtuellen Computern bereitzustellen, auf denen Windows Server 2016 ausgeführt wird.

## NOTE

RAS-Gateway unterstützt IPv4 und IPv6, einschließlich IPv4- und IPv6-Weiterleitung. Wenn Sie das RAS-Gateway mit Network Address Translation (NAT) konfigurieren, wird nur NAT44 unterstützt.

## Wer ist für das RAS-Gateway interessiert?

Wenn Sie ein Systemadministrator, ein Netzwerk Architekt oder ein anderer IT-Experte sind, kann das RAS-Gateway unter einem oder mehreren der folgenden Umstände von Interesse sein:

- Sie entwerfen oder unterstützen eine IT-Infrastruktur für eine Organisation, die Hyper-V zum Bereitstellen virtueller Computer (VMs) in virtuellen Netzwerken nutzt oder die Nutzung plant.
- Sie entwerfen oder unterstützen IT-Infrastruktur für eine Organisation, die Cloudtechnologie bereitgestellt hat oder die Bereitstellung plant.
- Sie möchten eine umfassende Netzwerkverbindung zwischen physischen und virtuellen Netzwerken bereitstellen.
- Sie möchten den Kunden Ihrer Organisation Zugriff auf Ihre virtuellen Netzwerke über das Internet bereitstellen.
- Sie möchten den Mitarbeitern Ihrer Organisation Remote Zugriff auf Ihr Unternehmensnetzwerk bieten.
- Sie möchten Niederlassungen an verschiedenen physischen Standorten über das Internet verbinden.

Dieses Thema, das für IT-Experten gedacht ist, enthält eine Übersicht über das RAS-Gateway, einschließlich Bereitstellungs Modi und Features für RAS-Gateways.

Dieses Thema enthält folgende Abschnitte:

- [RAS-Gateway-Bereitstellungs Modi](#)
- [Clustering des RAS-Gateways für hohe Verfügbarkeit](#)

- [RAS-Gatewayfeatures](#)
- [Bereitstellungs Szenarien für RAS-Gateways](#)
- [RAS-Gateway-Verwaltungs Tools](#)

## RAS-Gateway-Bereitstellungs Modi

RAS-Gateway umfasst die folgenden Bereitstellungs Modi:

### **Einzel Mandanten Modus**

In den meisten Organisationen ist die Verwendung des RAS-Gateways im Modus mit nur einem Mandanten die typische Konfiguration. Im Einzel Mandanten Modus können Sie das RAS-Gateway als Edge-VPN-Server, Edge-DirectAccess-Server oder beides gleichzeitig bereitstellen. In dieser Konfiguration stellt das RAS-Gateway Remote Mitarbeitern eine Verbindung mit Ihrem Netzwerk mithilfe von VPN-oder DirectAccess-Verbindungen bereit. Außerdem können Sie mit dem Modus für einzelne Mandanten Niederlassungen an verschiedenen physischen Standorten über das Internet verbinden.

### **Mehr Instanzen fähiger Modus**

Wenn Ihre Organisation ein CSP oder ein Unternehmen mit mehreren Mandanten ist, können Sie das RAS-Gateway im mehrinstanzfähigen Modus bereitstellen, um Netzwerk Datenverkehr zu und von virtuellen und physischen Netzwerken bereitzustellen.

Mehr Instanzen Fähigkeit ist die Fähigkeit einer cloudinfrastruktur, die Arbeits Auslastungen virtueller Computer mehrerer Mandanten zu unterstützen, Sie aber voneinander zu isolieren, während alle Arbeits Auslastungen in der gleichen Infrastruktur ausgeführt werden. Mehrere Arbeitsauslastungen eines einzelnen Mandanten können miteinander verbunden und remote verwaltet werden. Es gibt jedoch keine Verbindung zwischen diesen Systemen und den Arbeitsauslastungen anderer Mandanten, und auch die Remoteverwaltung durch andere Mandanten ist nicht möglich.

Ein Unternehmen kann beispielsweise über viele verschiedene virtuelle Subnetze verfügen, die jeweils einer bestimmten Abteilung zugeordnet sind, z. B. Forschung und Entwicklung oder der Buchhaltung. In einem weiteren Beispiel verfügt ein CSP über viele Mandanten mit isolierten virtuellen Subnetzen in demselben physischen Rechenzentrum. In beiden Fällen kann das RAS-Gateway Datenverkehr an einen und von jedem Mandanten weiterleiten, während gleichzeitig die entworfene Isolation der einzelnen Mandanten gewahrt bleibt. Diese Funktion macht das RAS-Gateway mehr Instanzen fähig.

Virtuelle Netzwerke werden mithilfe der Hyper-V-Netzwerkvirtualisierung erstellt, bei der es sich um eine Technologie handelt, die in Windows Server 2012 eingeführt wurde und in Windows Server 2016 verbessert wurde. RAS-Gateway ist in die Hyper-V-Netzwerkvirtualisierung integriert und kann Netzwerk Datenverkehr effektiv weiterleiten, wenn es viele verschiedene Kunden oder Mandanten gibt, die über isolierte virtuelle Netzwerke im selben Rechenzentrum verfügen.

Die Hyper-V-Netzwerkvirtualisierung bietet die Möglichkeit, ein virtuelles Computernetzwerk (VM) bereitzustellen, das unabhängig vom zugrunde liegenden physischen Netzwerk ist. Bei VM-Netzwerken, die sich aus einem oder mehreren virtuellen Subnetzen zusammensetzen, wird der exakte physische Speicherort eines IP-Subnetzes von der Topologie des virtuellen Netzwerks entkoppelt. Daher können Sie Ihre lokalen Subnetze problemlos in die Cloud verschieben und gleichzeitig Ihre vorhandenen IP-Adressen und die Topologie in der Cloud beibehalten. Dank dieser Möglichkeit zur Aufrechterhaltung der Infrastruktur können vorhandene Dienste weiterhin verwendet werden, und zwar unabhängig von deren physischem Speicherort in den Subnetzen. Dies bedeutet, dass mit der Hyper-V-Netzwerkvirtualisierung eine nahtlose Hybrid-Cloud zur Verfügung steht.

#### **NOTE**

Die Hyper-V-Netzwerkvirtualisierung ist eine netzwerküberlagerungs Technologie, die die generische Routing Kapselung ([nvGRE](#)) für die Netzwerkvirtualisierung verwendet, die es Mandanten ermöglicht, ihren eigenen Adressraum zu nutzen und CSPs eine bessere Skalierbarkeit zu ermöglichen.

In Windows Server 2016 leitet das RAS-Gateway Netzwerk Datenverkehr zwischen dem physischen Netzwerk und den VM-Netzwerkressourcen weiter, unabhängig davon, wo sich die Ressourcen befinden. Mithilfe des RAS-Gateways können Sie Netzwerk Datenverkehr zwischen physischen und virtuellen Netzwerken am selben physischen Standort oder an vielen verschiedenen physischen Standorten weiterleiten.

Wenn Sie z. b. über ein physisches Netzwerk und ein virtuelles Netzwerk am gleichen physischen Standort verfügen, können Sie einen Computer, auf dem Hyper-V ausgeführt wird, der mit einer RAS-Gateway-VM konfiguriert ist, als Weiterleitungs Gateway bereitstellen und den Datenverkehr zwischen dem virtuellen und physischen Netzwerk weiterleiten.

Wenn Ihre virtuellen Netzwerke in der Cloud vorhanden sind, kann Ihr CSP ein RAS-Gateway bereitstellen, sodass Sie eine VPN-Site-to-Site-Verbindung zwischen dem VPN-Server und dem RAS-Gateway des virtuellen Netzwerks herstellen können. Wenn Sie diesen Link eingerichtet haben, können Sie über die VPN-Verbindung eine Verbindung mit Ihren virtuellen Ressourcen in der Cloud herstellen.

Weitere Informationen finden Sie unter [hohe Verfügbarkeit des RAS-Gateways](#).

## Clustering des RAS-Gateways für hohe Verfügbarkeit

RAS-Gateway wird auf einem dedizierten Computer bereitgestellt, auf dem Hyper-V ausgeführt wird und der mit einem virtuellen Computer konfiguriert ist. Der virtuelle Computer wird dann als RAS-Gateway konfiguriert.

Für hohe Verfügbarkeit von Netzwerkressourcen können Sie RAS-Gateway mit Failover bereitstellen, indem Sie zwei physische Host Server mit Hyper-V verwenden, die jeweils auch einen virtuellen Computer (VM) ausführen, der als Gateway konfiguriert ist. Die virtuellen Gatewaycomputer werden dann als Cluster konfiguriert, um einen Failoverschutz vor Netzwerkausfällen und Hardwarefehlern zu bieten.

Wenn Ihre Organisation z. b. ein Unternehmen mit einer Private Cloud-Bereitstellung ist, benötigen Sie möglicherweise nur zwei RAS-Gateway-VMS, die jeweils auf einem anderen Computer installiert sind, auf dem Hyper-V ausgeführt wird. In diesem Szenario werden die virtuellen RAS-Gateway-Computer zu einem Cluster hinzugefügt, um Hochverfügbarkeit zu gewährleisten.

Ein weiteres Beispiel: Wenn Ihre Organisation ein clouddienstanbieter (Cloud Service Provider, CSP) mit 200 Mandanten in Ihrem Daten Center ist, können Sie acht RAS-Gateway-VMS verwenden, wobei jedes Paar von gruppierten RAS-Gateway-VMS Routing Dienste für 50 Mandanten bereitstellt. In diesem Szenario haben zwei Computer, auf denen Hyper-V ausgeführt wird, jeweils vier VMS, die als RAS-Gateways konfiguriert sind. Anschließend konfigurieren Sie vier RAS-Gateway-VM-Cluster, die jeweils einen virtuellen Computer auf jedem Computer mit Hyper-V enthalten.

Beim Bereitstellen des RAS-Gateways muss auf den Host Servern, auf denen Hyper-V ausgeführt wird, und den virtuellen Computern, die Sie als Gateways konfigurieren, Windows Server 2012 R2 oder Windows Server 2016 ausgeführt werden.

## RAS-Gatewayfeatures

RAS-Gateway umfasst die folgenden Funktionen:

- **Site-to-Site-VPN.** Diese RAS-Gatewayfunktion ermöglicht es Ihnen, zwei Netzwerke an verschiedenen physischen Standorten über das Internet mithilfe einer Site-to-Site-VPN-Verbindung zu verbinden. Wenn

Sie über eine zentrale und mehrere Zweigstellen verfügen, können Sie an jedem Standort ein Edge-RAS-Gateway bereitstellen und Site-to-Site-Verbindungen erstellen, um den Netzwerk Datenverkehr zwischen den Standorten bereitzustellen. Für CSPs, die viele Mandanten in Ihrem Rechenzentrum hosten, bietet das RAS-Gateway eine mehrinstanzfähige Gatewaylösung, die ihren Mandanten den Zugriff auf und die Verwaltung Ihrer Ressourcen über Standort-zu-Standort-VPN-Verbindungen von Remote Standorten ermöglicht und den Netzwerk Datenverkehr zwischen virtuelle Ressourcen in Ihrem Daten Center und in Ihrem physischen Netzwerk.

- **Punkt-zu-Standort-VPN.** Diese RAS-Gatewayfunktion ermöglicht es Organisationen Mitarbeitern oder Administratoren, von Remote Standorten aus eine Verbindung mit dem Netzwerk Ihrer Organisation herzustellen. Bei bereit Stellungen mit einem Mandanten des RAS-Gateways können Remote Mitarbeiter über eine VPN-Verbindung eine Verbindung mit Ihrem Unternehmensnetzwerk herstellen. Diese Verbindung ermöglicht es Ihnen, interne Netzwerkressourcen wie Intranetwebsites und Dateiserver zu verwenden. Für bereit Stellungen mit mehreren Mandanten können Mandanten Netzwerkadministratoren Punkt-zu-Standort-VPN-Verbindungen verwenden, um auf virtuelle Netzwerkressourcen im CSP-Daten Center zuzugreifen.
- **Dynamisches Routing mit Border Gateway Protocol (BGP).** BGP verringert den Bedarf an manueller Routingkonfiguration auf Routern, da es ein dynamisches Routingprotokoll ist, das automatisch Routen zwischen Standorten lernt, die über die Standort-zu-Standort-VPN-Verbindungen verbunden sind. Wenn Ihre Organisation über mehrere Standorte verfügt, die mithilfe von BGP-fähigen Routern wie RAS-Gateway verbunden sind, ermöglicht BGP den Routern die automatische Berechnung und Verwendung gültiger Routen untereinander im Falle einer Netzwerk Unterbrechung oder eines Fehlers. Weitere Informationen finden Sie unter [RFC 4271](#).
- **Netzwerk Adressübersetzung (Network Address Translation, NAT).** Mithilfe der Netzwerk Adressübersetzung (Network Address Translation, NAT) können Sie eine Verbindung mit dem öffentlichen Internet über eine einzige Schnittstelle mit einer einzelnen öffentlichen IP-Adresse gemeinsam nutzen. Von den Computern im privaten Netzwerk werden private, nicht Routing fähige Adressen verwendet. In NAT werden die privaten Adressen der öffentlichen Adresse zugeordnet. Mithilfe dieses RAS-Gatewayfeatures können Organisationen Mitarbeiter mit einzelinstanzbereitstellungen über das Gateway auf Internet Ressourcen zugreifen. Für CSPs ermöglicht diese Funktion Anwendungen, die auf Mandanten-VMS ausgeführt werden, auf das Internet zuzugreifen. Beispielsweise kann eine als Webserver konfigurierte Mandanten-VM externe Finanzressourcen kontaktieren, um Kreditkartentransaktionen zu verarbeiten.

## Bereitstellungs Szenarien für RAS-Gateways

Im folgenden finden Sie die empfohlenen Bereitstellungs Szenarien für das RAS-Gateway.

- **Unternehmens Edge-Bereitstellung** mit nur einem Mandanten Mit der Enterprise-Bereitstellung für einen einzelnen Mandanten können Sie mithilfe des Standort-zu-Standort-VPN-Features eine physische Verbindung mit mehreren anderen physischen Standorten über das Internet herstellen, und Border Gateway Protocol (BGP) ermöglicht Ihnen die Verwendung des dynamischen Routings. Sie können Remote Mitarbeitern auch den Zugriff auf Ihr Organisations Netzwerk mit Punkt-zu-Standort-VPN-Verbindungen und DirectAccess-Verbindungen ermöglichen. (DirectAccess-Verbindungen sind immer eingeschaltet. Außerdem bieten Sie den Vorteil, dass Sie Computer, die über DirectAccess verbunden sind, problemlos verwalten können, weil Sie immer verbunden sind, wenn Sie sich auf dem Internet befinden und mit dem Internet verbunden sind.) Sie können auch Single Tenant Enterprise RAS-Gateways mit NAT konfigurieren, damit Computer in Ihrem Intranet problemlos mit dem Internet kommunizieren können.
- **Edge-Bereitstellung des clouddienstanbieters.** Mit der mehr Instanzen fähigen RAS-Gateway-Bereitstellung für CSPs können Sie Ihren Mandanten alle Features anbieten, die bei der Bereitstellung von einem Unternehmen mit nur einem Mandanten zur Verfügung stehen. Standort-zu-Standort-VPN-Verbindungen zwischen virtuellen Mandanten Netzwerken in Ihrem Rechenzentrum und den Netzwerk

Standorten des Mandanten über das Internet bedeuten, dass Mandanten immer nahtlos auf Ihre clouddressourcen zugreifen können. Der Punkt-zu-Standort-VPN-Zugriff für Mandanten bedeutet, dass Mandanten Administratoren jederzeit eine Verbindung mit Ihren virtuellen Netzwerken in Ihrem Rechenzentrum herstellen können, um Ihre Ressourcen zu verwalten. BGP bietet dynamisches Routing und behält die Mandanten mit ihren Assets, auch wenn Netzwerkprobleme im Internet oder an anderen Orten auftreten. Mit NAT können Mandanten-VMS eine Verbindung mit Ressourcen im Internet herstellen, z. b. Kreditkarten-Verarbeitungs Ressourcen.

## RAS-Gateway-Verwaltungs Tools

Im folgenden finden Sie die Verwaltungs Tools für das RAS-Gateway.

- In Windows Server 2016 müssen Sie zum Bereitstellen eines RAS-gatewayrouters Windows PowerShell-Befehle verwenden. Weitere Informationen finden Sie unter [Remote Zugriffs-Cmdlets](#) für Windows Server 2016 und Windows 10.
- In System Center 2012 R2 Virtual Machine Manager (VMM) wird das RAS-Gateway als Windows Server-Gateway bezeichnet. In der VMM-Softwareschnittstelle sind eine begrenzte Anzahl von Border Gateway Protocol (BGP)-Konfigurationsoptionen verfügbar, einschließlich **lokaler BGP-IP-Adresse** und **autonomer System Nummern (ASN)**, **Liste der BGP-Peer-IP-Adressen** und **ASN-Werte**. Sie können jedoch Windows PowerShell-BGP-Befehle per Remotezugriff verwenden, um alle anderen Features des Windows Server-Gateways zu konfigurieren. Weitere Informationen finden Sie unter [Virtual Machine Manager \(VMM\)](#) und [Remote Zugriffs-Cmdlets](#) für Windows Server 2016 und Windows 10.

## Verwandte Themen

- [RAS-Gateway: Hohe Verfügbarkeit](#)
- [GRE-Tunneling in Windows Server](#)
- [GRE-Tunneling für RAS-Gateway: Durchsatz und Leistung](#)

# GRE-Tunneling in Windows Server 2016

27.03.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 bietet Aktualisierungen der allgemeinen Routing Kapselung (GRE-) Tunnel Funktion für das RAS-Gateway.

GRE ist ein einfaches Tunneling-Protokoll, das eine Vielzahl von Protokollen der Vermittlungsschicht in virtuellen Point-to-Point-Links über ein IP-Internetwerk kapseln kann. Die Microsoft GRE-Implementierung kann IPv4 und IPv6 Kapseln.

GRE-Tunnel sind in vielen Szenarien nützlich:

- Sie sind einfach und RFC 2890 kompatibel, sodass Sie mit verschiedenen Hersteller Geräten interoperabel sind.
- Sie können Border Gateway Protocol (BGP-) für dynamisches Routing verwenden.
- Sie können mehr Instanzen fähige GRE-RAS-Gateways für die Verwendung mit Software-Defined Networking (Sdn konfigurieren)
- Sie können System Center Virtual Machine Manager zum Verwalten von GRE-basierten RAS-Gateways verwenden.
- Sie können einen Durchsatz von bis zu 2,0 Gbit/s auf einem virtuellen Computer mit 6 Kernen erzielen, der als GRE-RAS-Gateway konfiguriert ist.
- Ein einzelnes Gateway unterstützt mehrere Verbindungs Modi.

GRE-basierte Tunnel ermöglichen Verbindungen zwischen virtuellen Mandantennetzwerken und externen Netzwerken. Da das GRE-Protokoll einfach ist und die Unterstützung für GRE auf den meisten Netzwerkgeräten verfügbar ist, ist es eine ideale Wahl für das Tunnelingverfahren, bei dem keine Datenverschlüsselung erforderlich ist.

Die GRE-Unterstützung in Standort-zu-Standort-Tunnels (S2S) löst das Problem der Weiterleitung zwischen virtuellen Mandanten Netzwerken und externen Mandanten Netzwerken mithilfe eines mehr Instanzen fähigen Gateways, wie weiter unten in diesem Thema beschrieben.

Die GRE-Tunnel Funktion ist so konzipiert, dass Sie die folgenden Anforderungen erfüllt:

- Ein Hostinganbieter muss virtuelle Netzwerke für die Weiterleitung erstellen können, ohne die Konfiguration des physischen Switches zu ändern.
  - Ein Hostinganbieter muss ihren extern ausgerichteten Netzwerken Subnetze hinzufügen können, ohne die Konfiguration der physischen Switches innerhalb der Infrastruktur zu ändern.
- Die GRE-Tunnel Funktion ermöglicht oder erweitert verschiedene wichtige Szenarien für das Hosten von Dienstanbietern mithilfe von Microsoft-Technologien zur Implementierung von Software-Defined Networking in ihren Dienst angeboten.

Im folgenden finden Sie einige Beispieldaten:

- [Zugriff von virtuellen Mandanten Netzwerken auf physische Mandanten Netzwerke](#)
- [Hoch Geschwindigkeits Konnektivität](#)

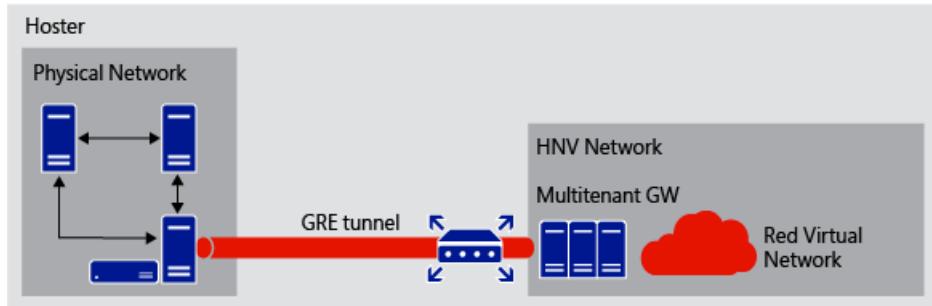
- Integration in VLAN-basierte Isolation
- Zugreifen auf freigegebene Ressourcen
- Dienste von Drittanbieter Geräten für Mandanten

## Wichtige Szenarien

Im folgenden finden Sie die wichtigsten Szenarien, die der GRE-Tunnel-Feature adressiert.

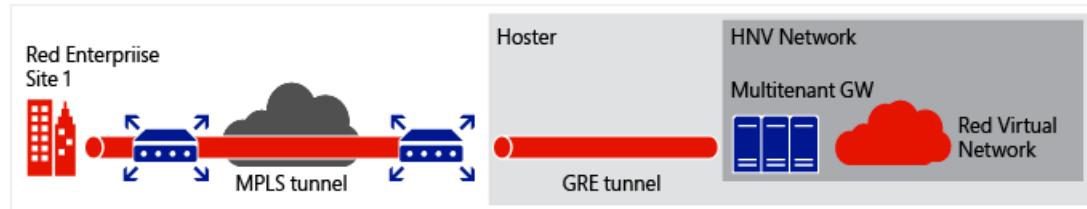
### Zugriff von virtuellen Mandanten Netzwerken auf physische Mandanten Netzwerke

Dieses Szenario ermöglicht eine skalierbare Möglichkeit, den Zugriff von virtuellen Mandanten Netzwerken auf physische Mandanten Netzwerke auf dem lokalen hostingdienstanbieter bereitzustellen. Ein GRE-Tunnelendpunkt wird auf dem mehr Instanzen fähigen Gateway eingerichtet, der andere GRE-Tunnelendpunkt wird auf einem Drittanbieter Gerät im physischen Netzwerk eingerichtet. Layer-3-Datenverkehr wird zwischen den virtuellen Computern im virtuellen Netzwerk und dem Drittanbieter Gerät im physischen Netzwerk weitergeleitet.



### Hoch Geschwindigkeits Konnektivität

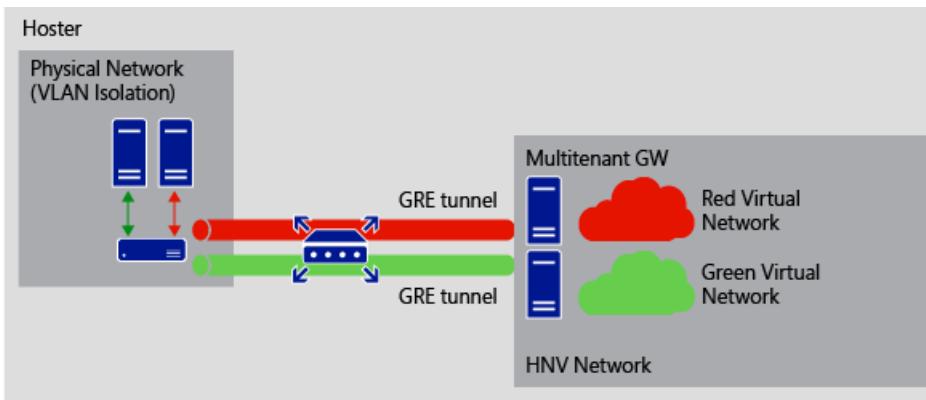
Dieses Szenario ermöglicht eine skalierbare Möglichkeit, eine hoch Geschwindigkeits Konnektivität zwischen dem lokalen Netzwerk des Mandanten und dem virtuellen Netzwerk im hostingdienstanbieter-Netzwerk bereitzustellen. Ein Mandant stellt über MPLS (Multiprotocol Label Switching) eine Verbindung mit dem Dienstanbieter Netzwerk her, bei der zwischen dem edgerouter des hostingdienstanbieters und dem mehr Instanzen fähigen Gateway und dem virtuellen Netzwerk des Mandanten ein GRE-Tunnel eingerichtet wird.



### Integration in VLAN-basierte Isolation

In diesem Szenario können Sie die VLAN-basierte Isolation mit der Hyper-V-Netzwerkvirtualisierung integrieren. Ein physisches Netzwerk im hostinganbieternetzwerk enthält ein Lasten Ausgleichs Modul, das die VLAN-basierte Isolation verwendet. Ein mehr Instanzen fähiges Gateway stellt GRE-Tunnel zwischen dem Load Balancer im physischen Netzwerk und dem mehr Instanzen fähigen Gateway im virtuellen Netzwerk her.

Zwischen Quelle und Ziel können mehrere Tunnel eingerichtet werden, und der GRE-Schlüssel wird verwendet, um zwischen den Tunnels zu unterscheiden.



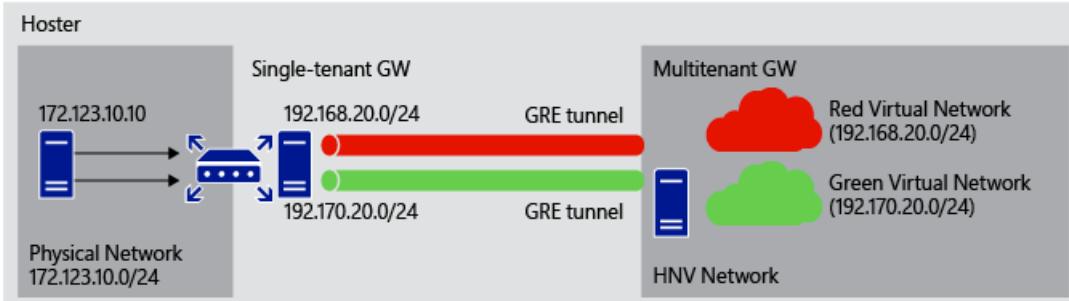
### Zugreifen auf freigegebene Ressourcen

In diesem Szenario können Sie auf freigegebene Ressourcen in einem physischen Netzwerk zugreifen, das sich im hostinganbieternetzwerk befindet.

Sie verfügen möglicherweise über einen gemeinsamen Dienst, der sich auf einem Server in einem physischen Netzwerk im hostinganbieternetzwerk befindet, das Sie für mehrere virtuelle Mandanten Netzwerke freigeben möchten.

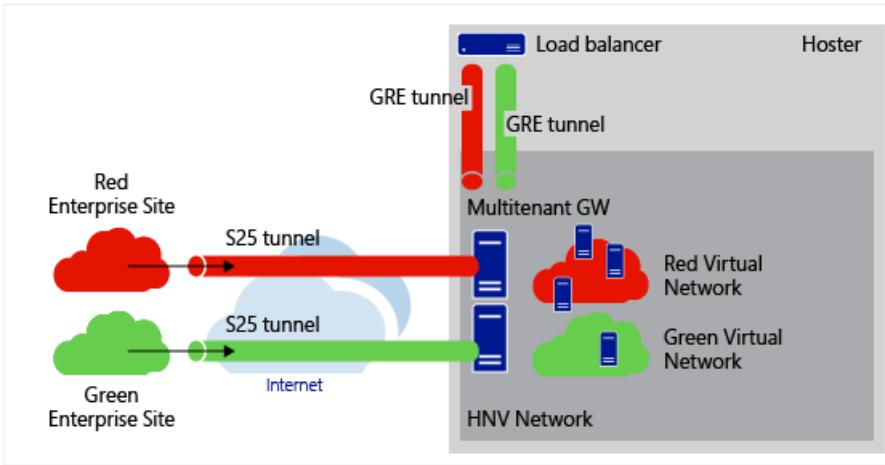
Die Mandanten Netzwerke mit nicht überlappenden Subnetzen greifen über einen GRE-Tunnel auf das gemeinsame Netzwerk zu. Eine einzige Mandanten-Gatewayroute zwischen den GRE-Tunneln, sodass Pakete an die entsprechenden Mandanten Netzwerke weitergeleitet werden.

In diesem Szenario kann das Gateway eines einzelnen Mandanten durch Hardware Geräte von Drittanbietern ersetzt werden.



### Dienste von Drittanbieter Geräten für Mandanten

Dieses Szenario kann verwendet werden, um Drittanbieter Geräte (z. b. Hardware-Lasten Ausgleichs Module) in den Daten Verkehrsfluss des virtuellen Mandanten Netzwerks zu integrieren. Beispielsweise wird der Datenverkehr von einem Unternehmens Standort über einen S2S-Tunnel an das mehr Instanzen fähige Gateway weitergeleitet. Der Datenverkehr wird über einen GRE-Tunnel an den Load Balancer weitergeleitet. Der Load Balancer leitet Datenverkehr an mehrere virtuelle Computer im virtuellen Netzwerk des Unternehmens weiter. Dasselbe geschieht für einen anderen Mandanten mit potenziell überlappenden IP-Adressen in den virtuellen Netzwerken. Der Netzwerk Datenverkehr wird mithilfe von VLANs auf dem Load Balancer isoliert und gilt für alle Layer 3-Geräte, von denen VLANs unterstützt werden.



## Konfiguration und Bereitstellung

Ein GRE-Tunnel wird als zusätzliches Protokoll innerhalb einer S2S-Schnittstelle verfügbar gemacht. Die Implementierung erfolgt auf ähnliche Weise wie ein IPSec-S2S-Tunnel, der im folgenden Netzwerk Blog beschrieben wird: mehr Instanzen fähige [Site-to-Site \(S2S\)-VPN Gateway mit Windows Server 2012 R2](#)

Im folgenden Thema finden Sie ein Beispiel für die Bereitstellung von Gateways, einschließlich GRE-Tunnel Gateways:

[Bereitstellen einer Software definierten Netzwerkinfrastruktur mithilfe von Skripts](#)

## Weitere Informationen

Weitere Informationen zum Bereitstellen von S2S-Gateways finden Sie in den folgenden Themen:

- [RAS-Gateway](#)
- [Border Gateway Protocol \(BGP\)](#)
- [Neu! Bereitstellungs Handbuch für das mehr Instanzen fähige Windows Server 2012 R2 RAS-Gateway](#)
- [Bereitstellen von Border Gateway Protocol \(BGP\) mit dem mehr Instanzen fähigen RAS-Gateway](#)

# RAS-Gateway GRE-Tunneling Durchsatz und Leistung

09.04.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server (halbjährlicher Kanal)

In diesem Thema erfahren Sie mehr über RAS-Server (RAS-) generische Routing Kapselung (GRE) Tunnel Leistung unter Windows Server, Version 1709, in einem nicht von Software definierten Netzwerk (Sdn-) basierten Testumgebung.

RAS-Gateway ist ein Software Router und ein Gateway, das Sie im Einzel Mandanten Modus oder im mehr Instanzen fähigen Modus verwenden können. In diesem Thema wird eine Konfiguration mit einem einzelnen Mandanten Modus mit hoher Verfügbarkeit und Failoverclustering behandelt. Die in diesem Thema dargestellten GRE-Tunnel Leistungsstatistiken gelten für das RAS-Gateway sowohl für den Single-Mandanten als auch für den mehr Instanzen fähigen Modus.

## NOTE

Failoverclustering ist eine Windows Server-Funktion, mit der Sie mehrere Server in einem fehlertoleranten Cluster gruppieren können. Weitere Informationen finden Sie unter [Failover-Clustering](#).

Der Modus für einzelne Mandanten ermöglicht Organisationen beliebiger Größe das Bereitstellen des Gateways als Äußeres oder Internet-das virtuelle private Netzwerk (VPN)-Server. Im Einzel Mandanten Modus können Sie das RAS-Gateway auf einem physischen Server oder virtuellen Computer (VM-)bereitstellen. In diesem Thema wird die Bereitstellung von RAS-Gateways auf zwei Virtual Machines () VMS beschrieben, die in einem Failovercluster konfiguriert sind.

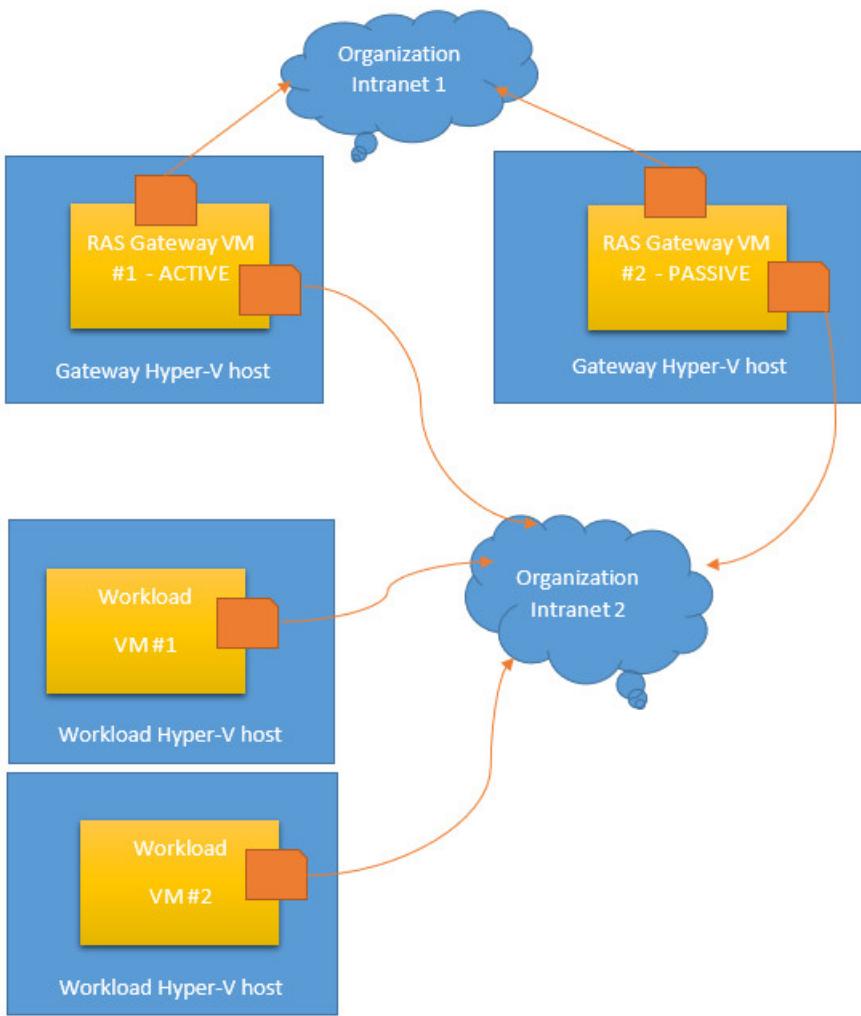
## IMPORTANT

Da GRE-Tunnel Kapselung, aber keine Verschlüsselung bereitstellen, sollten Sie das mit GRE konfigurierte RAS-Gateway nicht als Internet Edge-Gateway verwenden. Informationen zu den besten Verwendungsmöglichkeiten für das RAS-Gateway mit GRE-Tunneln finden Sie unter [GRE-Tunnelung in Windows Server](#).

GRE ist ein Lightweight-Tunnelingprotokoll, das eine Vielzahl von Protokollen der Netzwerkschicht innerhalb von virtuellen Punkten--Punkt Verknüpfungen über ein Internet Protokoll-Netzwerk Kapseln kann. Die Microsoft GRE-Implementierung kapselt sowohl IPv4 als auch IPv6.

Weitere Informationen finden Sie im Abschnitt **Bereitstellungs Szenarien für RAS-Gateways** im Thema [RAS-Gateway](#).

In diesem Testszenario, das in der folgenden Abbildung dargestellt wird, wird der gemessene Daten Verkehrsfluss vom Unternehmens Intranet 2 in das Unternehmens Intranet 1 verlagert. Virtuelle Computer für die Arbeitsauslastung von Mandanten senden Netzwerk Datenverkehr von Intranet 2 an Intranet 1 mithilfe des RAS-Gateways.



## Konfiguration der Test Umgebung

Dieser Abschnitt enthält Informationen über die Testumgebung und die Konfiguration des RAS-Gateways.

In der Testumgebung werden RAS-Gateway-VMS auf Hyper-V-Hosts in einem Failovercluster bereitgestellt, um Hochverfügbarkeit zu erhalten.

### Hyper-V-Host Konfiguration

Zwei Hyper-V-Hosts werden so konfiguriert, dass das Testszenario auf folgende Weise unterstützt wird.

- Zwei zweiseitig vernetzte physische Computer werden mit Windows Server konfiguriert, Version 1709
- Die beiden physischen Netzwerkadapter auf jedem der beiden Server sind mit unterschiedlichen Subnetzwerken verbunden, die beide Subnetze eines Unternehmensintranets darstellen. Sowohl Netzwerke als auch unterstützende Hardware verfügen über eine Kapazität von 10 Gbit/s.
- Hyperthreading auf den physischen Servern ist deaktiviert. Dies ermöglicht den maximalen Durchsatz von den physischen NICs.
- Die Hyper-V-Server Rolle wird auf beiden Servern installiert und mit zwei externen virtuellen Hyper-V-Switches konfiguriert, einer für jeden physischen Netzwerkadapter.
- Da beide Server mit demselben Intranet verbunden sind, können die Server miteinander kommunizieren.
- Die Hyper-V-Hosts werden in einem Failovercluster über das Intranet-Netzwerk konfiguriert.

#### NOTE

Weitere Informationen finden Sie unter [Hyper-V Virtual Switch](#).

## VM-Konfiguration

Zwei virtuelle Computer werden so konfiguriert, dass das Testszenario auf folgende Weise unterstützt wird.

- Auf jedem Server wird ein virtueller Computer installiert, auf dem Windows Server, Version 1709, ausgeführt wird. Jeder virtuelle Computer ist mit 10 Kernen und 8 GB RAM konfiguriert.
- Jeder virtuelle Computer wird auch mit zwei virtuellen Netzwerkadapters konfiguriert. Ein virtueller Netzwerkadapter ist mit dem virtuellen Switch für intranet1 verbunden, und der andere virtuelle Netzwerkadapter ist mit dem virtuellen Switch für intranet2 verbunden.
- Auf jedem virtuellen Computer ist das RAS-Gateway installiert und als GRE--basierter VPN-Server konfiguriert.
- Die Gateway-VMS werden in einem Failovercluster konfiguriert. Wenn Sie gruppiert sind, ist eine VM aktiv, und die andere VM ist passiv.

## Arbeitsauslastung Hyper-V-Hosts und VMS

Für diesen Test werden zwei Arbeits Auslastungen von Hyper-V-Hosts im Intranet installiert, und auf jedem Host ist eine VM installiert. Wenn Sie diesen Test in ihrer eigenen Testumgebung duplizieren, können Sie so viele Arbeits Auslastungs Server und VMS installieren, wie es für Ihre Zwecke geeignet ist.

- Bei der Arbeitsauslastung von Hyper-V-Hosts ist ein physischer Netzwerkadapter installiert, der mit dem Unternehmens Intranet verbunden ist.
- Im virtuellen Hyper-V-Switch wird auf jedem Host ein virtueller Switch erstellt. Der Switch ist extern und wird an den Netzwerkadapter gebunden, der mit dem Intranet verbunden ist.
- Die Arbeits Auslastungs-VMS werden mit 2 GB RAM und 2 Kernen konfiguriert.
- Die Arbeits Auslastungs-VMS verfügen jeweils über einen virtuellen Netzwerkadapter, der mit dem virtuellen Intranet-Switch verbunden ist.

## Traffic Generator-Tool

Das Tool für den Datenverkehrs Generator, das in diesem Test verwendet wird, ist das cttraffic-Tool. Das git-Repository für dieses Tool befindet sich unter <https://github.com/Microsoft/ctsTraffic>.

## Leistung des RAS-Gateways

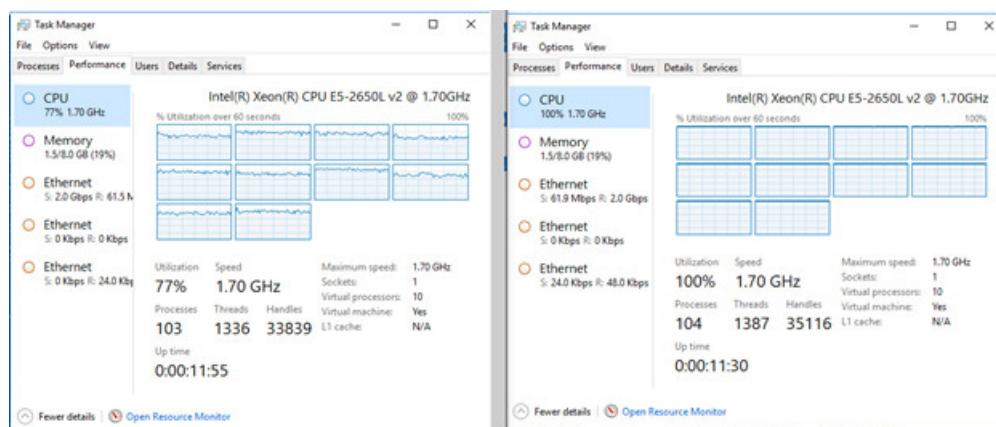
In den Abbildungen in diesem Abschnitt werden die Task-Manager-anzeigen von GRE-Tunnel Durchsatz mit mehreren TCP-Verbindungen dargestellt.

Sie können einen Durchsatz von bis zu 2,0 Gbit/s auf mehreren-Core-VMS erzielen, die als GRE-RAS-Gateways konfiguriert sind.

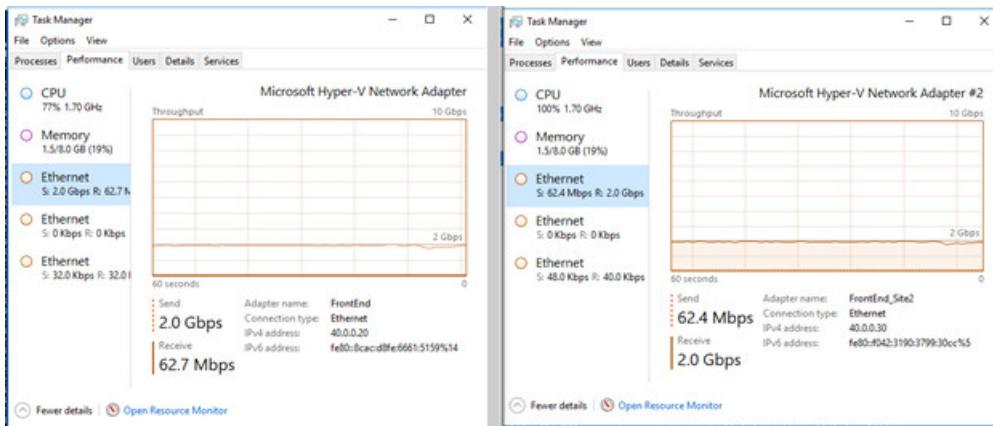
## GRE-Tunnel Leistung mit mehreren TCP-Sitzungen

Bei mehreren TCP-Sitzungen erreicht die CPU-Auslastung 100%, und der maximale Durchsatz im GRE-Tunnel beträgt 2,0 Gbit/s.

In der folgenden Abbildung wird die CPU-Auslastung für beide RAS-Gateway-VMS dargestellt. Die aktive VM, RAS-Gateway-VM-#1, befindet sich auf der linken Seite, während sich die passive VM, RAS-Gateway-VM #2, auf der rechten Seite befindet.



In der folgenden Abbildung wird der Ethernet-Netzwerk Durchsatz auf den virtuellen RAS-Gateway-Computern dargestellt. Die aktive VM, RAS-Gateway-VM-#1, befindet sich auf der linken Seite, während sich die passive VM, RAS-Gateway-VM #2, auf der rechten Seite befindet.

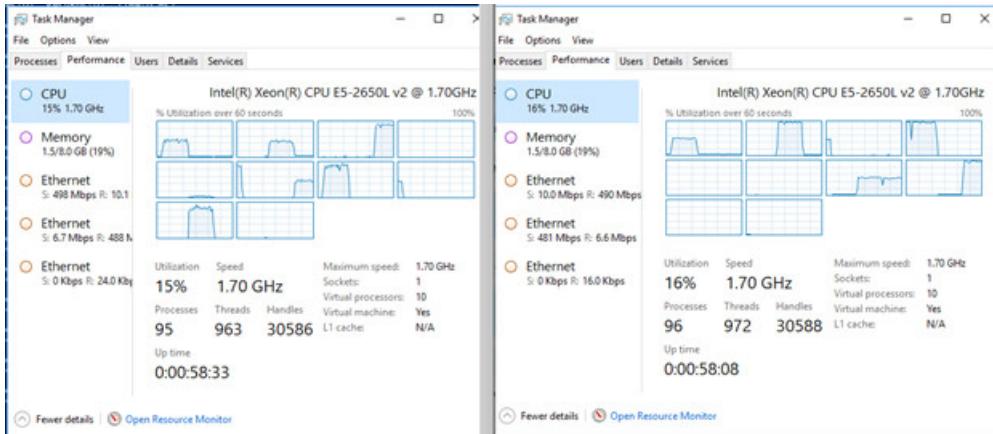


### **GRE-Tunnel Leistung mit einer TCP-Verbindung**

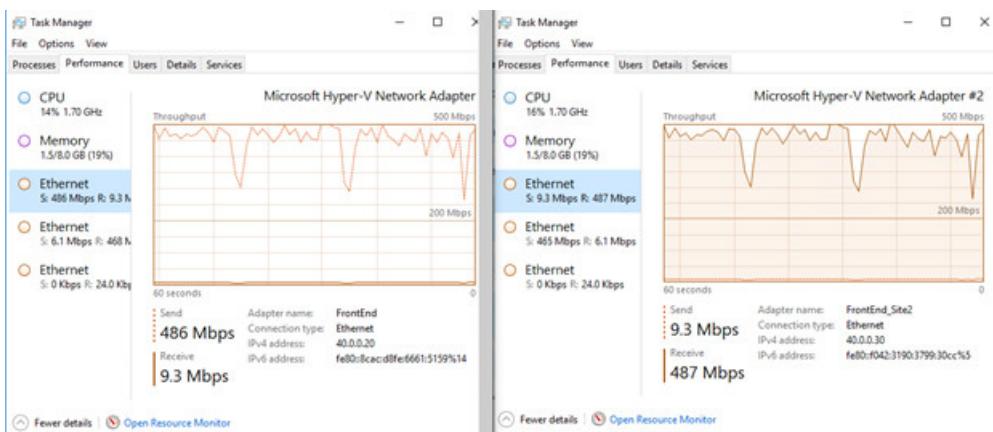
Wenn die Testkonfiguration von mehreren TCP-Sitzungen in eine einzelne TCP-Sitzung geändert wurde, erreicht nur ein CPU-Kern die maximale Kapazität der RAS-Gateway-VMS.

Der maximale Durchsatz im GRE-Tunnel liegt zwischen 400-500 Mbit/s.

In der folgenden Abbildung wird die CPU-Auslastung für beide RAS-Gateway-VMS dargestellt. Die aktive VM, RAS-Gateway-VM-#1, befindet sich auf der linken Seite, während sich die passive VM, RAS-Gateway-VM #2, auf der rechten Seite befindet.



In der folgenden Abbildung wird der Ethernet-Netzwerk Durchsatz auf den virtuellen RAS-Gateway-Computern dargestellt. Die aktive VM, RAS-Gateway-VM-#1, befindet sich auf der linken Seite, während sich die passive VM, RAS-Gateway-VM #2, auf der rechten Seite befindet.



Weitere Informationen zur Leistung des RAS-Gateways finden Sie unter [HNV Gateway Performance Tuning in](#)

Software Defined Networks.

# RAS-Server-Rolle-Dokumentation

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die Remote Zugriffs-Server Rollen Dokumentation enthält Anweisungen zum Bereitstellen der drei Rollen Dienste (Always on VPN-, Routing-und RAS-Diensts, webanwendungsproxy) einzeln oder auf demselben Server. Diese Dokumente gelten z. b. für Situationen, in denen Sie eine beliebige Kombination der drei Rollen Dienste bereitgestellt haben, z. b. das Bereitstellen von RRAS und DirectAccess auf demselben Server.

# Bereitstellen des Remotezugriffs in einem Unternehmen

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält eine Einführung in das DirectAccess-Szenario für das Unternehmen.

## IMPORTANT

Zum Bereitstellen von DirectAccess mithilfe dieser Anleitung müssen Sie einen DirectAccess-Server verwenden, auf dem Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird.

Bevor Sie mit der Bereitstellung beginnen, sollten Sie sich die folgende Liste mit nicht unterstützten Konfigurationen, bekannten Problemen und Voraussetzungen ansehen:

- [DirectAccess: Nicht unterstützte Konfigurationen](#)
- [DirectAccess: Bekannte Probleme](#)
- [Voraussetzungen für die Bereitstellung von DirectAccess](#)

## Szenariobeschreibung

Der Remotezugriff bietet eine Reihe von Unternehmensfeatures, u. a. das Bereitstellen mehrerer Remotezugriffsserver in einem Cluster, in dem der Lastausgleich mithilfe des Windows-Netzwerklastenausgleichs oder eines externen Lastenausgleichs vorgenommen wird, das Einrichten einer Bereitstellung für mehrere Standorte mit Remotezugriffsservern, die sich an unterschiedlichen geografischen Standorten befinden, und das Bereitstellen von DirectAccess mit zweistufiger Clientauthentifizierung unter Verwendung eines Einmalkennworts (One-Time Passwort, OTP).

## Inhalt dieses Szenarios

Jedes Unternehmensszenario wird in einem Dokument beschrieben, das Anweisungen zur Planung und zur Bereitstellung einschließt. Weitere Informationen finden Sie unter:

- [Bereitstellen des Remote Zugriffs in einem Cluster](#)
- [Bereitstellen mehrerer RAS-Server in einer Bereitstellung mit mehreren Standorten](#)
- [Bereitstellen des Remotezugriffs mit OTP-Authentifizierung](#)
- [Bereitstellen von Remote Zugriff in einer Umgebung mit mehreren Gesamtstrukturen](#)

## Praktische Anwendungen

Remotezugriffsszenarios in einem Unternehmen bieten Folgendes:

- **Erhöhung der Verfügbarkeit.** Das Bereitstellen mehrerer Remote Zugriffs Server in einem Cluster bietet

Skalierbarkeit und erhöht die Kapazität für Durchsatz und Anzahl der Benutzer. Die Verwendung des Lastenausgleichs im Cluster sorgt für hohe Verfügbarkeit. Wenn ein Server im Cluster ausfällt, können Remotebenutzer weiterhin über einen anderen Server im Cluster auf das interne Unternehmensnetzwerk zugreifen. Das Failover erfolgt unbemerkt, wenn der Client mithilfe einer virtuellen IP-Adresse (VIP) eine Verbindung mit dem Cluster herstellt.

- **Einfache Verwaltung.** Ein Cluster oder eine Bereitstellung mit mehreren Standorten kann mithilfe der Remote Zugriffs-Verwaltungskonsole, die auf einem der Cluster Server ausgeführt wird, als einzelne Entität konfiguriert und verwaltet werden. Darüber hinaus bietet eine Bereitstellung für mehrere Standorte Administratoren die Möglichkeit, die Remotezugriffsbereitstellung an Active Directory-Standorten auszurichten, wodurch eine einfachere Architektur erzielt wird. Gemeinsam genutzte Einstellungen können problemlos clusterserverübergreifend oder auf allen Einstiegspunktservern der Mehrstandort-Bereitstellung festgelegt werden. Die Remotezugriffseinstellungen können von jedem beliebigen Server im Cluster oder in der Bereitstellung und – mithilfe der Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT) – auch von einem Remotecomputer aus verwaltet werden. Darüber hinaus kann der ganze Cluster bzw. die Bereitstellung für mehrere Standorte über eine einzelne Remotezugriffs-Verwaltungskonsole überwacht werden.
- **Kosteneffizienz** Mithilfe einer Remote Zugriffs Bereitstellung für mehrere Standorte können Unternehmen Remote Zugriffs Server an mehreren Standorten bereitstellen, die den Client Standorten entsprechen. Hierdurch verfügen Remoteclients unabhängig von ihrem Standort über berechenbare Zugriffsmöglichkeiten, die gleichzeitig zur Senkung von Kosten und Intranetbandbreite beitragen, indem der Clientdatenverkehr über das Internet zu dem nächstgelegenen Remotezugriffsserver weitergeleitet wird.
- **Sicherheit.** Durch die Bereitstellung einer starken Client Authentifizierung mit einem einmaligen Kennwort anstelle von Standard Active Directory Kennwort erhöht sich die Sicherheit.

## In diesem Szenario enthaltene Rollen und Features

In der folgenden Tabelle sind die für das Unternehmensszenario erforderlichen Rollen und Features aufgeführt:

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Remotezugriffs-Serverrolle	<p>Diese Rolle wird mithilfe der Server-Manager-Konsole installiert und deinstalliert. Diese Rolle umfasst DirectAccess (zuvor ein Feature unter Windows Server 2008 R2) sowie die Routing- und RAS-Dienste (zuvor ein Rollendienst unter der Serverrolle für Netzwerkrichtlinien- und Zugriffsdienste). Die Remotezugriffs-Rolle besteht aus zwei Komponenten:</p> <ol style="list-style-type: none"> <li>1. DirectAccess und RRAS (Routing and Remote Access Services): VPN-DirectAccess und VPN werden in der Remote Zugriffs-Verwaltungskonsole verwaltet.</li> <li>2. RRAS-Routing-RRAS-Routing Features werden in der Legacy-Routing-und Remote Zugriffs Konsole verwaltet.</li> </ol> <p>Die Remotezugriffs-Serverrolle ist von den folgenden Serverfeatures abhängig:</p> <ul style="list-style-type: none"> <li>-Internetinformationsdienste (IIS): dieses Feature ist erforderlich, um den Netzwerkadressen Server und den Standardweb Test zu konfigurieren.</li> <li>-Gruppenrichtlinien-Verwaltungskonsole Feature-Feature ist für DirectAccess erforderlich, um die Gruppenrichtlinie Objekte (GPOs) in Active Directory zu erstellen und zu verwalten, und muss als erforderliches Feature für die Server Rolle installiert werden.</li> </ul>

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Feature "Tools für die Remotezugriffsverwaltung"	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"> <li>-Sie wird standardmäßig auf einem RAS-Server installiert, wenn die Remote Zugriffs Rolle installiert ist, und unterstützt die Benutzeroberfläche der Remote Verwaltungskonsole.</li> <li>-Es kann optional auf einem Server installiert werden, auf dem die Remote Zugriffs-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.</li> </ul> <p>Das Feature "Tools für die Remotezugriffsverwaltung" besteht aus den folgenden Komponenten:</p> <ol style="list-style-type: none"> <li>1. Remote Zugriffs-GUI und Befehlszeilen Tools</li> <li>2. Remote Zugriffs Modul für Windows PowerShell</li> </ol> <p>Abhängigkeiten umfassen:</p> <ol style="list-style-type: none"> <li>1. Gruppenrichtlinien-Verwaltungskonsole</li> <li>2. RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li> <li>3. Windows PowerShell 3,0</li> <li>4. grafische Verwaltungs Tools und Infrastruktur</li> </ol>
Windows-Netzwerklastenausgleich	Dieses Feature ermöglicht den Lastenausgleich für mehrere Remotezugriffsserver.

# Bereitstellen des Remotezugriffs in einem Cluster

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess- und RAS-Dienst (RAS-)VPN zu einer einzigen Remote Zugriffs Rolle. Sie können den Remote Zugriff in einer Reihe von Unternehmens Szenarios bereitstellen. Diese Übersicht bietet eine Einführung in das Unternehmens Szenario für die Bereitstellung mehrerer RAS-Server in einem Cluster Lastenausgleich mit Windows-Netzwerk Lastenausgleich (NLB) oder mit einem externen Lasten Ausgleichs Modul (ELB), wie z. b. F5 Big-IP.

## Szenariobeschreibung

Eine Cluster Bereitstellung sammelt mehrere RAS-Server in einer einzelnen Einheit, die dann als einzelner Kontaktpunkt für Remote Client Computer fungiert, die über DirectAccess oder VPN eine Verbindung mit dem internen Unternehmensnetzwerk herstellen, indem die externe virtuelle IP-(VIP) Adresse des Remote Zugriffs Clusters verwendet wird. Der Lastenausgleich für den Datenverkehr zum Cluster erfolgt mithilfe von Windows NLB oder mit einem externen Lasten Ausgleichs Modul (z. b. F5 Big-IP-).

## Erforderliche Komponenten

Bevor Sie mit der Bereitstellung dieses Szenarios beginnen, sollten Sie die Liste der wichtigen Anforderungen lesen:

- Standardlastenausgleich über Windows NLB.
- Externer Lastenausgleich wird unterstützt.
- Der Unicast-Modus ist der standardmäßige und empfohlene Modus für den NLB.
- Das Ändern von Richtlinien außerhalb der DirectAccess-Verwaltungskonsole oder von PowerShell-Cmdlets wird nicht unterstützt.
- Wenn NLB oder ein externer Lastenausgleich verwendet wird, kann das IPHTTPS-Präfix nicht in /59 geändert werden.
- Die Lastenausgleichsknoten müssen sich im gleichen IPv4-Subnetz befinden.
- Wenn bei ELB-bereit Stellungen Manage out erforderlich ist, können DirectAccess-Clients nicht Teredo verwenden. Nur IPHTTPS können für End-verwendet werden, um die Kommunikation-Ende zu beenden.
- Stellen Sie sicher, dass alle bekannten NLB-/ELB-Hotfixes installiert sind.
- ISATAP wird im Unternehmensnetzwerk nicht unterstützt. Wenn Sie ISATAP verwenden, sollten Sie es entfernen und das systemeigene IPv6 verwenden.

## Inhalt dieses Szenarios

Das Clusterbereitstellungsszenario umfasst eine Reihe von Schritten:

1. Stellen Sie [einen Always on-VPN-Server mit erweiterten Optionen](#) bereit. Bevor eine Cluster Bereitstellung eingerichtet wird, muss ein einzelner Remote Zugriffs Server mit erweiterten Einstellungen bereitgestellt werden.
2. [Planen Sie die Bereitstellung eines Remote Zugriffs Clusters](#). Um einen Cluster aus einer einzelnen Server

Bereitstellung zu erstellen, sind einige zusätzliche Schritte erforderlich, einschließlich der Vorbereitung von Zertifikaten für die Cluster Bereitstellung.

3. [Konfigurieren Sie einen Remote Zugriffs Cluster](#). Dies umfasst eine Reihe von Konfigurationsschritten, einschließlich der Vorbereitung des einzelnen Servers für Windows NLB oder des externen Load Balancers, der Vorbereitung zusätzlicher Server für den Cluster Beitritt und dem Aktivieren des Lasten Ausgleichs.

## Praktische Anwendungen

Der Zusammenschluss mehrerer Server zu einem Servercluster bietet Folgendes:

- Skalierbarkeit. Ein einzelner RAS-Server bietet ein eingeschränktes Maß an Server Zuverlässigkeit und skalierbarer Leistung. Durch die Gruppierung der Ressourcen von zwei oder mehr Servern zu einem einzigen Cluster können Sie die verfügbare Kapazität für die Benutzer und den Durchsatz erhöhen.
- Hohe Verfügbarkeit: Ein Cluster bietet hohe Verfügbarkeit für den Zugriff immer-. Wenn ein Server im Cluster ausfällt, können Remotebenutzer weiterhin über einen anderen Server im Cluster auf das Unternehmensnetzwerk zugreifen. Alle Server im Cluster verfügen über denselben Satz virtueller IP-Adressen (VIP-) Adressen, während gleichzeitig eine eindeutige, dedizierte IP-Adresse für jeden Server beibehalten wird.
- Vereinfachen Sie die-der-Verwaltung. Ein Cluster ermöglicht die Verwaltung mehrerer Server als einzelne Entität. Gemeinsam genutzte Einstellungen können problemlos clusterserverübergreifend festgelegt werden. Remote Zugriffs Einstellungen können von einem beliebigen Server im Cluster oder Remote mithilfe Remoteserver-Verwaltungstools (RSAT-)verwaltet werden. Darüber hinaus kann der ganze Cluster über eine einzelne Remotezugriffs-Verwaltungskonsole überwacht werden.

## In diesem Szenario enthaltene Rollen und Features

Die folgende Tabelle enthält die für dieses Szenario erforderlichen Rollen und Features:

ROLLEN/FUNKTION	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Remotezugriffs-Rolle	Diese Rolle wird mithilfe der Server-Manager-Konsole installiert und deinstalliert. Sie umfasst DirectAccess (zuvor ein Feature in Windows Server 2008 R2) und Routing-und RAS-Dienste (RRAS-), das zuvor ein Rollen Dienst unter der Netzwerk Richtlinien-und Zugriffs Dienste (NPAS) Server Rolle war. Die Remotezugriffs-Rolle besteht aus zwei Komponenten: -Always on VPN-und Routing-und RAS-Dienste (RRAS) VPN-DirectAccess und VPN werden in der Remote Zugriffs-Verwaltungskonsole verwaltet. -RRAS-Routing: RRAS-Routing Features werden in der Legacy-Routing-und Remote Zugriffs Konsole verwaltet.  Es bestehen folgende Abhängigkeiten: -Internetinformationsdienste (IIS)-Webserver: dieses Feature ist erforderlich, um den Netzwerkadressen Server und den Standardweb Test zu konfigurieren. -Interne Windows-Datenbank: wird für die lokale Kontoführung auf dem Remote Zugriffs Server verwendet.

ROLLEN/FUNKTION	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Feature "Tools für die Remotezugriffsverwaltung":  Diese Funktion ermöglicht die Verwaltung von DirectAccess und VPN auf einem RAS-Server. Sie kann optional auf einem Server installiert werden, auf dem die Remote Zugriffs Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"> <li>-Sie wird standardmäßig auf einem RAS-Server installiert, wenn die Remote Zugriffs Rolle installiert ist, und unterstützt die Benutzeroberfläche der Remote Verwaltungskonsole.</li> <li>-Es kann optional auf einem Server installiert werden, auf dem die Remote Zugriffs-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.</li> </ul> <p>Das Feature "Tools für die Remotezugriffsverwaltung" besteht aus den folgenden Komponenten:</p> <ul style="list-style-type: none"> <li>-Remote Zugriffs-GUI und Befehlszeilen Tools</li> <li>-Remote Zugriffs Modul für Windows PowerShell</li> </ul> <p>Abhängigkeiten umfassen:</p> <ul style="list-style-type: none"> <li>-Gruppenrichtlinien-Verwaltungskonsole</li> <li>-RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li> <li>-Windows PowerShell 3,0</li> <li>-Tools und Infrastruktur für die grafische Verwaltung</li> </ul>
Netzwerklastenausgleich	Dieses Feature ermöglicht den Lastenausgleich in einem Cluster mithilfe des Windows-Netzwerklastenausgleichs.

## Hardwareanforderungen

Für dieses Szenario müssen die folgenden Hardwareanforderungen erfüllt werden:

- Mindestens zwei Computer, die die Hardwareanforderungen für Windows Server 2012 erfüllen.
- Für das externe Load Balancer Szenario ist dedizierte Hardware erforderlich (d. h. F5 BigIP).
- Um das Szenario zu testen, müssen Sie mindestens einen Computer mit Windows 10 als Always on VPN-Client konfiguriert haben.

## Software Anforderungen

Für dieses Szenario gelten eine Reihe von Anforderungen:

- Softwareanforderungen für die Bereitstellung auf einem Einzelserver. Weitere Informationen finden Sie [unter Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#). Ein einzelner Remote Zugriff).
- Zusätzlich zu den Softwareanforderungen für einen einzelnen Server gibt es eine Reihe von Cluster-spezifischen Anforderungen:
  - Auf jedem Cluster Server muss der IP--Name des HTTPS-Zertifikat Antragstellers der ConnectTo-Adresse entsprechen. Eine Cluster Bereitstellung unterstützt eine Mischung aus Platzhalter-und nicht-Platzhalter Zertifikaten auf Cluster Servern.
  - Wenn der Netzwerkadressenserver auf dem Remotezugriffsserver installiert ist, muss das Netzwerkadressenserver-Zertifikat auf jedem Clusterserver den gleichen Antragstellernamen aufweisen. Darüber hinaus darf der Name des Netzwerkadressenserver-Zertifikats nicht mit dem Namen eines beliebigen Servers in der DirectAccess-Bereitstellung identisch sein.

- IP--HTTPS- und Netzwerkadressen Server-Zertifikate müssen mit derselben Methode ausgestellt werden, mit der das Zertifikat für den einzelnen Server ausgestellt wurde. Wenn der einzelne Server beispielsweise eine öffentliche Zertifizierungsstelle (ca) verwendet, müssen alle Server im Cluster über ein Zertifikat verfügen, das von einer öffentlichen Zertifizierungsstelle ausgestellt wurde. Wenn der einzelne Server ein selbst-signiertes Zertifikat für IP--HTTPS verwendet, müssen alle Server im Cluster ebenfalls entsprechend vorgehen.
- Das IPv6-Präfix, das DirectAccess-Clientcomputern in Serverclustern zugewiesen wird, muss 59 Bit umfassen. Wenn VPN aktiviert ist, muss das VPN-Präfix ebenfalls 59 Bit umfassen.

## Bekannte Probleme

Im Folgenden finden Sie bekannte Probleme beim Konfigurieren eines Clusterszenarios:

- Nach dem Konfigurieren von DirectAccess in einem IPv4--nur die Bereitstellung mit einem einzelnen Netzwerkadapter und nach dem standardmäßigen DNS64 (die IPv6-Adresse, die ": 3333::" enthält) automatisch auf dem Netzwerkadapter konfiguriert wird, wird beim Versuch, den Lasten-Ausgleich über die Remote Zugriffs-Verwaltungskonsole zu aktivieren, eine Eingabeaufforderung für den Benutzer bereitgestellt. Wenn eine IPv6-DIP-Adresse angegeben wird, tritt nach dem Klicken auf **Commit ausführen** ein Konfigurationsfehler mit folgender Fehlermeldung auf: Der Parameter ist falsch.

So lösen Sie dieses Problem:

1. Laden Sie die Sicherung herunter, und stellen Sie Skripts aus [Back up and Restore Remote Access Configuration](#) wieder her.
2. Sichern Sie die Remote Zugriffs-Gruppenrichtlinien Objekte mithilfe der heruntergeladenen Skript Sicherung-"remoteaccess.ps1".
3. Versuchen Sie, den Lastenausgleich bis zu dem Schritt zu aktivieren, bei dem ein Fehler auftritt. Erweitern Sie im Dialogfeld Lastenausgleich aktivieren den Bereich Details, klicken Sie mit der rechten-in den Detailbereich, und klicken Sie dann auf **Skript kopieren**.
4. Öffnen Sie Editor, und fügen Sie den Inhalt der Zwischenablage ein. Beispiel:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress @('10.244.4.19
/255.255.255.0', 'fdc4:29bd:abde:3333::2/128') -InternetVirtualIPAddress
@('fdc4:29bd:abde:3333::1/128', '10.244.4.21 /255.255.255.0') -ComputerName
'DA1.domain1.corp.contoso.com' -Verbose
```

5. Schließen Sie alle offenen Remotezugriffs-Dialogfelder und die Remotezugriffs-Verwaltungskonsole.
6. Bearbeiten Sie den eingefügten Text, und entfernen Sie die IPv6-Adressen. Beispiel:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress @('10.244.4.19 /255.255.255.0') -
InternetVirtualIPAddress @('10.244.4.21 /255.255.255.0') -ComputerName
'DA1.domain1.corp.contoso.com' -Verbose
```

7. Führen Sie den Befehl aus dem vorherigen Schritt in einem PowerShell-Fenster mit erhöhten Rechten aus.
8. Wenn das Cmdlet fehlschlägt, während es ausgeführt wird (nicht aufgrund falscher Eingabewerte), führen Sie den Befehl `Restore-remoteaccess.ps1` aus, und befolgen Sie die Anweisungen, um sicherzustellen, dass die Integrität der ursprünglichen Konfiguration gewahrt bleibt.
9. Nun können Sie die Remotezugriffs-Verwaltungskonsole wieder öffnen.

# Planen einer Clusterbereitstellung mit Remotezugriff

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess-und RAS-VPN (RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle. Diese Übersicht bietet eine Einführung in die Planungsschritte, die erforderlich sind, um einen Cluster mit Windows Server 2016-oder Windows Server 2012-Remote Zugriffs Servern bereitzustellen.

- [Planen einer erweiterten DirectAccess-Bereitstellung](#). Dieser Schritt umfasst die Planung der Infrastruktur, die für die Bereitstellung eines einzelnen Servers erforderlich ist. Dazu gehört die Planung von Netzwerk- und Servereinstellungen, Zertifikat Anforderungen, DNS-Einstellungen, Bereitstellung des Netzwerkadressen Servers, DirectAccess-Verwaltungs Servern, Active Directory Einstellungen und Gruppenrichtlinie Objekte (GPOs).
- [Schritt 2: Planen von Cluster Servern](#) .
- [Schritt 3: Planen einer Cluster Bereitstellung mit LastenAusgleich](#).
- Schritt 4: Notieren Sie Ihre Planungsentscheidungen für die erweiterte Remote Zugriffs Bereitstellung. Dieser Datensatz kann als Arbeitshilfe für die Personen verwendet werden, die in den Abschluss der Bereitstellungsschritte involviert sind.

Nachdem Sie diese Planungsschritte abgeschlossen haben, finden Sie weitere Informationen unter [Konfigurieren eines Remote Zugriffs Clusters](#).

Anweisungen zum Konfigurieren einer Cluster Bereitstellung als Proof of Concept in einer Lab-Umgebung finden Sie unter [Test Umgebungs Anleitung: veranschaulichen von DirectAccess in einem Cluster mit Windows-NLB](#).

# Schritt 1 Planen einer erweiterten Einzel Server Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt bei der Planung eines Remote Zugriffs mit der Bereitstellung eines einmaligen Kennworts (OTP)-Client Authentifizierung ist das Planen und Konfigurieren einer erweiterten Einzel Server Bereitstellung.

## Planen einer Bereitstellung auf einem einzelnen Server

Stellen Sie vor dem Bereitstellen des Remote Zugriffs mit OTP sicher, dass Sie alle Schritte zum Bereitstellen eines einzelnen Remote Zugriffs Servers abgeschlossen haben. Weitere Informationen finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).

# Schritt 2 Planen von Cluster Servern

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Planen Sie nach der Bereitstellung eines einzelnen RAS-Servers zusätzliche Server zum Cluster hinzu.

AUFGABE	BESCHREIBUNG
<a href="#">2,1 Installieren von Rollen und Features.</a>	Planen Sie für jeden Server, der dem Cluster hinzugefügt werden soll, die Installation der Remote Zugriffs Rolle und des Windows-NLB-Features (falls erforderlich), planen Sie die Topologie, die IP-Addressierung, das Routing und die Weiterleitung.
<a href="#">2,2 Konfigurieren von Servereinstellungen</a>	Konfigurieren Sie die Einstellungen für jeden Server, der dem Cluster hinzugefügt wird. Beachten Sie, dass Sie einen Server Cluster mit Lastenausgleich mithilfe von virtuellen Computern konfigurieren können. Damit Routing und Konnektivität ordnungsgemäß funktionieren, müssen Sie die virtuellen Computer so konfigurieren, dass Sie das Spoofing von Mac-Adressen verwenden.

## 2,1 Installieren von Rollen und Features

Planen Sie die Installation der Remote Zugriffs Rolle für jeden Server, den Sie dem Cluster hinzufügen möchten.

Planen Sie zusätzlich die Installation des Netzwerk Lastenausgleichs (Network Load Balancing, NLB), wenn Sie einen Lastenausgleich für den Datenverkehr mithilfe von Windows NLB zum Cluster ausführen möchten. Weitere Informationen finden Sie unter [Netzwerk Lastenausgleich](#).

## 2,2 Konfigurieren von Servereinstellungen

Planen Sie die IP-Adresse und die Domänen Einstellungen für jeden Server, der dem Cluster hinzugefügt wird.

Beachten Sie Folgendes:

1. Die Server im Cluster müssen alle derselben Domäne angehören.
2. Die Server im Cluster müssen sich im selben Subnetz befinden.
3. Jeder Server im Cluster muss die gleiche Anzahl von Netzwerkadapters aufweisen, die für die DirectAccess-Bereitstellung verwendet werden.

Wenn Sie einen Lastenausgleich für den Cluster mithilfe von Windows NLB durchgeführt haben, werden die folgenden Windows NLB-Einstellungen angewendet:

1. Vorgangs Modus-Unicast. Dies kann mit dem NLB-Manager in Multicast geändert werden. Diese Einstellung kann in der Remote Zugriffs-Verwaltungskonsole nicht geändert werden.
2. Lastfaktor ist als gleichwertig definiert, wobei alle Cluster Server über eine gleichmäßige Auslastung verfügen.
3. Filter Modus: für den Datenverkehr wird ein Lastenausgleich über mehrere Hosts ausgeführt.
4. Affinität: einzelne Affinität ist definiert.

5. Protokolle: beides

# Schritt 3: Planen einer Cluster Bereitstellung mit Lastenausgleich

09.04.2020 • 15 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der nächste Schritt besteht darin, die Lasten Ausgleichs Konfiguration und die Cluster Bereitstellung zu planen.

AUFGABE	BESCHREIBUNG
3,1 Planen des Lasten Ausgleichs	Entscheiden Sie, ob Sie den Windows-Netzwerk Lastenausgleich (Network Load Balancing, NLB) oder einen externen Lastenausgleich (ELB) verwenden möchten.
3,2 planen IP-HTTPS	Wenn kein selbst signiertes Zertifikat verwendet wird, benötigt der RAS-Server ein SSL-Zertifikat auf jedem Server im Cluster, um IP-HTTPS-Verbindungen zu authentifizieren.
3,3 Planen von VPN-Clientverbindungen	Beachten Sie die Anforderungen für VPN-Clientverbindungen.
3,4 Planen des Netzwerkadressen Servers	Wenn die Netzwerkadressen Server-Website auf dem Remote Zugriffs Server gehostet wird und kein selbst signiertes Zertifikat verwendet wird, stellen Sie sicher, dass jeder Server im Cluster über ein Serverzertifikat verfügt, um die Verbindung mit der Website zu authentifizieren.

## 3,1 Planen des Lasten Ausgleichs

Der Remote Zugriff kann auf einem einzelnen Server oder auf einem Cluster von Remote Zugriffs Servern bereitgestellt werden. Für den Datenverkehr an den Cluster kann ein Lastenausgleich ausgeführt werden, um für DirectAccess-Clients Hochverfügbarkeit und Skalierbarkeit zu bieten. Es gibt zwei Optionen für den Lastenausgleich:

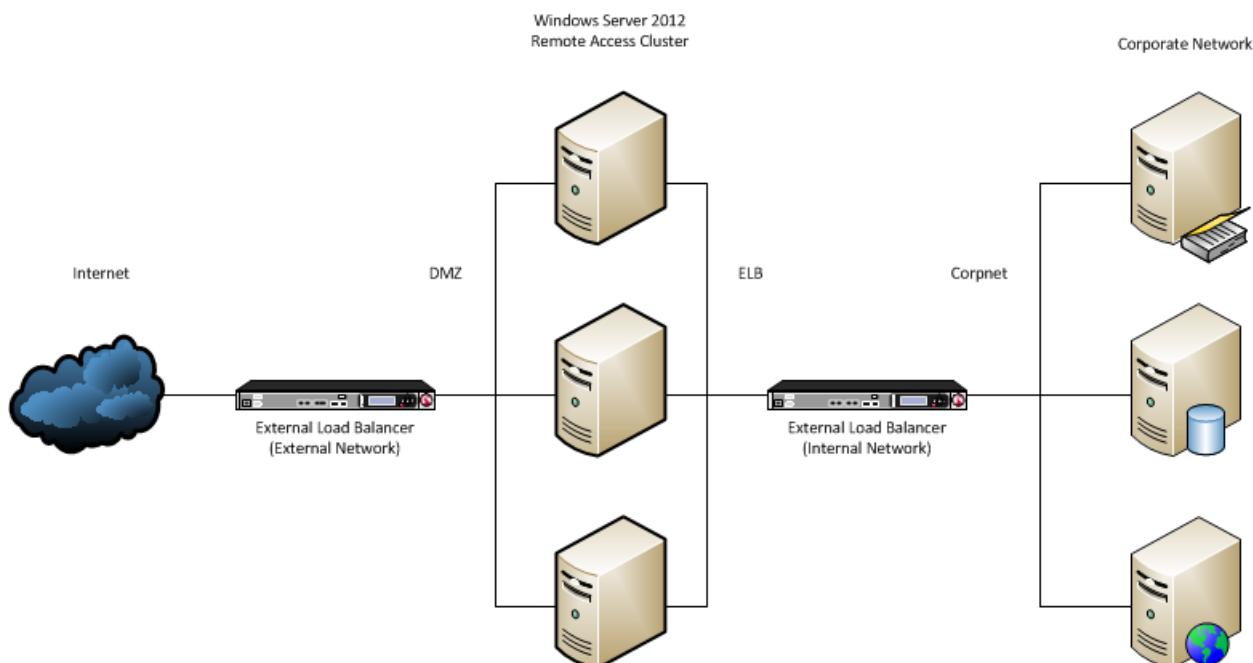
- **Windows NLB**-Windows NLB ist eine Windows Server-Funktion. Um es zu verwenden, benötigen Sie keine zusätzliche Hardware, da alle Server im Cluster für die Verwaltung der Datenverkehrs Auslastung verantwortlich sind. Windows-NLB unterstützt maximal acht Server in einem Remote Zugriffs Cluster.
- **Externer Lastenausgleich**: bei Verwendung eines externen Lasten Ausgleichs ist externe Hardware erforderlich, um die Auslastung des Datenverkehrs zwischen den Remote Zugriffs-Cluster Servern zu verwalten. Außerdem unterstützt die Verwendung eines externen Load Balancers maximal 32 RAS-Server in einem Cluster. Beim Konfigurieren des externen Lasten Ausgleichs sollten folgende Punkte berücksichtigt werden:
  - Der Administrator muss sicherstellen, dass die über den RAS-Assistenten für den Remote Zugriff konfigurierten virtuellen IP-Adressen auf dem externen Lasten Ausgleichs Modul (z. b. F5 BIG-IP local Traffic Manager System) verwendet werden. Wenn externer Lastenausgleich aktiviert ist, werden die IP-Adressen der externen und der internen Schnittstelle zu virtuellen IP-Adressen herauf gestuft und müssen auf den Lasten Ausgleichs Modulen gegeben werden. Dies geschieht, damit der Administrator den DNS-Eintrag für den öffentlichen Namen der Cluster Bereitstellung nicht ändern muss. Außerdem werden die IPSec-Tunnel Endpunkte von den Server-IPS abgeleitet. Wenn der

Administrator separate virtuelle IPS bereitstellt, kann der Client keine Verbindung mit dem Server herstellen. Ein Beispiel für die Konfiguration von DirectAccess mit externem Lastenausgleich finden Sie unter Beispiel für externe Load Balancer Konfiguration von 3.1.1.

- Viele externe Lasten Ausgleichs Module (einschließlich F5) unterstützen keinen Lastenausgleich von IPv6 zu 4 und ISATAP. Wenn es sich bei dem RAS-Server um einen ISATAP-Router handelt, sollte die ISATAP-Funktion auf einen anderen Computer verschoben werden. Wenn sich die ISATAP-Funktion auf einem anderen Computer befindet, müssen die DirectAccess-Server außerdem über eine systemeigene IPv6-Konnektivität mit dem ISATAP-Router verfügen. Beachten Sie, dass diese Konnektivität vorhanden sein sollte, bevor Sie DirectAccess konfigurieren.
- Wenn Teredo verwendet werden muss, müssen für den externen Lastenausgleich alle Remote Zugriffs Server über zwei aufeinander folgende öffentliche IPv4-Adressen als dedizierte IP-Adressen verfügen. Die virtuellen IP-Adressen des Clusters müssen auch über zwei aufeinander folgende öffentliche IPv4-Adressen verfügen. Dies gilt nicht für Windows NLB, bei dem nur die virtuellen IPS des Clusters über zwei aufeinander folgende öffentliche IPv4-Adressen verfügen müssen. Wenn Teredo nicht verwendet wird, sind zwei aufeinander folgende IP-Adressen nicht erforderlich.
- Der Administrator kann von der Windows-Netzwerk lastenverwaltung zum externen Load Balancer wechseln und umgekehrt. Beachten Sie, dass der Administrator nicht von einem externen Lasten Ausgleichs Modul zu Windows NLB wechseln kann, wenn er mehr als acht Server in der externen Load Balancer-Bereitstellung aufweist.

### 3.1.1 externe Load Balancer Konfigurationsbeispiel

In diesem Abschnitt werden die Konfigurationsschritte zum Aktivieren eines externen Load Balancers für eine neue Remote Zugriffs Bereitstellung beschrieben. Wenn Sie einen externen Load Balancer verwenden, könnte der Remote Zugriffs Cluster wie in der folgenden Abbildung aussehen, wobei die RAS-Server über einen Load Balancer im internen Netzwerk und das Internet über einen Load Balancer mit dem Unternehmensnetzwerk verbunden sind. Verbindung mit dem externen Netzwerk:



#### Informationen zur Planung

1. Externe VIPs (IPS, die der Client für die Verbindung mit dem Remote Zugriff verwendet) wurden als 131.107.0.102, 131.107.0.103
2. Load Balancer in externen Netzwerk-Self-IPS-131.107.0.245 (Internet), 131.107.1.245

Das Umkreis Netzwerk (auch als demilitarisierte Zone und DMZ bezeichnet) liegt zwischen dem Load Balancer im externen Netzwerk und dem RAS-Server.

3. IP-Adressen für den RAS-Server im Umkreis Netzwerk 131.107.1.102, 131.107.1.103
4. IP-Adressen für den RAS-Server im ELB-Netzwerk (d. h. zwischen dem RAS-Server und dem Load Balancer im internen Netzwerk)-30.11.1.101, 2006:2005:11:1::101
5. Load Balancer on Internal Network Self-IPS-30.11.1.245 2006:2005:11:1::245 (ELB), 30.1.1.245 2006:2005:1:1::245 (Corpnet)
6. Interne VIPs (IP-Adressen, die für den Clientweb Test verwendet werden, und für den Netzwerkadressen Server, wenn Sie auf den RAS-Servern installiert sind), werden als 30.1.1.10, 2006:2005:1:1::10

#### Schritte

1. Konfigurieren Sie den externen Netzwerkadapter des RAS-Servers, der mit dem Umkreis Netzwerk verbunden ist, mit den Adressen 131.107.0.102, 131.107.0.103. Dieser Schritt ist erforderlich, damit die DirectAccess-Konfiguration die richtigen IPSec-Tunnel Endpunkte erkennt.
2. Konfigurieren Sie den internen Netzwerkadapter des RAS-Servers (der mit dem ELB-Netzwerk verbunden ist) mit den IP-Adressen des Webtests/Netzwerkadressen Servers (30.1.1.10, 2006:2005:1:1::10). Dieser Schritt ist erforderlich, um Clients den Zugriff auf die Webtest-IP zu gestatten, sodass der netzwerkkonnektivitätsproxy den Verbindungsstatus für DirectAccess ordnungsgemäß angibt. Dieser Schritt ermöglicht auch den Zugriff auf den Netzwerkadressen Server, wenn er auf dem DirectAccess-Server konfiguriert ist.

#### NOTE

Stellen Sie sicher, dass der Domänen Controller vom RAS-Server aus mit dieser Konfiguration erreichbar ist.

3. Konfigurieren Sie den DirectAccess-Einzel Server auf dem Remote Zugriffs Server.
4. Aktivieren Sie den externen Lastenausgleich in der DirectAccess-Konfiguration. Verwenden Sie 131.107.1.102 als externe dedizierte IP-Adresse (DIP) (131.107.1.103 wird automatisch ausgewählt), verwenden Sie 30.11.1.101, 2006:2005:11:1::101 als interne Dips.
5. Konfigurieren Sie die externen virtuellen IPS (VIP) auf dem externen Lasten Ausgleichs Modul mit den Adressen 131.107.0.102 und 131.107.0.103. Konfigurieren Sie außerdem die internen VIPs auf dem externen Load Balancer mit den Adressen 30.1.1.10 und 2006:2005:1:1::10.
6. Der Remote Zugriffs Server wird nun mit den geplanten IP-Adressen konfiguriert, und die externen und internen IP-Adressen für den Cluster werden gemäß den geplanten IP-Adressen konfiguriert.

## 3,2 planen IP-HTTPS

1. **Zertifikat Anforderungen:** während der Bereitstellung des einzelnen RAS-Servers haben Sie die Verwendung eines IP-HTTPS-Zertifikats ausgewählt, das von einer öffentlichen oder internen Zertifizierungsstelle (Certification Authority, ca) ausgestellt wurde, oder ein selbst signiertes Zertifikat. Für die Cluster Bereitstellung müssen Sie für jedes Mitglied des Remote Zugriffs Clusters denselben Zertifikattyp verwenden. Wenn Sie also ein von einer öffentlichen Zertifizierungsstelle ausgestelltes Zertifikat verwendet haben (empfohlen), müssen Sie ein von einer öffentlichen Zertifizierungsstelle ausgestelltes Zertifikat auf jedem Mitglied des Clusters installieren. Der Antragsteller Name des neuen Zertifikats muss mit dem Antragsteller Namen des IP-HTTPS-Zertifikats identisch sein, das zurzeit in der Bereitstellung verwendet wird. Beachten Sie Folgendes: Wenn Sie selbst signierte Zertifikate verwenden, werden diese bei der Cluster Bereitstellung automatisch auf jedem Server konfiguriert.
2. **Präfix Anforderungen:** der Remote Zugriff ermöglicht den Lastenausgleich für SSL-basierten Datenverkehr und DirectAccess-Datenverkehr. Für den Lastenausgleich für den gesamten IPv6-basierten DirectAccess-Datenverkehr muss der Remote Zugriff das IPv4-Tunnelingverfahren für alle Übergangs

Technologien untersuchen. Da der IP-HTTPS-Datenverkehr verschlüsselt ist, ist die Untersuchung des Inhalts des IPv4-Tunnels nicht möglich. Um den IP-HTTPS-Datenverkehr für den Lastenausgleich zu aktivieren, müssen Sie ein breit genug IPv6-Präfix zuordnen, damit jedem Cluster Mitglied ein anderes IPv6/64-Präfix zugewiesen werden kann. Sie können maximal 32 Server in einem Cluster mit Lastenausgleich konfigurieren. Daher müssen Sie ein Präfix/59 angeben. Dieses Präfix muss an die interne IPv6-Adresse des Remote Zugriffs Clusters Routing fähig sein und ist im Setup-Assistenten für den Remote Zugriffs Server konfiguriert.

#### NOTE

Die Präfix Anforderungen sind nur in einem IPv6-fähigen internen Netzwerk (nur IPv6 oder IPv4 + IPv6) relevant. In einem reinen IPv4-Unternehmensnetzwerk wird das Client Präfix automatisch konfiguriert und kann vom Administrator nicht geändert werden.

## 3,3 Planen von VPN-Clientverbindungen

Es gibt eine Reihe von Überlegungen zu VPN-Clientverbindungen:

- Der Lastenausgleich für den VPN-Client Verkehr ist nicht möglich, wenn VPN-Client Adressen mithilfe von DHCP zugeordnet werden Ein statischer Addresspool ist erforderlich.
- RRAS kann auf einem Cluster mit Lastenausgleich aktiviert werden, der nur für DirectAccess bereitgestellt wurde, indem **VPN** auf der Taskbereich der Remote Zugriffs-Verwaltungskonsole aktiviert ist.
- Alle VPN-Änderungen, die in der Routing-und RAS-Verwaltungskonsole (rrasmgmt.msc) abgeschlossen wurden, müssen manuell auf allen RAS-Servern im Cluster repliziert werden.
- Um den Lastenausgleich für den VPN-IPv6-Client Datenverkehr zu ermöglichen, müssen Sie ein IPv6-Präfix von 59 Bit angeben.

## 3,4 Planen des Netzwerkadressen Servers

Wenn Sie die Netzwerkadressen Server-Website auf dem einzelnen RAS-Server ausführen, haben Sie während der Bereitstellung die Verwendung eines von einer internen Zertifizierungsstelle (Certification Authority, ca) ausgestellten Zertifikats oder eines selbst signierten Zertifikats ausgewählt. Beachten Sie Folgendes:

1. Jedes Mitglied des Remote Zugriffs Clusters muss über ein Zertifikat für den Netzwerkadressen Server verfügen, das dem DNS-Eintrag für die Netzwerkadressen Server-Website entspricht.
2. Das Zertifikat für die einzelnen Cluster Server muss auf die gleiche Weise ausgestellt werden wie das Zertifikat auf dem aktuellen Netzwerkadressen Serverzertifikat des Remote Zugriffs Servers. Wenn Sie z. b. ein von einer internen Zertifizierungsstelle ausgestelltes Zertifikat verwendet haben, müssen Sie für jedes Mitglied des Clusters ein von der internen Zertifizierungsstelle ausgestelltes Zertifikat installieren.
3. Wenn Sie ein selbst signiertes Zertifikat verwendet haben, wird bei der Cluster Bereitstellung automatisch ein selbst signiertes Zertifikat für jeden Server konfiguriert.
4. Der Antragsteller Name des Zertifikats darf nicht mit dem Namen eines beliebigen Servers in der Remote Zugriffs Bereitstellung identisch sein.

# Konfigurieren eines Clusters mit Remotezugriff

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren Always on VPN-und RRAS-VPN (Routing and Remote Access Service) in einer einzigen Remote Zugriffs Rolle. Diese Übersicht bietet eine Einführung in die Konfigurationsschritte, die erforderlich sind, um einen einzelnen Remote Zugriffs Server unter Windows Server 2016 oder Windows Server 2012 in einem Cluster mit Lastenausgleich bereitzustellen.

- Schritt 1: bereitstellen [eines Always on-VPN-Servers mit erweiterten Optionen](#).
- [Schritt 2: Vorbereiten von Cluster Servern](#).
- [Schritt 3: Konfigurieren eines Clusters mit Lastenausgleich](#).
- [Schritt 4: Überprüfen Sie den Cluster](#).

# Schritt 1 Implementieren einer einzelnen Server Bereitstellung für den Remote Zugriff

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Konfigurationsschritt zum Bereitstellen des Remote Zugriffs in einer Topologie mit mehreren Standorten ist die Implementierung einer erweiterten Bereitstellung mit einem einzelnen Server und das Hinzufügen von Servern zu jedem Multisite-Einstiegspunkt.

## Implementieren einer Bereitstellung auf einem einzelnen Server

Bevor Sie eine Bereitstellung für mehrere Standorte konfigurieren können, müssen Sie wie unter Bereitstellen eines [einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) beschrieben eine erweiterte Bereitstellung für den Remote Zugriff mit einem Server konfigurieren.

## Siehe auch

- [Schritt 2: Konfigurieren der Infrastruktur für mehrere Standorte](#)

# Schritt 2 Vorbereiten von Cluster Servern

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Bevor Sie eine Cluster Bereitstellung konfigurieren können, bereiten Sie zusätzliche Server vor, die dem Cluster hinzugefügt werden sollen.

AUFGABE	BESCHREIBUNG
<a href="#">2,1 Konfigurieren der Remote Zugriffs Infrastruktur</a>	Konfigurieren Sie auf jedem Server, den Sie dem Cluster hinzufügen möchten, die Server Topologie, die IP-Adressierung, das Routing und die Weiterleitung. Wenn Sie einen Cluster mit Lastenausgleich für virtuelle Computer konfigurieren, müssen Sie die virtuellen Computer so konfigurieren, dass Sie das Spoofing von Mac-Adressen verwenden. Fügen Sie außerdem jeden Server derselben Domäne hinzu, und verbinden Sie alle Server mit dem gleichen Subnetz.
<a href="#">2,2 Installieren der Remote Zugriffs Rolle</a>	Installieren Sie auf jedem zusätzlichen Server, den Sie dem Cluster hinzufügen möchten, die Remote Zugriffs Rolle.
<a href="#">2,3 Installieren von NLB</a>	Installieren Sie auf dem bereitgestellten Remote Zugriffs Server und auf jedem zusätzlichen Server, den Sie dem Cluster hinzufügen möchten, das NLB-Feature. Beachten Sie, dass dieser Schritt bei der Verwendung eines externen Load Balancer nicht erforderlich ist.

## 2,1 Konfigurieren der Remote Zugriffs Infrastruktur

Zum Konfigurieren eines Remote Zugriffs Clusters müssen Sie die Server Topologie, die IP-Adressierung, das Routing und die Weiterleitung auf jedem Server konfigurieren, der Teil des Clusters sein wird.

### So konfigurieren Sie die Remote Zugriffs Infrastruktur

1. Konfigurieren Sie jeden der Server, die sich im Cluster befinden, mit derselben Topologie wie der erste RAS-Server.
2. Konfigurieren Sie jeden Server, der sich im Cluster befinden soll, mit entsprechender IP-Adressierung, Routing und Weiterleitung basierend auf der Konfiguration des ersten RAS-Servers. Beachten Sie, dass alle Server im Cluster mit demselben Subnetz verbunden sein müssen.
3. Verknüpfen Sie jeden Server, der sich im Cluster befinden soll, mit derselben Domäne wie der erste RAS-Server.

## 2,2 Installieren der Remote Zugriffs Rolle

Zum Konfigurieren eines Remote Zugriffs Clusters müssen Sie die Remote Zugriffs Rolle auf allen Servern installieren, die einen Teil des Clusters bilden.

### So installieren Sie die Remote Zugriffs Rolle auf Always on VPN-Servern

1. Klicken Sie auf dem DirectAccess-Server in der Server-Manager-Konsole im **Dashboard** auf **Rollen und Features hinzufügen**.
2. Klicken Sie dreimal auf **Weiter**, um zur Anzeige für die Serverrollenauswahl zu gelangen.
3. Wählen Sie im Dialogfeld **Server Rollen auswählen** die Option **Remote Zugriff** aus, und klicken Sie dann auf **weiter**.
4. Klicken Sie drei Mal auf **weiter**.
5. Wählen Sie im Dialogfeld **Rollen Dienste auswählen** die Option **DirectAccess und VPN (RAS)** aus, und klicken Sie dann auf **Features hinzufügen**.
6. Wählen Sie **Routing, webanwendungsproxy** aus, klicken Sie auf **Features hinzufügen** und dann auf **weiter**.
7. Klicken Sie auf **Weiter** und dann auf **Installieren**.
8. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.
9. Wiederholen Sie diesen Vorgang auf allen Servern, für die Sie Cluster Mitglieder sein möchten.

## 2,3 Installieren von NLB

Wenn Sie einen Remote Zugriffs Cluster konfigurieren möchten, müssen Sie die Funktion für den Netzwerk Lastenausgleich auf jedem Server installieren, der einen Teil des Clusters bilden soll.

### NOTE

Dieser Schritt ist nicht erforderlich, wenn ein externer Load Balancer verwendet wird.

### So installieren Sie die NLB-Rolle

1. Klicken Sie auf dem DirectAccess-Server in der Server-Manager-Konsole im **Dashboard** auf **Rollen und Features hinzufügen**.
2. Klicken Sie viermal auf **weiter**, um zum Bildschirm für die Server Funktionsauswahl zu gelangen.
3. Klicken Sie im Dialogfeld **Features auswählen** auf **Netzwerk Lastenausgleich**, klicken Sie auf **Features hinzufügen**, klicken Sie auf **weiter**, und klicken Sie dann auf **Installieren**.
4. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.
5. Wiederholen Sie diesen Vorgang auf allen Servern, für die Sie Cluster Mitglieder sein möchten.

## Siehe auch

- [Schritt 3: Konfigurieren eines Clusters mit Lastenausgleich](#)

# Schritt 3: Konfigurieren eines Clusters mit Lastenausgleich

09.04.2020 • 29 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nachdem Sie die Server für den Cluster vorbereitet haben, konfigurieren Sie den Lastenausgleich auf dem einzelnen Server, konfigurieren Sie die erforderlichen Zertifikate, und stellen Sie den Cluster bereit.

AUFGABE	BESCHREIBUNG
<a href="#">3,1 Konfigurieren des IPv6-Präfixes</a>	Wenn die Unternehmensumgebung IPv4 + IPv6 oder nur IPv6 ist, stellen Sie auf dem einzelnen RAS-Server sicher, dass das IPv6-Präfix, das DirectAccess-Client Computern zugewiesen ist, groß genug ist, um alle Server im Cluster abzudecken.
<a href="#">3,2 Aktivieren des Lasten Ausgleichs</a>	Aktivieren Sie den Lastenausgleich auf dem einzelnen Remote Zugriffs Server.
<a href="#">3,3 Installieren des IP-HTTPS-Zertifikats</a>	Jeder Server im Cluster erfordert ein Serverzertifikat zur Authentifizierung der IP-HTTPS-Verbindung. Exportieren Sie das IP-HTTPS-Zertifikat vom einzelnen RAS-Server, und stellen Sie es auf jedem Server bereit, den Sie dem Cluster hinzufügen. Dies ist nur erforderlich, wenn nicht selbst signierte Zertifikate verwendet werden.
<a href="#">3,4 Installieren des Netzwerkadressen Server-Zertifikats</a>	Wenn der Netzwerkadressen Server auf dem einzelnen Server lokal bereitgestellt wird, müssen Sie das Netzwerkadressen Server-Zertifikat auf jedem Server im Cluster bereitstellen. Wenn der Netzwerkadressen Server auf einem externen Server gehostet wird, ist ein Zertifikat auf jedem Server nicht erforderlich. Dies ist nur erforderlich, wenn nicht selbst signierte Zertifikate verwendet werden.
<a href="#">3,5 Hinzufügen von Servern zum Cluster</a>	Fügen Sie alle Server zum Cluster hinzu. Der Remote Zugriff darf auf den Servern, die hinzugefügt werden sollen, nicht konfiguriert werden.
<a href="#">3,6 Entfernen eines Servers aus dem Cluster</a>	Anweisungen zum Entfernen eines Servers aus dem Cluster.
<a href="#">3,7 Deaktivieren des Lasten Ausgleichs</a>	Anweisungen zum Deaktivieren des Lasten Ausgleichs.

## NOTE

Die für die DIP-Adresse ausgewählte IP-Adresse darf nicht auf den Netzwerkadapters des ersten Remote Zugriffs Servers im Cluster verwendet werden. Das Starten der DirectAccess-Bereitstellung mit VIP und DIP, die dem Netzwerkadapter hinzugefügt werden, führt zu einem Fehler.

#### **NOTE**

Stellen Sie sicher, dass Sie keine DIP verwenden, die bereits auf einem anderen Computer im Netzwerk vorhanden ist.

## 3,1 Konfigurieren des IPv6-Präfixes

### **So konfigurieren Sie das Präfix**

1. Klicken Sie auf dem Remote Zugriffs Server auf **Start**, und klicken Sie dann auf **Remote Zugriffs Verwaltung**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remotezugriffs-Verwaltungskonsole auf **Konfiguration**.
3. Klicken Sie im mittleren Bereich der Konsole im Bereich **Schritt 2 DirectAccess-Server** auf **Bearbeiten**.
4. Klicken Sie auf **Präfix Konfiguration**. Geben Sie auf der Seite **Präfix Konfiguration unter IPv6-Präfix, das DirectAccess-Client Computern zugewiesen ist** das IPv6-Präfix ein, das für DirectAccess-Client Computer mit der Subnetzlänge 59 verwendet wird, z. B. **2001: db8:1: 1000::/59**. Wenn VPN auch mit IPv6 aktiviert wurde, wird ein IPv6-Präfix angezeigt, und die Subnetzlänge muss in 59 geändert werden. Klicken Sie auf **Weiter**.
5. Klicken Sie im mittleren Bereich der Konsole auf **Fertigstellen**.
6. Überprüfen Sie im Dialogfeld **Remote Zugriffs Überprüfung** die Konfigurationseinstellungen, und klicken Sie **dann auf übernehmen**. Klicken Sie im Dialogfeld **Anwenden der Einstellungen zum Einrichten des Remotezugriffs** auf **Schließen**.

## 3,2 Aktivieren des Lasten Ausgleichs

### **So aktivieren Sie den Lastenausgleich**

1. Klicken Sie auf dem konfigurierten DirectAccess-Server auf **Start**, und klicken Sie dann auf **Remote Zugriffs Verwaltung**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remote Zugriffs-Verwaltungskonsole im linken Bereich auf **Konfiguration**, und klicken Sie dann im Bereich **Tasks** auf **Lastenausgleich aktivieren**.
3. Klicken Sie im Assistenten zum Aktivieren des Lasten Ausgleichs auf **weiter**.
4. Je nachdem, was Sie in den Planungsschritten gewählt haben:
  - a. Windows-NLB: Klicken Sie auf der Seite **Lasten Ausgleichs Methode** auf **Windows-Netzwerk Lastenausgleich (NLB) verwenden**, und klicken Sie dann auf **weiter**.
  - b. Externer Load Balancer: Klicken Sie auf der Seite **Lasten Ausgleichs Methode** auf **externen Load Balancer verwenden**, und klicken Sie dann auf **weiter**.
5. Führen Sie in einer einzelnen Netzwerkadapter Bereitstellung auf der Seite **dedizierte IP-Adressen** die folgenden Schritte aus, und klicken Sie dann auf **weiter**:
  - a. Geben Sie im Feld **IPv4-Adresse** die neue IPv4-Adresse für diesen RAS-Server ein. bei der aktuellen IPv4-Adresse handelt es sich um die virtuelle IP-Adresse (VIP) des Clusters mit Lastenausgleich. Geben Sie im Feld **Subnetzmaske** die Subnetzmaske ein.
  - b. Wenn es sich bei der Unternehmensumgebung um native IPv6 handelt, geben Sie im Feld **IPv6-Adresse** die neue IPv6-Adresse für diesen RAS-Server ein. bei der aktuellen IPv6-Adresse handelt es sich um die VIP des Clusters mit Lastenausgleich. Geben Sie im Feld **Subnetzpräfix-Länge** die

Länge des Subnetzpräfixes ein.

6. Führen Sie in einer Bereitstellung mit zwei Netzwerkadapters auf der Seite **externe dedizierte IP-Adressen** die folgenden Schritte aus, und klicken Sie dann auf **weiter**:
  - a. Geben Sie im Feld **IPv4-Adresse** die neue externe IPv4-Adresse für diesen RAS-Server ein. bei der aktuellen IPv4-Adresse handelt es sich um die virtuelle IP-Adresse (VIP) des Lasten Ausgleichs Clusters. Geben Sie im Feld **Subnetzmaske** die Subnetzmaske ein.
  - b. Wenn derzeit systemeigene IPv6-Adressen auf dem Netzwerkadapter des Remote Zugriffs Servers mit Internet Zugriff konfiguriert sind, geben Sie im Feld **IPv6-Adresse** die neue externe IPv6-Adresse für diesen RAS-Server ein. bei der aktuellen IPv6-Adresse handelt es sich um die VIP des Lasten Ausgleichs Clusters. Geben Sie im Feld **Subnetzprefix-Länge** die Länge des Subnetzpräfixes ein.
7. Führen Sie in einer Bereitstellung mit zwei Netzwerkadapters auf der Seite **interne dedizierte IP-Adressen** die folgenden Schritte aus, und klicken Sie dann auf **weiter**:
  - a. Geben Sie im Feld **IPv4-Adresse** die neue interne IPv4-Adresse für diesen RAS-Server ein. bei der aktuellen IPv4-Adresse handelt es sich um die VIP des Lasten Ausgleichs Clusters. Geben Sie im Feld **Subnetzmaske** die Subnetzmaske ein.
  - b. Wenn es sich bei der Unternehmensumgebung um native IPv6 handelt, geben Sie im Feld **IPv6-Adresse** die neue interne IPv6-Adresse für diesen RAS-Server ein. bei der aktuellen IPv6-Adresse handelt es sich um die VIP des Lasten Ausgleichs Clusters. Geben Sie im Feld **Subnetzprefix-Länge** die Länge des Subnetzpräfixes ein.
8. Klicken Sie auf der Seite **Zusammenfassung** auf **Commit**.
9. Klicken Sie im Dialogfeld **Lastenausgleich aktivieren** auf **Schließen**.
10. Klicken Sie im Assistenten zum Aktivieren des Lasten Ausgleichs auf **Schließen**.

**NOTE**

Wenn externer Lastenausgleich verwendet wird, notieren Sie sich die virtuellen IPS, und stellen Sie Sie als auf den externen Lasten Ausgleichs Modulen bereit.

### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

Wenn Sie sich für die Verwendung von Windows NLB in den Planungsschritten entschieden haben, führen Sie Folgendes aus:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress "2.1.1.20/255.255.255.0" -InternalDedicatedIPAddress
@("10.1.1.30/255.255.255.0","3ffe::20/64") -InternetVirtualIPAddress
@("2.1.1.1/255.255.255.0","2.1.1.2/255.255.255.0") -InternalVirtualIPAddress
@("10.1.1.2/255.255.255.0","3ffe::2/64")
```

Wenn Sie sich für die Verwendung eines externen Load Balancers in den Planungsschritten entschieden haben, führen Sie Folgendes aus:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress "2.1.1.20/255.255.255.0" -InternalDedicatedIPAddress @("10.1.1.30/255.255.255.0","3ffe::20/64") -UseThirdPrtyLoadBalancer
```

#### NOTE

Es wird empfohlen, keine Änderungen an den Einstellungen des Load Balancers mit Änderungen an anderen Einstellungen einzuschließen, wenn Sie staginggruppen Richtlinien Objekte verwenden. Alle Änderungen an den Einstellungen des Load Balancers müssen zuerst angewendet werden, und dann sollten andere Konfigurationsänderungen vorgenommen werden. Nachdem Sie den Lastenausgleich auf einem neuen DirectAccess-Server konfiguriert haben, sollten Sie außerdem einige Zeit für die Anwendung von IP-Änderungen auf die DNS-Server im Unternehmen zulassen, bevor Sie andere DirectAccess-Einstellungen ändern, die sich auf den neuen Cluster beziehen.

## 3,3 Installieren des IP-HTTPS-Zertifikats

Zum Ausführen dieses Verfahrens ist mindestens die Mitgliedschaft in der lokalen Gruppe **Administratoren** oder eine gleichwertige Berechtigung erforderlich.

### So installieren Sie das IP-HTTPS-Zertifikat

1. Klicken Sie auf dem konfigurierten RAS-Server auf **Start**, geben Sie **MMC** ein, und drücken Sie **EINGABETASTE**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** auf **Zertifikate**, klicken Sie auf **Hinzufügen**, klicken Sie auf **Computer Konto**, klicken Sie auf **weiter**, klicken Sie auf **Fertigstellen** und dann auf **OK**.
4. Navigieren Sie im linken Bereich der Konsole zu **Zertifikate (lokaler Computer) \personal\zertifikate**. Klicken Sie mit der rechten Maustaste auf das IP-HTTPS-Zertifikat, zeigen Sie auf **Alle Tasks**, und klicken Sie auf
5. Klicken Sie auf der Seite **Zertifikatexport-Assistent – Willkommen** auf **Weiter**.
6. Klicken Sie auf der Seite **Privaten Schlüssel exportieren** auf **Ja, privaten Schlüssel exportieren**, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf der Seite **Format der exportierbare Datei** auf **privater Informationsaustausch-PKCS-#12 (.PFX)**, und klicken Sie dann auf **weiter**.
8. Aktivieren Sie auf der Seite **Sicherheit** das Kontrollkästchen **Kennwort**, geben Sie ein Kennwort in das Feld **Kennwort** ein, und bestätigen Sie das Kennwort, und klicken Sie dann auf **weiter**.
9. Geben Sie auf der Seite **zu exportierendes Datei** einen Namen für die Zertifikat Datei ein, und speichern Sie Sie auf dem Desktop, und klicken Sie dann auf **weiter**.
10. Klicken Sie auf der Seite **Fertigstellen des Assistenten** auf **Fertig stellen**.
11. Klicken Sie im Dialogfeld **Zertifikat Export-Assistent** auf **OK**.
12. Kopieren Sie das Zertifikat auf alle Server, die Sie als Cluster Mitglieder gruppieren möchten.
13. Klicken Sie auf dem neuen DirectAccess-Server auf **Start**, geben Sie **MMC** ein, und drücken Sie **EINGABETASTE**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
14. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.

15. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen auf Zertifikate**, klicken Sie auf **Hinzufügen**, klicken Sie auf **Computer Konto**, klicken Sie auf **weiter**, klicken Sie auf **Fertigstellen** und dann auf **OK**.
16. Navigieren Sie im linken Bereich der Konsole zu **Zertifikate (lokaler Computer) \personal\zertifikate**. Klicken Sie mit der rechten Maustaste auf den Knoten **Zertifikate**, zeigen Sie auf **Alle Tasks**, und klicken Sie auf **importieren**.
17. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
18. Klicken Sie auf der Seite **zu importierende Datei** auf **Durchsuchen**, um das Zertifikat zu suchen. Wählen Sie das Zertifikat aus, und klicken Sie auf **weiter**.
19. Geben Sie auf der Seite Schutz für den **privaten Schlüssel** im Feld **Kennwort** das Kennwort ein, und klicken Sie dann auf **weiter**.
20. Klicken Sie auf der Seite **Zertifikatspeicher** auf **Weiter**.
21. Klicken Sie auf der Seite **Abschließen des Zertifikatimport-Assistenten** auf **Fertig stellen**.
22. Klicken Sie im Dialogfeld **Zertifikat Import-Assistent** auf **OK**.
23. Wiederholen Sie die Schritte 13-22 auf allen Servern, bei denen es sich um Cluster Mitglieder handeln soll.

### 3,4 Installieren des Netzwerkadressen Server-Zertifikats

Zum Ausführen dieses Verfahrens ist mindestens die Mitgliedschaft in der lokalen Gruppe **Administratoren** oder eine gleichwertige Berechtigung erforderlich.

#### **So installieren Sie ein Zertifikat für den Netzwerk Speicherort**

1. Klicken Sie auf dem Remote Zugriffs Server auf **Start**, geben Sie **MMC** ein, und drücken Sie dann die **EINGABETASTE**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie im Menü **Datei** auf **Snap-Ins hinzufügen bzw. entfernen**.
3. Klicken Sie auf **Zertifikate, Hinzufügen, Computer Konto, weiter**, klicken Sie auf **lokaler Computer**, klicken Sie auf **Fertigstellen**, und klicken Sie dann auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
6. Klicken Sie zweimal auf **Weiter**.
7. Klicken Sie auf der Seite **Zertifikate anfordern** auf die Vorlage **Webserver Zertifikat**, und klicken Sie dann auf **Weitere Informationen sind erforderlich, um sich für dieses Zertifikat zu registrieren**.

Wenn die Vorlage für das Webserver Zertifikat nicht angezeigt wird, stellen Sie sicher, dass das Remote Zugriffs Server-Computer Konto über die Berechtigung "registrieren" für die Webserver-Zertifikat Vorlage verfügt. Weitere Informationen finden Sie unter [Konfigurieren von Berechtigungen für die Webserver-Zertifikat Vorlage](#).

8. Wählen Sie im Dialogfeld **Zertifikat Eigenschaften auf der Register Karte Antragsteller** unter **Antragsteller Name für Typ** die Option **allgemeiner Name** aus.
9. Geben Sie unter **Wert** den voll qualifizierten Domänen Namen (FQDN) für den Intranetnamen der Netzwerkadressen Server-Website ein (z. b. `nls.Corp.contoso.com`), und klicken Sie dann auf **Hinzufügen**.

10. Klicken Sie auf **OK**, **Registrieren** und dann auf **Fertig stellen**.
11. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, dass ein neues Zertifikat mit dem vollqualifizierten Domänennamen unter **Serverauthentifizierung** mit der Option **Beabsichtigte Zwecke** registriert wurde.
12. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und klicken Sie anschließend auf **Eigenschaften**.
13. Geben Sie unter **Anzeigenamen** den Namen **Netzwerkadressenzertifikat** ein, und klicken Sie dann auf **OK**.

**TIP**

Die Schritte 12 und 13 sind optional, erleichtern es Ihnen jedoch, das Zertifikat für den Netzwerk Speicherort beim Konfigurieren des Remote Zugriffs auszuwählen.

14. Wiederholen Sie diesen Vorgang auf allen Servern, für die Sie Cluster Mitglieder sein möchten.

### 3,5 Hinzufügen von Servern zum Cluster

#### So fügen Sie dem Cluster Server hinzu

1. Klicken Sie auf dem konfigurierten DirectAccess-Server auf **Start**, und klicken Sie dann auf **Remote Zugriffs Verwaltung**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remotezugriffs-Verwaltungskonsole auf **Konfiguration**. Klicken Sie im Bereich **Tasks** unter **Cluster mit Lastenausgleich** auf **Server hinzufügen oder entfernen**.
3. Klicken Sie im Dialogfeld **Server hinzufügen oder entfernen** auf **Server hinzufügen**.
4. Geben Sie im Dialogfeld **Server hinzufügen** auf der Seite **Server auswählen** den Namen des zusätzlichen Remote Zugriffs Servers ein, und klicken Sie dann auf **weiter**.
5. Führen Sie auf der Seite **Netzwerkadapter** einen der folgenden Schritte aus:
  - Wenn Sie eine Topologie mit zwei Netzwerkadapters bereitstellen, wählen Sie in **externer Adapter** den Adapter aus, der mit dem externen Netzwerk verbunden ist. Wählen Sie unter **interner Adapter** den Adapter aus, der mit dem internen Netzwerk verbunden ist.
  - Wenn Sie eine Topologie mit einem Netzwerkadapter bereitstellen, wählen Sie unter **Netzwerkadapter** den Adapter aus, der mit dem internen Netzwerk verbunden ist.
6. Klicken Sie auf der Seite **Netzwerkadapter** unter **Wählen Sie das zum Authentifizieren von IP-HTTPS-Verbindungen verwendete Zertifikat auf Durchsuchen**, um das IP-HTTPS-Zertifikat zu suchen und auszuwählen, und klicken Sie dann auf **weiter**.
7. Klicken Sie auf der Seite **Netzwerkadressen Server** auf **Durchsuchen**, um das Zertifikat für die Netzwerkadressen Server-Website auszuwählen, die auf dem Remote Zugriffs Server ausgeführt wird, und klicken Sie dann auf **weiter**.

**NOTE**

Die Seite **Netzwerkadressen Server** wird nur angezeigt, wenn die Netzwerkadressen Server-Website auf dem Remote Zugriffs Server ausgeführt wird.

#### **NOTE**

Wenn auch VPN auf dem RAS-Server konfiguriert wurde, werden Sie aufgefordert, an dieser Stelle die Informationen zum VPN-IP-Adresspool hinzuzufügen.

8. Klicken Sie auf der Seite **Zusammenfassung** auf **Hinzufügen**.
9. Klicken Sie auf der Seite **Abschluss des Vorgangs** auf **Schließen**.
10. Wiederholen Sie diesen Vorgang für alle Remote Zugriffs Server, die dem Cluster hinzugefügt werden sollen.
11. Klicken Sie im Dialogfeld **Server hinzufügen oder entfernen** auf **Commit**.
12. Klicken Sie im Dialogfeld zum **Hinzufügen und Entfernen von Servern** auf **Schließen**.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Add-RemoteAccessLoadBalancerNode -RemoteAccessServer <server name>
```

#### **NOTE**

Wenn VPN nicht in einem Cluster mit Lastenausgleich aktiviert wurde, sollten Sie keine VPN-Adressbereiche angeben, wenn Sie dem Cluster mithilfe von Windows PowerShell-Cmdlets einen neuen Server hinzufügen. Wenn dies versehentlich erfolgt ist, entfernen Sie den Server aus dem Cluster, und fügen Sie ihn erneut dem Cluster hinzu, ohne die VPN-Adressbereiche anzugeben.

## 3,6 Entfernen eines Servers aus dem Cluster

### **So entfernen Sie einen Server aus dem Cluster**

1. Klicken Sie auf dem konfigurierten Remote Zugriffs Server auf **Start**, und klicken Sie dann auf **Remote Zugriffs Verwaltung**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remotezugriffs-Verwaltungskonsole auf **Konfiguration**. Klicken Sie im Bereich **Tasks** unter **Cluster mit LastenAusgleich** auf **Server hinzufügen oder entfernen**.
3. Wählen Sie im Dialogfeld **Server hinzufügen oder entfernen** den Remote Zugriffs Server aus, den Sie entfernen möchten, und klicken Sie dann auf **Server entfernen**.
4. Stellen Sie im Dialogfeld **Server Warnung entfernen** sicher, dass Sie den richtigen Server ausgewählt haben, und klicken Sie dann auf **OK**.
5. Wiederholen Sie diesen Vorgang für alle Remote Zugriffs Server, die aus dem Cluster entfernt werden sollen.
6. Klicken Sie im Dialogfeld **Server hinzufügen oder entfernen** auf **Commit**.
7. Klicken Sie im Dialogfeld zum **Hinzufügen und Entfernen von Servern** auf **Schließen**.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Remove-RemoteAccessLoadBalancerNode -RemoteAccessServer <server name>
```

## 3,7 Deaktivieren des Lasten Ausgleichs

Führen Sie diesen Schritt mithilfe von Windows PowerShell aus.

### So deaktivieren Sie den Lastenausgleich

1. Klicken Sie auf dem konfigurierten DirectAccess-Server auf **Start**, und klicken Sie dann auf **Remote Zugriffs Verwaltung**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remotezugriffs-Verwaltungskonsole auf **Konfiguration**. Klicken Sie im Bereich **Tasks** unter **Cluster mit LastenAusgleich** auf **Lastenausgleich deaktivieren**.
3. Klicken Sie im Dialogfeld **Lastenausgleich deaktivieren** auf **OK**.
4. Klicken Sie im Dialogfeld " **Lastenausgleich deaktivieren** " auf **Schließen**.

### Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
set-RemoteAccessLoadBalancer -disable
```

Durch das Deaktivieren des Lasten Ausgleichs werden Remote Zugriffs Einstellungen und NLB-Einstellungen (sofern konfiguriert) von allen Servern außer dem Server entfernt, von dem aus Sie ausgeführt werden. Auf diesem RAS-Server werden NLB-Einstellungen entfernt (sofern konfiguriert), aber die Remote Zugriffs Einstellungen bleiben erhalten.

Wenn Sie auf **Konfigurationseinstellungen entfernen** klicken, werden Remote Zugriff und NLB (sofern konfiguriert) von allen Servern in der Bereitstellung entfernt.

#### **NOTE**

- Wenn der Remote Zugriff beim Bereitstellen des Lasten Ausgleichs deinstalliert wird, verbleiben alle Server mit Dips. Die VIPs werden entfernt. Dies bewirkt, dass alle Routen im Unternehmensnetzwerk, die für die VIPs-Adressen vorgesehen sind, fehlschlagen. Dies wirkt sich auch auf DNS-Einträge aus, die zu den VIPs aufgelöst wurden, wie z. b. den Antragsteller Namen des Netzwerkadressen Servers Um dieses Problem zu vermeiden, deaktivieren Sie den Lastenausgleich, bei dem die VIPs auf dem letzten RAS-Server belassen werden, und deinstallieren Sie dann den Remote Zugriff.
- Nachdem Sie das Cmdlet "**Set-remoteaccessloadbalancer**" zum Deaktivieren des Lasten Ausgleichs verwendet haben, warten Sie zwei Minuten, bevor Sie ein beliebiges anderes Cmdlet ausführen. Dies sollte auch in allen Skripts erfolgen, die nach dem **Set-remoteaccessloadbalancer-deaktivierte** Cmdlet ein anderes Cmdlet ausführen.
- Durch die Deaktivierung des Lasten Ausgleichs wird die virtuelle IP-Adresse des Clusters in eine dedizierte IP-Adresse geändert. Daher schlägt jeder Vorgang, bei dem der Name des Servers abgefragt wird, so lange fehl, bis der zwischengespeicherte DNS-Eintrag auf dem Server abläuft. Stellen Sie sicher, dass Sie keine PowerShell-Cmdlets für den Remote Zugriff ausführen, nachdem Sie den Lastenausgleich deaktiviert haben, bis der Cache auf dem Server abgelaufen ist. Dieses Problem ist häufiger, wenn Sie versuchen, den Lastenausgleich auf einem Computer von einem anderen Computer in einer anderen Domäne zu deaktivieren. Dies geschieht auch, wenn Sie den Lastenausgleich über die Remote Zugriffs-Verwaltungskonsole deaktivieren und das Laden der Konfiguration möglicherweise verhindern. Die Konfiguration wird geladen, nachdem der Cache abgelaufen ist oder geleert wurde.

## Siehe auch

- [Schritt 4: Überprüfen des Clusters](#)

# Schritt 4 Überprüfen des Clusters

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie überprüfen, ob Sie die DirectAccess-Cluster Bereitstellung richtig konfiguriert haben.

## **So überprüfen Sie den Zugriff auf interne Ressourcen über den Cluster**

1. Stellen Sie eine Verbindung von einem DirectAccess-Clientcomputer mit dem Unternehmensnetzwerk her, und rufen Sie die Gruppenrichtlinie ab.
2. Verbinden Sie den Clientcomputer mit dem externen Netzwerk, und versuchen Sie, auf interne Ressourcen zuzugreifen.

Sie sollten auf alle Unternehmensressourcen zugreifen können.

3. Testen Sie die Konnektivität über jeden Server im Cluster, indem Sie die Verbindung mit dem externen Netzwerk ausschalten oder trennen, bis auf einen der Cluster Server. Versuchen Sie auf dem Client Computer, auf Unternehmensressourcen zuzugreifen. Wiederholen Sie den Test auf einem anderen Cluster Server.

Sie sollten in der Lage sein, über jeden Cluster Server auf alle Unternehmensressourcen zuzugreifen.

# Bereitstellen Sie mehrere RAS-Server in einer Bereitstellung mit mehreren Standorten

09.04.2020 • 18 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess-und RAS-VPN (RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle. Der Remotezugriff kann in einer Reihe von Unternehmenszenarios bereitgestellt werden. Diese Übersicht bietet eine Einführung in das Unternehmens Szenario für die Bereitstellung von Remote Zugriffs Servern in einer Konfiguration mit mehreren Standorten.

## Szenariobeschreibung

In einer Bereitstellung mit mehreren Standorten werden zwei oder mehr RAS-Server oder Server Cluster als verschiedene Einstiegspunkte an einem einzigen Standort oder an verteilten geografischen Orten bereitgestellt und konfiguriert. Durch die Bereitstellung mehrerer Einstiegspunkte an einem einzigen Standort können Server Redundanz oder RAS-Server mit vorhandener Netzwerkarchitektur bereitgestellt werden. Durch die Bereitstellung nach geografischem Standort wird die effiziente Nutzung von Ressourcen sichergestellt, da Remote Client Computer mithilfe eines am nächsten liegenden Einstiegs Punkts eine Verbindung mit internen Netzwerkressourcen herstellen können. Der Datenverkehr in einer Bereitstellung mit mehreren Standorten kann mit einem externen globalen Load Balancer verteilt und ausgeglichen werden.

Bei einer Bereitstellung mit mehreren Standorten werden Client Computer unter Windows 10, Windows 8 oder Windows 7 unterstützt. Auf Client Computern, auf denen Windows 10 oder Windows 8 ausgeführt wird, wird automatisch ein Einstiegspunkt identifiziert, oder der Benutzer kann einen Einstiegspunkt manuell auswählen. Die automatische Zuweisung erfolgt in der folgenden Prioritäts Reihenfolge:

1. Verwenden Sie einen vom Benutzer manuell ausgewählten Einstiegspunkt.
2. Verwenden Sie einen Einstiegspunkt, der von einem externen globalen Load Balancer identifiziert wird, wenn ein solcher bereitgestellt wird.
3. Verwenden Sie den nächstgelegenen Einstiegspunkt, der vom Client Computer mithilfe eines automatischen Test Mechanismus identifiziert wird.

Die Unterstützung für Clients, auf denen Windows 7 ausgeführt wird, muss für jeden Einstiegspunkt manuell aktiviert werden, und die Auswahl eines Einstiegs Punkts durch diese Clients wird nicht unterstützt.

## Erforderliche Komponenten

Bevor Sie mit der Bereitstellung dieses Szenarios beginnen, sollten Sie die Liste der wichtigen Anforderungen lesen:

- Die Bereitstellung [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) muss vor einer Bereitstellung mit mehreren Standorten bereitgestellt werden.
- Windows 7-Clients stellen immer eine Verbindung mit einem bestimmten Standort her. Sie sind nicht in der Lage, eine Verbindung mit dem nächstgelegenen Standort basierend auf dem Standort des Clients herzustellen (im Gegensatz zu Windows 10-, 8-oder 8,1-Clients).
- Das Ändern von Richtlinien außerhalb der DirectAccess-Verwaltungskonsole oder von PowerShell-Cmdlets wird nicht unterstützt.

- Eine Public Key-Infrastruktur muss bereitgestellt werden.

Weitere Informationen finden Sie unter: [Testumgebungsanleitung – Minimodul: Basis-PKI für Windows Server 2012](#)

- Das Unternehmensnetzwerk muss IPv6-fähig sein. Wenn Sie ISATAP verwenden, sollten Sie es entfernen und das systemeigene IPv6 verwenden.

## Inhalt dieses Szenarios

Das Szenario für die Bereitstellung für mehrere Standorte umfasst eine Reihe von Schritten:

1. Stellen Sie [einen einzelnen DirectAccess-Server mit erweiterten Einstellungen](#) bereit. Vor dem Einrichten einer Bereitstellung für mehrere Standorte muss ein einzelner Remote Zugriffs Server mit erweiterten Einstellungen bereitgestellt werden.
2. [Planen Sie eine Bereitstellung für mehrere Standorte](#). Zum Erstellen einer Bereitstellung für mehrere Standorte auf einem einzelnen Server sind eine Reihe zusätzlicher Planungsschritte erforderlich, einschließlich der Konformität mit den Voraussetzungen für mehrere Standorte und der Planung für Active Directory Sicherheitsgruppen, Gruppenrichtlinie Objekte (GPOs), DNS und Client Einstellungen.
3. [Konfigurieren Sie eine Bereitstellung für mehrere Standorte](#). Dies umfasst eine Reihe von Konfigurationsschritten, einschließlich der Vorbereitung der Active Directory-Infrastruktur, der Konfiguration des vorhandenen Remote Zugriffs Servers und der Addition mehrerer RAS-Server als Einstiegspunkte für die Bereitstellung für mehrere Standorte.
4. Problembehandlung bei einer [Bereitstellung mit mehreren Standorten](#). In diesem Abschnitt zur Problembehandlung werden einige der häufigsten Fehler beschrieben, die beim Bereitstellen des Remote Zugriffs in einer Bereitstellung mit mehreren Standorten auftreten können.

## Praktische Anwendungen

Eine Bereitstellung mit mehreren Standorten bietet Folgendes:

- Verbesserte Leistung: bei einer Bereitstellung mit mehreren Standorten können Client Computer mithilfe des Remote Zugriffs auf interne Ressourcen zugreifen, indem Sie den nächstgelegenen und am besten geeigneten Einstiegspunkt verwenden. Der Client greift effizient auf interne Ressourcen zu, und die Geschwindigkeit von Client Internet Anforderungen, die über DirectAccess weitergeleitet werden, wurde verbessert. Der Datenverkehr über Einstiegspunkte kann mithilfe eines externen globalen Load Balancers ausgeglichen werden.
- Erleichterte Verwaltung: mit mehreren Standorten können Administratoren die Bereitstellung des Remote Zugriffs an eine Active Directory Standorte-Bereitstellung ausrichten und so eine vereinfachte Architektur bereitstellen. Freigegebene Einstellungen können problemlos auf Einstiegspunkt Server oder Cluster festgelegt werden. Remote Zugriffs Einstellungen können von einem beliebigen Server in der Bereitstellung oder Remote mithilfe von Remoteserver-Verwaltungstools (RSAT) verwaltet werden. Außerdem kann die gesamte Bereitstellung für mehrere Standorte über eine einzelne Remote Zugriffs-Verwaltungskonsole überwacht werden.

## In diesem Szenario enthaltene Rollen und Features

In der folgenden Tabelle sind die in diesem Szenario verwendeten Rollen und Features aufgeführt.

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
---------------	---

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Remotezugriffs-Rolle	<p>Diese Rolle wird mithilfe der Server-Manager-Konsole installiert und deinstalliert. Sie umfasst DirectAccess (zuvor ein Feature unter Windows Server 2008 R2) sowie die Routing- und RAS-Dienste (RRAS, zuvor ein Rollendienst unter der Serverrolle für Netzwerkrichtlinien- und Zugriffsdienste). Die Remotezugriffs-Rolle besteht aus zwei Komponenten:</p> <ul style="list-style-type: none"> <li>-DirectAccess und RRAS (Routing and Remote Access Services) VPN-DirectAccess und VPN werden in der Remote Zugriffs-Verwaltungskonsole verwaltet.</li> <li>-RRAS-Routing: RRAS-Routing Features werden in der Legacy-Routing- und Remote Zugriffs Konsole verwaltet.</li> </ul> <p>Es bestehen folgende Abhängigkeiten:</p> <ul style="list-style-type: none"> <li>-Internetinformationsdienste (IIS)-Webserver: dieses Feature ist erforderlich, um den Netzwerkadressen Server und den Standard Webtest zu konfigurieren.</li> <li>-Interne Windows-Datenbank: wird für die lokale Kontoführung auf dem Remote Zugriffs Server verwendet.</li> </ul>
Feature "Tools für die Remotezugriffsverwaltung"	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"> <li>-Sie wird standardmäßig auf einem RAS-Server installiert, wenn die Remote Zugriffs Rolle installiert ist, und unterstützt die Benutzeroberfläche der Remote Verwaltungskonsole.</li> <li>-Es kann optional auf einem Server installiert werden, auf dem die Remote Zugriffs-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.</li> </ul> <p>Das Feature "Tools für die Remotezugriffsverwaltung" besteht aus den folgenden Komponenten:</p> <ul style="list-style-type: none"> <li>-Remote Zugriffs-GUI und Befehlszeilen Tools</li> <li>-Remote Zugriffs Modul für Windows PowerShell</li> </ul> <p>Abhängigkeiten umfassen:</p> <ul style="list-style-type: none"> <li>-Gruppenrichtlinien-Verwaltungskonsole</li> <li>-RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li> <li>-Windows PowerShell 3,0</li> <li>-Tools und Infrastruktur für die grafische Verwaltung</li> </ul>

## Hardwareanforderungen

Für dieses Szenario müssen die folgenden Hardwareanforderungen erfüllt werden:

- Mindestens zwei RAS-Computer, die in einer Bereitstellung mit mehreren Standorten gesammelt werden sollen.
- Um das Szenario zu testen, ist mindestens ein Computer erforderlich, auf dem Windows 8 ausgeführt wird und der als DirectAccess-Client konfiguriert ist. Um das Szenario für Clients mit Windows 7 zu testen, ist mindestens ein Computer erforderlich, auf dem Windows 7 ausgeführt wird.
- Für den Lastenausgleich des Datenverkehrs auf Einstiegspunkt Server ist ein externer globaler Load Balancer eines Drittanbieters erforderlich.

## Software Anforderungen

Für dieses Szenario müssen die folgenden Softwareanforderungen erfüllt werden:

- Softwareanforderungen für die Bereitstellung auf einem Einzelserver.
- Zusätzlich zu den Softwareanforderungen für einen einzelnen Server gibt es eine Reihe von Anforderungen für mehrere Standorte:
  - IPSec-Authentifizierungsanforderungen: bei einer Bereitstellung für mehrere Standorte muss DirectAccess mithilfe der IPSec-Computer Zertifikat Authentifizierung bereitgestellt werden. Die Option zum Ausführen der IPSec-Authentifizierung mithilfe des RAS-Servers als Kerberos-Proxy wird nicht unterstützt. Zum Bereitstellen der IPSec-Zertifikate ist eine interne Zertifizierungsstelle erforderlich.
  - Anforderungen an die IP-HTTPS-und Netzwerkadressen Server: die für IP-HTTPS und den Netzwerkadressen Server erforderlichen Zertifikate müssen von einer Zertifizierungsstelle ausgestellt werden. Die Option zum Verwenden von Zertifikaten, die vom Remote Zugriffs Server automatisch ausgestellt und selbst signiert werden, wird nicht unterstützt. Zertifikate können von einer internen Zertifizierungsstelle oder von einer externen Zertifizierungsstelle eines Drittanbieters ausgestellt werden.
  - Active Directory Anforderungen: mindestens ein Active Directory Standort ist erforderlich. Der Remote Zugriffs Server sollte sich am-Standort befinden. Für schnellere Update Zeiten wird empfohlen, dass jeder Standort über einen beschreibbaren Domänen Controller verfügt, obwohl dies nicht zwingend erforderlich ist.
  - Sicherheitsgruppen Anforderungen: Anforderungen lauten wie folgt:
    - Für alle Windows 8-Client Computer von allen Domänen ist eine einzelne Sicherheitsgruppe erforderlich. Es wird empfohlen, für jede Domäne eine eindeutige Sicherheitsgruppe dieser Clients zu erstellen.
    - Für jeden Einstiegspunkt, der zur Unterstützung von Windows 7-Clients konfiguriert ist, ist eine eindeutige Sicherheitsgruppe mit Windows 7-Computern erforderlich. Es wird empfohlen, für jeden Einstiegspunkt in jeder Domäne eine eindeutige Sicherheitsgruppe zu haben.
    - Computer dürfen immer nur einer Sicherheitsgruppe zugeordnet werden, die DirectAccess-Clients enthält. Wenn Clients in mehreren Gruppen enthalten sind, funktioniert die Namensauflösung für Clientanforderungen nicht wie erwartet.
  - GPO-Anforderungen: GPOs können manuell erstellt werden, bevor der Remote Zugriff konfiguriert wird, oder Sie werden automatisch während der Remote Zugriffs Bereitstellung erstellt. Die Anforderungen lauten wie folgt:
    - Ein eindeutiges Client-GPO ist für jede Domäne erforderlich.
    - Ein Server-GPO ist für jeden Einstiegspunkt in der Domäne erforderlich, in der sich der Einstiegspunkt befindet. Wenn sich also mehrere Einstiegspunkte in derselben Domäne befinden, werden mehrere Server-Gruppenrichtlinien Objekte (eines für jeden Einstiegspunkt) in der Domäne angezeigt.
    - Für jede Domäne ist ein eindeutiges Windows 7-Client-Gruppenrichtlinien Objekt für jeden Einstiegspunkt erforderlich, der für die Windows 7-Client Unterstützung aktiviert ist.

## Bekannte Probleme

Im folgenden finden Sie bekannte Probleme beim Konfigurieren eines Szenarios mit mehreren Standorten:

- **Mehrere Einstiegspunkte im gleichen IPv4-Subnetz.** Wenn Sie mehrere Einstiegspunkte im gleichen

IPv4-Subnetz hinzufügen, wird eine IP-Adress Konflikt Meldung angezeigt, und die DNS64-Adresse für den Einstiegspunkt wird nicht erwartungsgemäß konfiguriert. Dieses Problem tritt auf, wenn IPv6 nicht auf den internen Schnittstellen der Server im Unternehmensnetzwerk bereitgestellt wurde. Um dieses Problem zu vermeiden, führen Sie den folgenden Windows PowerShell-Befehl auf allen aktuellen und zukünftigen RAS-Servern aus:

```
Set-NetIPInterface -InterfaceAlias <InternalInterfaceName> -AddressFamily IPv6 -DadTransmits 0
```

- Wenn die für DirectAccess-Clients für die Verbindung mit dem RAS-Server angegebene öffentliche Adresse ein Suffix enthält, das in NRPT enthalten ist, funktioniert DirectAccess möglicherweise nicht wie erwartet. Stellen Sie sicher, dass die NRPT eine Ausnahme für den öffentlichen Namen aufweist. Bei einer Bereitstellung mit mehreren Standorten sollten Ausnahmen für die öffentlichen Namen aller Einstiegspunkte hinzugefügt werden. Beachten Sie, dass diese Ausnahmen automatisch hinzugefügt werden, wenn die Tunnel Erzwingung aktiviert ist. Sie werden entfernt, wenn die Tunnel Erzwingung deaktiviert ist.
- Wenn Sie das Windows PowerShell-Cmdlet **Deaktivieren-damultisite** verwenden, haben die Parameter "WhatIf" und "Confirm" keine Auswirkung, und die Funktion "Multisite" wird deaktiviert, und die Gruppenrichtlinien Objekte von Windows 7 werden entfernt.
- Wenn Windows 7-Clients, die DCA in einer Bereitstellung mit mehreren Standorten verwenden, auf Windows 8 aktualisiert werden, funktioniert der netzwerkkonnektivitätsassistent nicht. Dieses Problem kann im Vorfeld des Client Upgrades behoben werden, indem die Windows 7-Gruppenrichtlinien Objekte mithilfe der folgenden Windows PowerShell-Cmdlets geändert werden:

```
Set-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant" -ValueName "TemporaryValue" -Type Dword -Value 1  
Remove-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant"
```

Wenn der Client bereits aktualisiert wurde, verschieben Sie den Client Computer in die Sicherheitsgruppe Windows 8.

- Wenn Sie Domänen Controller Einstellungen mithilfe des Windows PowerShell-Cmdlets **Set-daentrypointdc** ändern und der angegebene Computername-Parameter ein RAS-Server an einem anderen Einstiegspunkt als der der Bereitstellung mit mehreren Standorten hinzugefügt wird, wird eine Warnung mit dem Hinweis angezeigt, dass der angegebene Server erst nach der nächsten Richtlinien Aktualisierung aktualisiert wird. Die tatsächlichen Server, die nicht aktualisiert wurden, können mit dem **Konfigurations Status** im **Dashboard** der **Remote Zugriffs-Verwaltungskonsole** angezeigt werden. Dadurch entstehen keine funktionalen Probleme. Sie können jedoch **gpupdate/force** auf den Servern ausführen, die nicht aktualisiert wurden, damit der Konfigurations Status sofort aktualisiert wird.
- Wenn Multisite in einem reinen IPv4-Unternehmensnetzwerk bereitgestellt wird, wird durch Ändern des IPv6-Präfixes für das interne Netzwerk auch die DNS64-Adresse geändert, aber nicht die Adresse der Firewallregeln, die DNS-Abfragen an den DNS64-Dienst erlauben. Um dieses Problem zu beheben, führen Sie die folgenden Windows PowerShell-Befehle aus, nachdem Sie das interne IPv6-Präfix geändert haben:

```

$dns64Address = (Get-DAClientDnsConfiguration).NrptEntry | ?{ $_.DirectAccessDnsServers -match ':3333::1' } | Select-Object -First 1 -ExpandProperty DirectAccessDnsServers

$serverGpoName = (Get-RemoteAccess).ServerGpoName

$serverGpoDc = (Get-DAEntryPointDC).DomainControllerName

$gpoSession = Open-NetGPO -PolicyStore $serverGpoName -DomainController $serverGpoDc

Get-NetFirewallRule -GPOSession $gpoSession | ? {$_['Name'] -in @('0FDEEC95-1EA6-4042-8BA6-6EF5336DE91A',
'24FD98AA-178E-4B01-9220-D0DADA9C8503')} | Set-NetFirewallRule -LocalAddress $dns64Address

Save-NetGPO -GPOSession $gpoSession

```

- Wenn DirectAccess bereitgestellt wurde, als eine vorhandene ISATAP-Infrastruktur vorhanden war, wird beim Entfernen eines Einstiegs Punkts, bei dem es sich um einen ISATAP-Host handelt, die IPv6-Adresse des DNS64-Diensts aus den DNS-Serveradressen aller DNS-Suffixe in der NRPT entfernt.

Um dieses Problem zu beheben, entfernen Sie im Assistenten zum **Einrichten des Infrastruktur Servers** auf der Seite **DNS** die geänderten DNS-Suffixe, und fügen Sie Sie erneut mit den richtigen DNS-Serveradressen hinzu, indem Sie im Dialogfeld **DNS-Serveradressen** auf **erkennen** klicken.

# Planen einer Bereitstellung mit mehreren Standorten

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016, Windows Server 2012 kombinieren DirectAccess- und RRAS-VPN (Routing and Remote Access Service, Routing- und RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle. Diese Übersicht bietet eine Einführung in die erforderlichen Planungsschritte für die Bereitstellung von Windows Server 2016 oder Windows Server 2012 Remote Access in einer Konfiguration mit mehreren Standorten.

1. Stellen Sie [einen einzelnen DirectAccess-Server mit erweiterten Einstellungen](#) bereit. Dieser Schritt umfasst die Planung der Infrastruktur, die für die Bereitstellung eines einzelnen Servers erforderlich ist. Dazu gehört die Planung von Netzwerk- und Servereinstellungen, Zertifikat Anforderungen, DNS-Einstellungen, Bereitstellung des Netzwerkadressen Servers, DirectAccess-Verwaltungs Servern, Active Directory Einstellungen und Gruppenrichtlinie Objekte (GPOs).
2. [Schritt 2: Planen der Infrastruktur für mehrere Standorte](#). Dieser Schritt umfasst Active Directory- und GPO-Planung und DNS-Konfiguration.
3. [Schritt 3: Planen der Bereitstellung für mehrere Standorte](#). Dieser Schritt umfasst die Planung von Zertifikat Einstellungen, die Netzwerkadressen Server-Konfiguration, Einstellungen für Client Einstiegspunkte, IPv6-Präfix Einstellungen und optional globale Einstellungen für den Lastenausgleich.

## NOTE

Notieren Sie Ihre Planungsentscheidungen für die erweiterte Remote Zugriffs Bereitstellung. Dieser Datensatz kann als Arbeitshilfe für die Personen verwendet werden, die in den Abschluss der Bereitstellungsschritte involviert sind.

Nachdem Sie diese Planungsschritte abgeschlossen haben, finden Sie weitere Informationen unter [Konfigurieren einer Bereitstellung für mehrere Standorte](#).

# Schritt 1 Planen einer erweiterten Einzel Server Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt bei der Planung eines Remote Zugriffs mit der Bereitstellung eines einmaligen Kennworts (OTP)-Client Authentifizierung ist das Planen und Konfigurieren einer erweiterten Einzel Server Bereitstellung.

## Planen einer Bereitstellung auf einem einzelnen Server

Stellen Sie vor dem Bereitstellen des Remote Zugriffs mit OTP sicher, dass Sie alle Schritte zum Bereitstellen eines einzelnen Remote Zugriffs Servers abgeschlossen haben. Weitere Informationen finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).

# Schritt 2 Planen der Infrastruktur für mehrere Standorte

09.04.2020 • 24 minutes to read • [Edit Online](#)

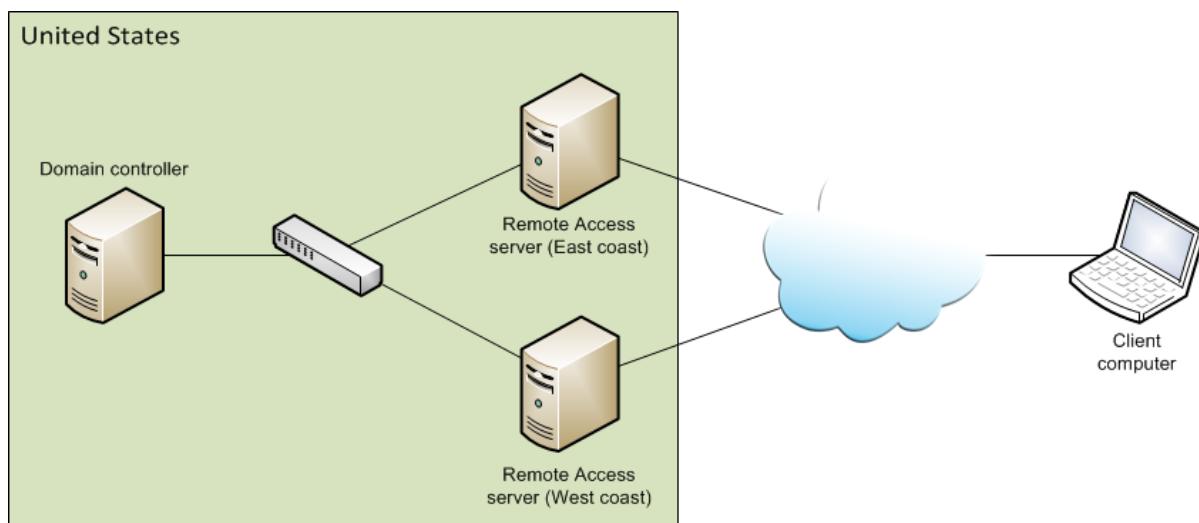
Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der nächste Schritt beim Bereitstellen des Remote Zugriffs in einer Topologie mit mehreren Standorten besteht darin, die Infrastrukturplanung für mehrere Standorte abzuschließen, einschließlich, Active Directory, Sicherheitsgruppen und Gruppenrichtlinie Objekten.

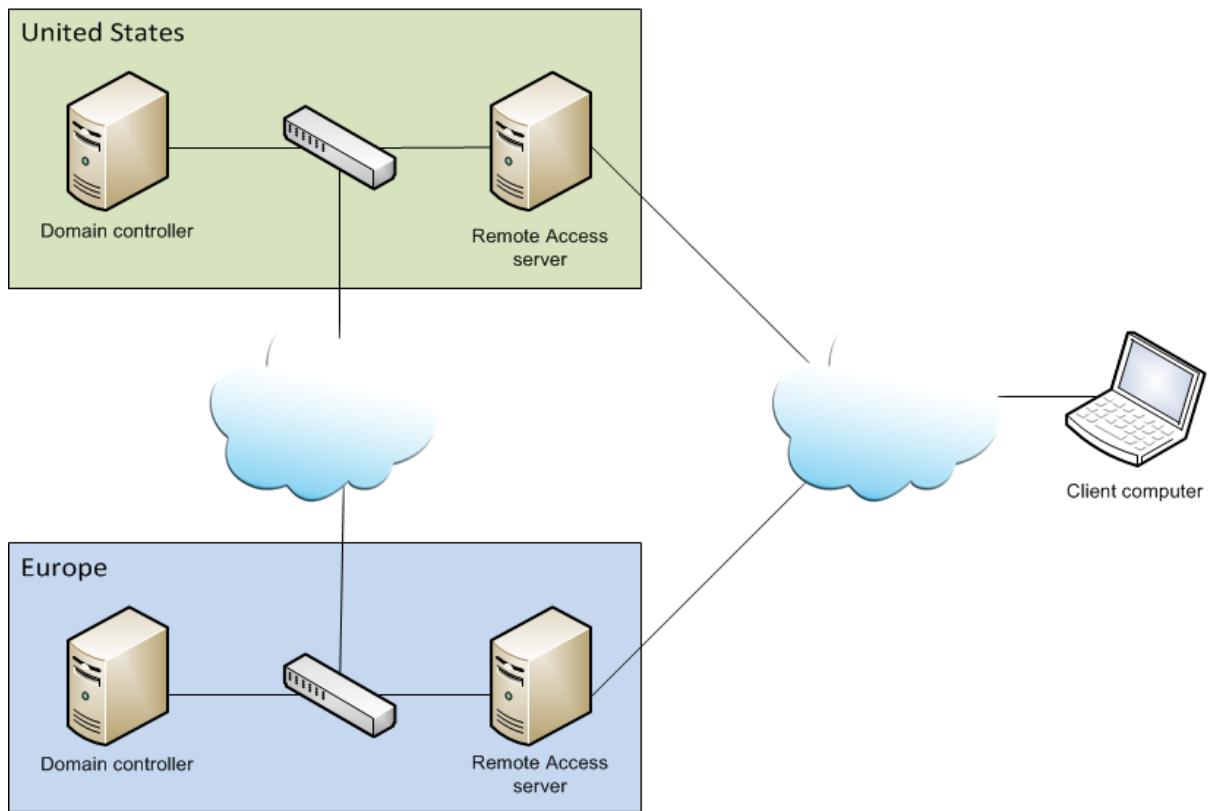
## 2,1 Plan Active Directory

Eine Remote Zugriffs Bereitstellung für mehrere Standorte kann in einer Reihe von Topologien konfiguriert werden:

- **Einzelne Active Directory Site, mehrere Einstiegspunkte:** in dieser Topologie verfügen Sie über einen einzelnen Active Directory Standort für Ihre gesamte Organisation mit schnellen intranetverknüpfungen auf der gesamten Website, aber Sie verfügen über mehrere RAS-Server, die in ihrer gesamten Organisation bereitgestellt werden, die jeweils als Einstiegspunkt fungieren. Ein geografisches Beispiel für diese Topologie ist die Verwendung einer einzelnen Active Directory Site für die USA mit Einstiegspunkten an der Ostküste und der Westküste.



- **Mehrere Active Directory Standorte, mehrere Einstiegspunkte:** in dieser Topologie verfügen Sie über zwei oder mehr Active Directory Standorte mit einem Remote Zugriffs Server, die als Einstiegspunkt für jeden Standort bereitgestellt werden. Jeder RAS-Server ist dem Active Directory Domänen Controller für den Standort zugeordnet. Ein geografisches Beispiel für diese Topologie ist die Verwendung einer Active Directory Site für die USA und einer für Europa mit einem einzelnen Einstiegspunkt für jeden Standort. Beachten Sie Folgendes: Wenn Sie über mehrere Active Directory Standorte verfügen, benötigen Sie keinen Einstiegspunkt, der mit jedem Standort verknüpft ist. Außerdem können einige Active Directory Websites mehrere Einstiegspunkte zugeordnet werden.



An einem Einstiegspunkt mit mehreren Standorten können Sie einen einzelnen RAS-Server, mehrere RAS-Server oder einen Remote Zugriffs Server-Cluster konfigurieren.

### **Bewährte Methoden und Empfehlungen Active Directory**

Beachten Sie die folgenden Empfehlungen und Einschränkungen für Active Directory-Bereitstellung in einem Szenario mit mehreren Standorten:

1. Jede Active Directory Site kann einen oder mehrere RAS-Server oder einen Server Cluster enthalten, der als Einstiegspunkte für mehrere Standorte für Client Computer fungiert. Es ist jedoch nicht erforderlich, dass eine Active Directory Site einen Einstiegspunkt hat.
2. Ein Einstiegspunkt mit mehreren Standorten kann nur einer einzelnen Active Directory Site zugeordnet werden. Wenn auf Client Computern, auf denen Windows 8 ausgeführt wird, eine Verbindung mit einem bestimmten Einstiegspunkt hergestellt wird, werden Sie als zu der Active Directory Site, die dem Einstiegspunkt zugeordnet ist, als
3. Es wird empfohlen, dass jeder Active Directory Standort über einen Domänen Controller verfügt. Der Domänen Controller kann schreibgeschützt sein.
4. Wenn jeder Active Directory Standort einen Domänen Controller enthält, wird das Gruppenrichtlinien Objekt für einen Server im Einstiegspunkt von einem der Domänen Controller in der Active Directory Site verwaltet, die dem Endpunkt zugeordnet ist. Wenn an diesem Standort keine Domänen Controller mit aktiviertem Schreibzugriff vorhanden sind, wird das Gruppenrichtlinien Objekt für einen Server auf einem Domänen Controller mit aktiviertem Schreibzugriff verwaltet, der dem ersten Remote Zugriffs Server am nächsten liegt, der im Einstiegspunkt konfiguriert ist. Der nächstgelegene Wert wird durch eine Berechnung der Link Kosten festgelegt. Beachten Sie, dass in diesem Szenario nach dem vornehmen von Konfigurationsänderungen bei der Replikation zwischen dem Domänen Controller, der das Gruppenrichtlinien Objekt verwaltet, und dem schreibgeschützten Domänen Controller auf dem Active Directory Standort des Servers eine Verzögerung auftreten kann.
5. Client-Gruppenrichtlinien Objekte und optionale Anwendungsserver-Gruppenrichtlinien Objekte werden auf dem Domänen Controller verwaltet, der als primärer Domänen Controller Emulator (PDC) ausgeführt wird. Dies bedeutet, dass Client-Gruppenrichtlinien Objekte nicht notwendigerweise an der Active Directory Site

verwaltet werden, die den Einstiegspunkt enthält, mit dem Clients eine Verbindung herstellen.

6. Wenn der Domänen Controller für einen Active Directory Standort nicht erreichbar ist, stellt der RAS-Server eine Verbindung mit einem alternativen Domänen Controller am Standort her (falls verfügbar). Wenn dies nicht der Fall ist, wird eine Verbindung mit dem Domänen Controller eines anderen Standorts hergestellt, um ein aktualisiertes GPO abzurufen und Clients zu authentifizieren. In beiden Fällen können die Remote Zugriffs-Verwaltungskonsole und die PowerShell-Cmdlets nicht zum Abrufen oder Ändern von Konfigurationseinstellungen verwendet werden, bis der Domänen Controller verfügbar ist. Beachten Sie Folgendes:
  - a. Wenn der Server, auf dem der PDC-Emulator ausgeführt wird, nicht verfügbar ist, müssen Sie einen verfügbaren Domänen Controller mit aktualisierten GPOs als PDC-Emulator angeben.
  - b. Wenn der Domänen Controller, von dem ein Server-Gruppenrichtlinien Objekt verwaltet wird, nicht verfügbar ist, verwenden Sie das PowerShell-Cmdlet Set-daentrypointdc, um einen neuen Domänen Controller dem Einstiegspunkt zuzuordnen. Der neue Domänen Controller muss vor dem Ausführen des Cmdlets über aktuelle GPOs verfügen.

## 2,2 Planen von Sicherheitsgruppen

Während der Bereitstellung eines einzelnen Servers mit erweiterten Einstellungen wurden alle Client Computer, die über DirectAccess auf das interne Netzwerk zugreifen, in einer Sicherheitsgruppe gesammelt. Bei einer Bereitstellung mit mehreren Standorten wird diese Sicherheitsgruppe nur für Windows 8-Client Computer verwendet. Bei einer Bereitstellung mit mehreren Standorten werden Windows 7-Client Computer für jeden Einstiegspunkt in der Bereitstellung für mehrere Standorte in separaten Sicherheitsgruppen erfasst. Wenn Sie z. b. zuvor alle Client Computer in der Gruppe DA\_Clients gruppiert haben, müssen Sie jetzt alle Windows 7-Computer aus dieser Gruppe entfernen und Sie in einer anderen Sicherheitsgruppe platzieren. Beispielsweise erstellen Sie in der Topologie mehrere Einstiegspunkte für mehrere Active Directory Standorte eine Sicherheitsgruppe für den USA Einstiegspunkt (DA\_Clients\_US) und einen für den Einstiegspunkt Europa (DA\_Clients\_Europe). Platzieren Sie alle Windows 7-Client Computer, die sich in der USA befinden, in der Gruppe DA\_Clients\_US und alle, die sich in Europa in der DA\_Clients\_Europe Gruppe befinden. Wenn Sie über keine Windows 7-Client Computer verfügen, müssen Sie keine Sicherheitsgruppen für Windows 7-Computer planen.

Die folgenden Sicherheitsgruppen sind erforderlich:

- Eine Sicherheitsgruppe für alle Windows 8-Client Computer. Es wird empfohlen, für jede Domäne eine eindeutige Sicherheitsgruppe für diese Clients zu erstellen.
- Eine eindeutige Sicherheitsgruppe, die Windows 7-Client Computer für jeden Einstiegspunkt enthält. Es wird empfohlen, für jede Domäne eine eindeutige Gruppe zu erstellen. Beispiel: domain1 \ DA\_Clients\_Europe; Domäne2 \ DA\_Clients\_Europe; Domain1 \ DA\_Clients\_US; Domäne2 \ DA\_Clients\_US.

## 2,3 planen Gruppenrichtlinie Objekte

DirectAccess-Einstellungen, die während der Remote Zugriffs Bereitstellung konfiguriert werden, werden in GPOs gesammelt. Ihre Einzel Server Bereitstellung verwendet bereits GPOs für DirectAccess-Clients, den Remote Zugriffs Server und optional für Anwendungsserver. Für eine Bereitstellung mit mehreren Standorten sind folgende Gruppenrichtlinien Objekte erforderlich:

- Ein Server-GPO für jeden Einstiegspunkt.
- Ein Gruppenrichtlinien Objekt für jede Domäne mit Client Computern, auf denen Windows 8 ausgeführt wird.
- Ein Gruppenrichtlinien Objekt für jeden Einstiegspunkt und jede Domäne, die Windows 7-Client Computer enthält.

GPOs können wie folgt konfiguriert werden:

- **Automatisch:** Sie können angeben, dass GPOs automatisch durch den Remote Zugriff erstellt werden. Für jedes GPO wird ein Standardname angegeben, der geändert werden kann.
- **Manuell:** Sie können Gruppenrichtlinien Objekte verwenden, die vom Active Directory-Administrator manuell erstellt wurden.

#### NOTE

Wenn DirectAccess für die Verwendung bestimmter Gruppenrichtlinien Objekte konfiguriert ist, kann es nicht für die Verwendung unterschiedlicher GPOs konfiguriert werden.

### 2.3.1 automatisch erstellte Gruppenrichtlinien Objekte

Beachten Sie beim Verwenden automatisch erstellter Gruppenrichtlinienobjekte Folgendes:

- Automatisch erstellte Gruppenrichtlinienobjekte werden entsprechend des Speicherorts und Verknüpfungszielparameters wie folgt angewendet:
  - Für das Server-Gruppenrichtlinien Objekt zeigen der Speicherort und die Verknüpfungs Parameter auf die Domäne, die den Remote Zugriffs Server enthält.
  - Für Client-Gruppenrichtlinien Objekte wird das Verknüpfungs Ziel auf den Stamm der Domäne festgelegt, in der das Gruppenrichtlinien Objekt erstellt wurde. Für jede Domäne, die Client Computer enthält, wird ein Gruppenrichtlinien Objekt erstellt, und das Gruppenrichtlinien Objekt wird mit dem Stamm der einzelnen Domänen verknüpft..
- Für automatisch erstellte Gruppenrichtlinien Objekte benötigt der RAS-Server Administrator die folgenden Berechtigungen, um DirectAccess-Einstellungen anzuwenden:
  - Berechtigungen zum Erstellen von Gruppenrichtlinien Objekten für erforderliche Domänen.
  - Verknüpfungsberechtigungen für alle ausgewählten Clientdomänenstämme.
  - Die Berechtigung zum Erstellen des WMI-Filters für GPOs ist erforderlich, wenn DirectAccess nur für mobile Computer konfiguriert wurde.
  - Link Berechtigungen für die Stämme von Domänen, die den Einstiegspunkten zugeordnet sind (die Server-GPO-Domänen)
  - Es wird empfohlen, dass der Remotezugriffsadministrator über Leserechte für Gruppenrichtlinienobjekte für jede Domäne verfügt. Dadurch wird der Remote Zugriff aktiviert, um sicherzustellen, dass GPOs mit doppelten Namen beim Erstellen von Gruppenrichtlinien Objekten für die Bereitstellung für mehrere Standorte nicht vorhanden sind.
  - Active Directory Replikations Berechtigungen für Domänen, die Einstiegspunkten zugeordnet sind. Dies liegt daran, dass beim ersten Hinzufügen von Einstiegspunkten das Server-GPO für den Einstiegspunkt auf dem Domänen Controller erstellt wird, der diesem Einstiegspunkt am nächsten ist. Da die Verknüpfungs Erstellung jedoch nur auf dem PDC-Emulator unterstützt wird, muss das Gruppenrichtlinien Objekt vom Domänen Controller, auf dem es erstellt wurde, auf den Domänen Controller repliziert werden, auf dem der PDC-Emulator ausgeführt wird, bevor der Link erstellt wird

Beachten Sie, dass eine Warnung ausgegeben wird, wenn die richtigen Berechtigungen für die Replikation und verknüpfte Gruppenrichtlinien Objekte nicht vorhanden sind. Der Remote Zugriffs Vorgang wird fortgesetzt, die Replikation und Verknüpfung werden jedoch nicht ausgeführt. Wenn eine Link Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, auch nachdem die Berechtigungen vorhanden sind. Stattdessen muss der Administrator die Links manuell erstellen.

## **manuell erstellte Gruppenrichtlinien Objekte**

Beachten Sie beim Verwenden manuell erstellter Gruppenrichtlinienobjekte Folgendes:

- Die folgenden Gruppenrichtlinien Objekte sollten für die Bereitstellung für mehrere Standorte manuell erstellt werden:
  - **Server-GPO**: ein Server-Gruppenrichtlinien Objekt für jeden Einstiegspunkt (in der Domäne, in der sich der Einstiegspunkt befindet). Dieses GPO wird auf jedem RAS-Server im Einstiegspunkt angewendet.
  - **Client-GPO (Windows 7)** : ein Gruppenrichtlinien Objekt für jeden Einstiegspunkt und jede Domäne mit Windows 7-Client Computern, die eine Verbindung zu Einstiegspunkten in der Bereitstellung für mehrere Standorte herstellen. Zum Beispiel domain1 \ DA\_W7\_Clients\_GPO\_Europe; Domäne2 \ DA\_W7\_Clients\_GPO\_Europe; Domain1 \ DA\_W7\_Clients\_GPO\_US; Domäne2 \ DA\_W7\_Clients\_GPO\_US. Wenn keine Windows 7-Client Computer eine Verbindung mit Einstiegspunkten herstellen, sind GPOs nicht erforderlich.
- Es ist nicht erforderlich, zusätzliche GPOs für Windows 8-Client Computer zu erstellen. Ein Gruppenrichtlinien Objekt für jede Domäne, die Client Computer enthält, wurde bereits erstellt, als der einzelne RAS-Server bereitgestellt wurde. Bei einer Bereitstellung mit mehreren Standorten fungieren diese Client-Gruppenrichtlinien Objekte als GPOs für Windows 8-Clients.
- Die GPOs sollten vorhanden sein, bevor Sie in den Bereitstellungs-Assistenten für mehrere Standorte auf die Schaltfläche Commit klicken
- Beim Verwenden manuell erstellter Gruppenrichtlinienobjekte wird in der gesamten Domäne eine Suche nach einer Verknüpfung zum Gruppenrichtlinienobjekt durchgeführt. Wenn das Gruppenrichtlinienobjekt in der Domäne nicht verknüpft ist, wird im Domänenstamm automatisch eine Verknüpfung erstellt. Wenn die zum Erstellen der Verknüpfung erforderlichen Berechtigungen nicht verfügbar sind, wird eine Warnung ausgegeben.
- Wenn Sie die DirectAccess-Einstellungen mithilfe von manuell erstellten Gruppenrichtlinien Objekten anwenden, benötigt der RAS-Server Administrator vollständige GPO-Berechtigungen (bearbeiten, löschen, Ändern der Sicherheit) für die manuell erstellten Gruppenrichtlinien Objekte.

Beachten Sie, dass eine Warnung ausgegeben wird, wenn die richtigen Berechtigungen für die Replikation und verknüpfte Gruppenrichtlinien Objekte nicht vorhanden sind. Der Remote Zugriffs Vorgang wird fortgesetzt, die Replikation und Verknüpfung werden jedoch nicht ausgeführt. Wenn eine Link Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, auch nachdem die Berechtigungen vorhanden sind. Stattdessen muss der Administrator die Links manuell erstellen.

### **2.3.3 Verwalten von Gruppenrichtlinien Objekten in einer Umgebung mit mehreren Domänen Controllern**

Jedes GPO wird von einem bestimmten Domänen Controller wie folgt verwaltet:

- Das Server-Gruppenrichtlinien Objekt wird von einem der Domänen Controller an der Active Directory Site verwaltet, die dem Server zugeordnet ist, oder, wenn Domänen Controller an diesem Standort schreibgeschützt sind, von einem schreibgeschützten Domänen Controller, der dem ersten Server am Einstiegspunkt am nächsten ist.
- Client-Gruppenrichtlinien Objekte werden vom Domänen Controller verwaltet, der als PDC-Emulator ausgeführt wird.

Beachten Sie Folgendes, wenn Sie GPO-Einstellungen manuell ändern möchten:

- Führen Sie für Server-Gruppenrichtlinien Objekte das PowerShell-Cmdlet `Get-DAEntryPointDC -EntryPointName <name of entry point>` aus, um zu ermitteln, welcher Domänen Controller mit einem bestimmten Einstiegspunkt verknüpft ist.

- Wenn Sie mit den PowerShell-Cmdlets für Netzwerke oder der Gruppenrichtlinie Management Console Änderungen vornehmen, wird standardmäßig der Domänen Controller verwendet, der als PDC-Emulator fungiert.
- Beachten Sie Folgendes, wenn Sie Einstellungen auf einem Domänen Controller ändern, bei dem es sich nicht um den Domänen Controller handelt, der dem Einstiegspunkt (für Server-Gruppenrichtlinien Objekte) oder dem PDC-Emulator (für Client-GPOs) zugeordnet ist:
  1. Stellen Sie vor dem Ändern der Einstellungen sicher, dass der Domänen Controller mit einem aktuellen GPO repliziert wird, und [Sichern Sie GPO-Einstellungen](#), bevor Sie Änderungen vornehmen. Wenn das Gruppenrichtlinien Objekt nicht aktualisiert wird, können Konflikte bei der Replikation auftreten, was zu einer beschädigten Remote Zugriffs Konfiguration führt.
  2. Nachdem Sie die Einstellungen geändert haben, müssen Sie darauf warten, dass die Änderungen auf den Domänen Controller repliziert werden, der den Gruppenrichtlinien Objekten zugeordnet ist. Nehmen Sie keine weiteren Änderungen mithilfe der Remote Zugriffs-Verwaltungskonsole oder PowerShell-Cmdlets für den Remote Zugriff vor, bis die Replikation beendet ist. Wenn ein Gruppenrichtlinien Objekt auf zwei verschiedenen Domänen Controllern bearbeitet wird, bevor die Replikation beendet ist, können Mergekonflikte auftreten, was zu einer beschädigten Konfiguration führt.
- Alternativ können Sie die Standardeinstellung im Dialogfeld **Domänen Controller ändern** in der Gruppenrichtlinie-Verwaltungskonsole oder mithilfe des PowerShell-Cmdlets **Open-NetGpo** ändern, damit Änderungen, die über die-Konsole oder die-Cmdlets für Netzwerke vorgenommen wurden, den von Ihnen angegebenen Domänen Controller verwenden.
  1. Klicken Sie hierzu in der Gruppenrichtlinie-Verwaltungskonsole mit der rechten Maustaste auf den Domänen-oder Standort Container, und klicken Sie dann auf **Domänen Controller ändern**.
  2. Geben Sie in PowerShell den Parameter Domain Controller für das Cmdlet Open-netgpo an. Wenn Sie z. b. die privaten und öffentlichen Profile in der Windows-Firewall auf einem Gruppenrichtlinien Objekt mit dem Namen domain1 \ DA\_Server\_GPO\_Europe mit einem Domänen Controller namens Europe-DC.Corp.contoso.com aktivieren möchten, gehen Sie wie folgt vor:

```
$gpoSession = Open-NetGPO -PolicyStore "domain1\DA_Server_GPO_Europe" -DomainController "europe-dc.corp.contoso.com"
Set-NetFirewallProfile -GpoSession $gpoSession -Name @("Private","Public") -Enabled True
Save-NetGPO -GpoSession $gpoSession
```

#### **Ändern der Domänen Controller Zuordnung**

Um die Einheitlichkeit der Konfiguration in einer Bereitstellung für mehrere Standorte zu wahren, müssen Sie sicherstellen, dass jedes GPO von einem einzigen Domänencontroller verwaltet wird. In einigen Szenarien kann es erforderlich sein, einen anderen Domänen Controller für ein GPO zuzuweisen:

- **Wartung und Ausfall von Domänen Controllern:** Wenn der Domänen Controller, von dem ein Gruppenrichtlinien Objekt verwaltet wird, nicht verfügbar ist, kann es erforderlich sein, das GPO auf einem anderen Domänen Controller zu verwalten.
- **Optimierung der Konfigurations Verteilung:** nach der Änderung der Netzwerkinfrastruktur ist es möglicherweise erforderlich, das Server-Gruppenrichtlinien Objekt eines Einstiegs Punkts auf einem Domänen Controller an demselben Active Directory Standort wie den Einstiegspunkt zu verwalten.

## **2,4 Planen des DNS**

Beachten Sie beim Planen von DNS für eine Bereitstellung mit mehreren Standorten Folgendes:

1. Client Computer verwenden die ConnectTo-Adresse, um eine Verbindung mit dem Remote Zugriffs Server herzustellen. Für jeden Einstiegspunkt in der Bereitstellung ist eine andere ConnectTo-Adresse erforderlich. Jeder Einstiegspunkt "ConnectTo Address" muss im öffentlichen DNS verfügbar sein, und die von Ihnen gewählte Adresse muss mit dem Antragsteller Namen des IP-HTTPS-Zertifikats, das Sie für die IP-HTTPS-Verbindung bereitstellen, identisch sein.
2. Außerdem erzwingt der Remote Zugriff das symmetrische Routing. Daher können nur Teredo-und IP-HTTPS-Clients eine Verbindung herstellen, wenn eine Bereitstellung für mehrere Standorte aktiviert ist. Damit systemeigene IPv6-Clients eine Verbindung herstellen können, muss die ConnectTo-Adresse (die IP-HTTPS-URL) sowohl in die externen IPv6-und IPv4-Adressen des Remote Zugriffs Servers aufgelöst werden.
3. RAS erstellt einen Standard-Webtest, der von DirectAccess-Clientcomputern dazu verwendet wird, die Konnektivität zum internen Netzwerk zu prüfen. Während der Konfiguration des einzelnen Servers sollten die folgenden Namen in DNS registriert werden:
  - a. DirectAccess-WebProbe Host: sollte in die interne IPv4-Adresse des RAS-Servers oder die IPv6-Adresse in einer reinen IPv6-Umgebung aufgelöst werden.
  - b. DirectAccess-corpconnectivityhost: sollte in eine localhost-Adresse (Loopback) aufgelöst werden (entweder: 1 oder 127.0.0.1, je nachdem, ob IPv6 im Unternehmensnetzwerk bereitgestellt wird).

Bei einer Bereitstellung für mehrere Standorte muss für jeden Einstiegspunkt ein zusätzlicher DNS-Eintrag für DirectAccess-WebProbe Host erstellt werden. Beim Hinzufügen eines Einstiegs Punkts versucht der Remote Zugriff, diesen zusätzlichen DirectAccess-WebProbe Host-Eintrag automatisch zu erstellen. Wenn dies jedoch nicht möglich ist, wird eine Warnung angezeigt, und Sie müssen den Eintrag manuell erstellen.

**NOTE**

Wenn DNS-Bereinigung in Ihrer DNS-Infrastruktur aktiviert ist, wird empfohlen, das Bereinigung für die DNS-Einträge zu deaktivieren, die automatisch durch den Remote Zugriff erstellt werden.

# Schritt 3 Planen der Bereitstellung für mehrere Standorte

09.04.2020 • 34 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Planen Sie nach dem Planen der Infrastruktur für mehrere Standorte alle zusätzlichen Zertifikat Anforderungen, die Auswahl von Einstiegspunkten durch Client Computer und die in der Bereitstellung zugewiesenen IPv6-Adressen.

In den folgenden Abschnitten finden Sie ausführliche Informationen zur Planung.

## 3,1 Planen von IP-HTTPS-Zertifikaten

Wenn Sie die Einstiegspunkte konfigurieren, konfigurieren Sie jeden Einstiegspunkt mit einer bestimmten ConnectTo-Adresse. Das IP-HTTPS-Zertifikat für jeden Einstiegspunkt muss der ConnectTo-Adresse entsprechen. Beachten Sie beim Erhalt des Zertifikats Folgendes:

- Sie können keine selbstsignierten Zertifikate in einer Bereitstellung für mehrere Standorte verwenden.
- Die Verwendung einer öffentlichen Zertifizierungsstelle wird empfohlen, damit Zertifikatsperllisten schneller verfügbar sind.
- Geben Sie im Feld Betreff entweder die IPv4-Adresse des externen Adapters des Remote Zugriffs Servers an (wenn die ConnectTo-Adresse als IP-Adresse und nicht als DNS-Name angegeben wurde), oder geben Sie den voll qualifizierten Namen der IP-HTTPS-URL an.
- Der allgemeine Name des Zertifikats sollte dem Namen der IP-HTTPS-Website entsprechen. Die Verwendung einer Platzhalter-URL, die dem Namen des ConnectTo-DNS entspricht, wird ebenfalls unterstützt.
- Bei IP-HTTPS-Zertifikaten können Platzhalter im Antragsteller Namen verwendet werden. Das gleiche Platzhalter Zertifikat kann für alle Einstiegspunkte verwendet werden.
- Geben Sie im Feld „Erweiterte Schlüsselverwendung“ die Serverauthentifizierungs-Objektkennung (OID) an.
- Wenn Sie Client Computer unter Windows 7 in der Bereitstellung für mehrere Standorte unterstützen, geben Sie im Feld CRL-Verteilungs Punkte einen Zertifikat Sperr Listen-Verteilungs Punkt an, auf den DirectAccess-Clients, die mit dem Internet verbunden sind, zugreifen können. Dies ist für Clients, auf denen Windows 8 ausgeführt wird, nicht erforderlich (Standardmäßig ist die CRL-Sperr Überprüfung für IP-HTTPS auf diesen Clients deaktiviert).
- Das IP-HTTPS-Zertifikat muss einen privaten Schlüssel enthalten.
- Das IP-HTTPS-Zertifikat muss direkt in den persönlichen Speicher des Computers und nicht in den Benutzer importiert werden.

## 3,2 Planen des Netzwerkadressen Servers

Die Netzwerkadressen Server-Website kann auf dem Remote Zugriffs Server oder einem anderen Server in Ihrer Organisation gehostet werden. Wenn Sie den Netzwerkadressen Server auf dem Remote Zugriffs Server hosten, wird die Website automatisch erstellt, wenn Sie den Remote Zugriff bereitstellen. Wenn Sie den Netzwerkadressen

Server auf einem anderen Server hosten, auf dem ein Windows-Betriebssystem in Ihrer Organisation ausgeführt wird, müssen Sie sicherstellen, dass Internetinformationsdienste (IIS) installiert ist, um die Website zu erstellen.

### **3.2.1 Zertifikat Anforderungen für den Netzwerkadressen Server**

Stellen Sie sicher, dass die Netzwerkadressen Server-Website die folgenden Anforderungen für die Zertifikat Bereitstellung erfüllt:

- Hierfür ist ein HTTPS-Serverzertifikat erforderlich.
- Wenn sich der Netzwerkadressen Server auf dem RAS-Server befindet und Sie die Verwendung eines selbst signierten Zertifikats bei der Bereitstellung des einzelnen RAS-Servers ausgewählt haben, müssen Sie die Bereitstellung auf einem einzelnen Server so konfigurieren, dass ein von einer internen Zertifizierungsstelle ausgestelltes Zertifikat verwendet wird.
- DirectAccess-Clientcomputer müssen der Zertifizierungsstelle vertrauen, die das Serverzertifikat zur Netzwerkadressenserver-Website ausgegeben hat.
- DirectAccess-Client Computer im internen Netzwerk müssen in der Lage sein, den Namen der Netzwerkadressen Server-Website aufzulösen.
- Die Netzwerkadressen Server-Website muss für Computer im internen Netzwerk hoch verfügbar sein.
- Der Netzwerkadressenserver darf nicht für DirectAccess-Clientcomputer auf dem internen Netzwerk erreichbar sein.
- Das Serverzertifikat muss anhand einer Zertifikat Sperr Liste (CRL) überprüft werden.
- Platzhalter Zertifikate werden nicht unterstützt, wenn der Netzwerkadressen Server auf dem Remote Zugriffs Server gehostet wird.

Beachten Sie Folgendes, wenn Sie das für den Netzwerkadressen Server zu verwendende Website Zertifikat abrufen:

1. Im Feld Antragsteller muss eine IP-Adresse der Intranetschnittstelle des Netzwerkadressenservers oder der FQDN der Netzwerkadressen-URL angegeben sein. Beachten Sie, dass Sie keine IP-Adresse angeben sollten, wenn der Netzwerkadressen Server auf dem Remote Zugriffs Server gehostet wird. Dies liegt daran, dass der Netzwerkadressen Server den gleichen Antragsteller Namen für alle Einstiegspunkte verwenden muss und nicht alle Einstiegspunkte dieselbe IP-Adresse aufweisen.
2. Im Feld Erweiterte Schlüsselverwendung muss die Serverauthentifizierungs-OID angegeben sein.
3. Verwenden Sie für das Feld CRL-Verteilungs Punkte einen Zertifikat Sperr Listen-Verteilungs Punkt, auf den DirectAccess-Clients, die mit dem Intranet verbunden sind, zugreifen können.

### **3.2.2 DNS für den Netzwerkadressen Server**

Wenn Sie den Netzwerkadressen Server auf dem Remote Zugriffs Server hosten, müssen Sie für jeden Einstiegspunkt in der Bereitstellung einen DNS-Eintrag für die Netzwerkadressen Server-Website hinzufügen. Beachten Sie Folgendes:

- Der Antragsteller Name des ersten Netzwerkadressen Server-Zertifikats in der Bereitstellung für mehrere Standorte wird als Netzwerkadressen Server-URL für alle Einstiegspunkte verwendet. Daher dürfen der Antragsteller Name und die Netzwerkadressen Server-URL nicht mit dem Computernamen des der erste RAS-Server in der Bereitstellung. Dabei muss es sich um einen für den Netzwerkadressen Server dedizierten voll qualifizierten Namen handeln.
- Der vom Netzwerkadressen Server-Datenverkehr bereitgestellte Dienst wird mithilfe von DNS auf Einstiegspunkte ausgeglichen. Daher sollte ein DNS-Eintrag mit der gleichen URL für jeden Einstiegspunkt vorhanden sein, der mit der internen IP-Adresse des Einstiegs Punkts konfiguriert ist.

- Alle Einstiegspunkte müssen mit einem Netzwerkadressen Server-Zertifikat identisch sein, das den gleichen Antragsteller Namen hat (der der Netzwerkadressen Server-URL entspricht).
- Die Netzwerkadressen Server-Infrastruktur (DNS-und Zertifikat Einstellungen) für einen Einstiegspunkt muss erstellt werden, bevor der Einstiegspunkt hinzugefügt wird.

### 3,3 planen Sie das IPSec-Stamm Zertifikat für alle Remote Zugriffs Server.

Beachten Sie beim Planen der IPSec-Client Authentifizierung in einer Bereitstellung für mehrere Standorte Folgendes:

1. Wenn Sie sich für die Verwendung des integrierten Kerberos-Proxys für die Computer Authentifizierung entschieden haben, wenn Sie den einzelnen RAS-Server einrichten, müssen Sie die Einstellung so ändern, dass die von einer internen Zertifizierungsstelle ausgestellten Computer Zertifikate verwendet werden, da der Kerberos-Proxy für einen multistandort nicht unterstützt wird. Nutzung.
2. Wenn Sie ein selbst signiertes Zertifikat verwendet haben, müssen Sie die Bereitstellung auf einem einzelnen Server so konfigurieren, dass ein von einer internen Zertifizierungsstelle ausgestelltes Zertifikat verwendet wird.
3. Damit die IPSec-Authentifizierung während der Client Authentifizierung erfolgreich ist, müssen alle RAS-Server über ein Zertifikat verfügen, das von der IPSec-Stamm-oder zwischen Zertifizierungsstelle ausgestellt wurde, und mit der Clientauthentifizierungs-OID für die erweiterte Schlüssel Verwendung.
4. Auf allen RAS-Servern in der Bereitstellung für mehrere Standorte muss dasselbe IPSec-Stamm Zertifikat oder zwischen Zertifikat installiert sein.

### 3,4 Planen des Lasten Ausgleichs für globale Server

In einer Bereitstellung mit mehreren Standorten können Sie zusätzlich einen globalen Lastenausgleich für den Server konfigurieren. Ein Global Server Load Balancer kann für Ihre Organisation nützlich sein, wenn die Bereitstellung eine große geografische Verteilung abdeckt, da er die Auslastung des Datenverkehrs zwischen den Einstiegspunkten verteilen kann. Der Lastenausgleich des globalen Servers kann so konfiguriert werden, dass DirectAccess-Clients die Einstiegspunkt Informationen des nächstgelegenen Einstiegs Punkts bereitgestellt werden. Der Prozess funktioniert wie folgt:

1. Client Computer, auf denen Windows 10 oder Windows 8 ausgeführt wird, verfügen über eine Liste der IP-Adressen des globalen Server Load Balancers, die jeweils einem Einstiegspunkt zugeordnet sind.
2. Der Windows 10-oder Windows 8-Client Computer versucht, den FQDN des Load Balancers des globalen Servers im öffentlichen DNS in eine IP-Adresse aufzulösen. Wenn die aufgelöste IP-Adresse als IP-Adresse für den Lastenausgleich des globalen Servers eines Einstiegs Punkts aufgeführt ist, wählt der Client Computer automatisch diesen Einstiegspunkt aus und stellt eine Verbindung mit der IP-HTTPS-URL (ConnectTo-Adresse) oder der zugehörigen Teredo-Server-IP-Adresse her. Beachten Sie, dass die IP-Adresse des Load Balancers des globalen Servers nicht mit der ConnectTo-Adresse oder der Teredo-Server Adresse des Einstiegs Punkts identisch sein muss, da die Client Computer nie versuchen, eine Verbindung mit der IP-Adresse des globalen Server-Lasten Ausgleichs Moduls herzustellen.
3. Wenn sich der Client Computer hinter einem WebProxy befindet (und keine DNS-Auflösung verwenden kann), oder wenn der FQDN des globalen Server Lastenausgleichs-FQDN nicht in eine konfigurierte IP-Adresse für den Lastenausgleich des globalen Servers aufgelöst wird, wird automatisch ein Einstiegspunkt mit einem HTTPS-Test ausgewählt. die IP-HTTPS-URLs aller Einstiegspunkte. Der Client stellt eine Verbindung mit dem Server her, der zuerst antwortet.

Eine Liste der Global Server Load Balancing-Geräte, die den Remote Zugriff unterstützen, finden Sie auf der Seite

## 3,5 Planen der DirectAccess-Client Einstiegspunkt Auswahl

Wenn Sie eine Bereitstellung für mehrere Standorte konfigurieren, werden Windows 10-und Windows 8-Client Computer standardmäßig mit den Informationen konfiguriert, die zum Herstellen einer Verbindung mit allen Einstiegspunkten in der Bereitstellung und zum automatischen Herstellen einer Verbindung mit einem einzelnen Einstiegspunkt basierend auf einer Auswahl erforderlich sind. projiziert. Sie können die Bereitstellung auch so konfigurieren, dass Windows 10-und Windows 8-Client Computer den Einstiegspunkt, mit dem eine Verbindung hergestellt werden soll, manuell auswählen können. Wenn ein Windows 10-oder Windows 8-Client Computer zurzeit mit dem USA Einstiegspunkt verbunden ist und die automatische Auswahl von Einstiegspunkten aktiviert ist, versucht der Client Computer nach einigen Minuten, eine Verbindung herzustellen, wenn der USA Einstiegspunkt nicht erreichbar ist. über den Einstiegspunkt in Europa. Es wird empfohlen, die automatische Auswahl von Einstiegspunkten zu verwenden Wenn Sie jedoch eine manuelle Auswahl von Einstiegspunkten zulassen, können Endbenutzer die Verbindung zu einem anderen Einstiegspunkt basierend auf den aktuellen Netzwerkbedingungen herstellen. Wenn z. b. ein Computer mit dem USA Einstiegspunkt verbunden ist und die Verbindung mit dem internen Netzwerk erheblich langsamer wird als erwartet. In dieser Situation kann der Endbenutzer manuell auswählen, eine Verbindung mit dem Einstiegspunkt in Europa herzustellen, um die Verbindung mit dem internen Netzwerk zu verbessern.

### NOTE

Nachdem ein Endbenutzer einen Einstiegspunkt manuell ausgewählt hat, wird der Client Computer nicht auf die automatische Auswahl des Einstiegs Punkts zurückgesetzt. Das heißt, wenn der manuell ausgewählte Einstiegspunkt nicht mehr erreichbar ist, muss der Endbenutzer entweder die automatische Auswahl der Einstiegspunkte wiederherstellen oder einen anderen Einstiegspunkt manuell auswählen.

Windows 7-Client Computer werden mit den Informationen konfiguriert, die zum Herstellen einer Verbindung mit einem einzelnen Einstiegspunkt in der Bereitstellung für mehrere Standorte erforderlich sind. Sie können die Informationen für mehrere Einstiegspunkte nicht gleichzeitig speichern. Beispielsweise kann ein Windows 7-Client Computer so konfiguriert werden, dass er eine Verbindung mit dem USA Einstiegspunkt herstellt, nicht jedoch mit dem Einstiegspunkt in Europa. Wenn der USA Einstiegspunkt nicht erreichbar ist, verliert der Windows 7-Client Computer die Konnektivität zum internen Netzwerk, bis der Einstiegspunkt erreichbar ist. Der Endbenutzer kann keine Änderungen vornehmen, um zu versuchen, eine Verbindung mit dem Einstiegspunkt in Europa herzustellen.

## 3,6 Planen von Präfixen und Routing

### Internes IPv6-Präfix

Beim Bereitstellen des einzelnen RAS-Servers haben Sie die internen IPv6-Präfixe für das Netzwerk in einer Bereitstellung mit mehreren Standorten festgestellt:

1. Wenn Sie alle Ihre Active Directory Websites bei der Konfiguration der Bereitstellung für den Remote Zugriff mit einem Server eingefügt haben, werden in der Remote Zugriffs-Verwaltungskonsole bereits die IPv6-Präfixe für das interne Netzwerk definiert.
2. Wenn Sie zusätzliche Active Directory Standorte für die Bereitstellung mit mehreren Standorten erstellen, müssen Sie neue IPv6-Präfixe für die zusätzlichen Standorte planen und diese im Remote Zugriff definieren. Beachten Sie, dass IPv6-Präfixe nur mithilfe der Remote Zugriffs-Verwaltungskonsole oder mithilfe von PowerShell-Cmdlets konfiguriert werden können, wenn IPv6 im internen Unternehmensnetzwerk bereitgestellt wird.

### IPv6-Präfix für DirectAccess-Client Computer (IP-HTTPS-Präfix)

1. Wenn IPv6 im internen Unternehmensnetzwerk bereitgestellt wird, müssen Sie ein IPv6-Präfix planen, das

DirectAccess-Client Computern an zusätzlichen Einstiegspunkten in der Bereitstellung zugewiesen werden soll.

2. Stellen Sie sicher, dass die IPv6-Präfixe, die den DirectAccess-Client Computern in den einzelnen Einstiegspunkten zugewiesen werden, unterschiedlich sind und dass sich die IPv6-Präfixe nicht überlappen.
3. Wenn IPv6 nicht im Unternehmensnetzwerk bereitgestellt wird, wird beim Hinzufügen des Einstiegs Punkts automatisch ein IP-HTTPS-Präfix für jeden Einstiegspunkt ausgewählt.

### **IPv6-Präfix für VPN-Clients**

Wenn Sie VPN auf dem einzelnen RAS-Server bereitgestellt haben, beachten Sie Folgendes:

1. Das Hinzufügen eines IPv6-VPN-Präfixes zu einem Einstiegspunkt ist nur erforderlich, wenn Sie eine IPv6-Verbindung zwischen VPN-Client und dem Unternehmensnetzwerk zulassen möchten.
2. Das VPN-Präfix kann nur mithilfe der Remote Zugriffs-Verwaltungskonsole oder des PowerShell-Cmdlets für einen Einstiegspunkt konfiguriert werden, wenn IPv6 im internen Unternehmensnetzwerk bereitgestellt wird und VPN auf dem Einstiegspunkt aktiviert ist.
3. Das VPN-Präfix sollte in jedem Einstiegspunkt eindeutig sein und darf sich nicht mit anderen VPN-oder IP-HTTPS-Präfixen überschneiden.
4. Wenn IPv6 nicht im Unternehmensnetzwerk bereitgestellt wird, wird den VPN-Clients, die eine Verbindung mit dem Einstiegspunkt herstellen, keine IPv6-Adresse zugewiesen.

### **Routing**

Bei einer Bereitstellung mit mehreren Standorten wird das symmetrische Routing mithilfe von Teredo und IP-HTTPS erzwungen. Beachten Sie Folgendes, wenn IPv6 im Unternehmensnetzwerk bereitgestellt wird:

1. Die Teredo-und IP-HTTPS-Präfixe der einzelnen Einstiegspunkte müssen über das Unternehmensnetzwerk an den zugehörigen RAS-Server Routing fähig sein.
2. Die Routen müssen in der Routing Infrastruktur des Unternehmensnetzwerks konfiguriert werden.
3. Für jeden Einstiegspunkt sollten eine bis drei Routen im internen Netzwerk vorhanden sein:
  - a. IP-HTTPS-Präfix: dieses Präfix wird vom Administrator im Assistenten zum Hinzufügen von Einstiegspunkten ausgewählt.
  - b. VPN-IPv6-Präfix (optional). Dieses Präfix kann nach dem Aktivieren von VPN für einen Einstiegspunkt ausgewählt werden.
  - c. Teredo-Präfix (optional). Dieses Präfix ist nur relevant, wenn der RAS-Server mit zwei aufeinander folgenden öffentlichen IPv4-Adressen auf dem externen Adapter konfiguriert ist. Das Präfix basiert auf der ersten öffentlichen IPv4-Adresse des Adress Paars. Angenommen, die externen Adressen lauten wie folgt:
    - a. www.xxx.yyy.zzz
    - b. www.xxx.yyy.zzz + 1

Dann ist das zu konfigurierende Teredo-Präfix 2001:0:WWXX:YYZZ::/64, wobei WWXX: YYZZ die hexadezimale Darstellung der IPv4-Adresse www.xxx.yyy.zzz ist.

Beachten Sie, dass Sie das folgende Skript verwenden können, um das Teredo-Präfix zu berechnen:

```

$TeredoIPv4 = (Get-NetTeredoConfiguration).ServerName # Use for a Remote Access server that is
already configured
$TeredoIPv4 = "20.0.0.1" # Use for an IPv4 address

[Byte[]] $TeredoServerAddressBytes = `

[System.Net.IPAddress]::Parse("2001::").GetAddressBytes()[0..3] + `

[System.Net.IPAddress]::Parse($TeredoIPv4).GetAddressBytes() + `

[System.Net.IPAddress]::Parse("::").GetAddressBytes()[0..7]

Write-Host "The server's Teredo prefix is $([System.Net IPAddress]$TeredoServerAddressBytes)/64"

```

- d. Alle oben genannten Routen müssen an die IPv6-Adresse des internen Adapters des Remote Zugriffs Servers (oder an die interne virtuelle IP-Adresse (VIP) für einen Einstiegspunkt mit Lastenausgleich weitergeleitet werden.

#### **NOTE**

Wenn IPv6 im Unternehmensnetzwerk bereitgestellt wird und die RAS-Server-Verwaltung Remote über DirectAccess ausgeführt wird, müssen jedem RAS-Server Routen für die Teredo-und IP-HTTPS-Präfixe aller anderen Einstiegspunkte hinzugefügt werden, damit der Datenverkehr wird an das interne Netzwerk weitergeleitet.

#### **Active Directory standortspezifische IPv6-Präfixe**

Wenn ein Client Computer, auf dem Windows 10 oder Windows 8 ausgeführt wird, mit einem Einstiegspunkt verbunden ist, wird der Client Computer sofort dem Active Directory-Standort des Einstiegs Punkts zugeordnet und mit IPv6-Präfixen konfiguriert, die dem Einstiegspunkt zugeordnet sind. Für Client Computer wird die Verbindung mit Ressourcen mithilfe dieser IPv6-Präfixe bevorzugt, da Sie dynamisch in der IPv6-Präfix Richtlinien Tabelle mit höherer Priorität konfiguriert werden, wenn eine Verbindung mit einem Einstiegspunkt hergestellt wird.

Wenn in Ihrer Organisation eine Active Directory Topologie mit standortspezifischen IPv6-Präfixen verwendet wird (z. b. wird ein interner Ressourcen-voll qualifizierten Namen app.Corp.com sowohl in Nordamerika als auch in Europa mit einer standortspezifischen IP-Adresse an jedem Standort gehostet), wird dies nicht konfiguriert. der Standardwert ist die Remote Zugriffs Konsole, und die standortspezifischen IPv6-Präfixe sind für jeden Einstiegspunkt nicht konfiguriert. Wenn Sie dieses optionale Szenario aktivieren möchten, müssen Sie jeden Einstiegspunkt mit den spezifischen IPv6-Präfixen konfigurieren, die von Client Computern bevorzugt werden, die eine Verbindung mit einem bestimmten Einstiegspunkt herstellen. Gehen Sie hierzu wie folgt vor:

1. Führen Sie für jedes GPO, das für Windows 10-oder Windows 8-Client Computer verwendet wird, das PowerShell-Cmdlet Set-daentrypointtableitem aus.
2. Legen Sie den entrypointrange-Parameter für das Cmdlet mit den standortspezifischen IPv6-Präfixen fest. Führen Sie z. b. Folgendes aus, um die standortspezifischen Präfixe 2001: db8:1: 1::/64 und 2001: DB: 1:2::/64 zu einem Einstiegspunkt mit dem Namen "Europa" hinzuzufügen.

```

$entryPointName = "Europe"
$prefixesToAdd = @("2001:db8:1:1::/64", "2001:db8:1:2::/64")
$clientGpos = (Get-DAClient).GpoName
$clientGpos | % { Get-DAEntryPointTableItem -EntryPointName $entryPointName -PolicyStore $_ | %{ Set-
DAEntryPointTableItem -PolicyStore $_.PolicyStore -EntryPointName $_.EntryPointName -EntryPointRange
($_.EntryPointRange) + $prefixesToAdd}}

```

3. Wenn Sie den entrypointrange-Parameter ändern, stellen Sie sicher, dass Sie die vorhandenen 128-Bit-Präfixe, die zu den IPSec-Tunnel Endpunkten und der DNS64-Adresse gehören, nicht entfernen.

## **3,7 Planen des Übergangs zu IPv6 bei Bereitstellung des Remote**

# Zugriffs für mehrere Standorte

Viele Organisationen verwenden das IPv4-Protokoll im Unternehmensnetzwerk. Mit der Erschöpfung verfügbarer IPv4-Präfixe nehmen viele Organisationen den Übergang von IPv4 ausschließlich zu reinen IPv6-Netzwerken vor.

Diese Umstellung wird am ehesten in zwei Phasen durchgeführt:

1. Von einer reinen IPv4-zu einem IPv6-und IPv4-Unternehmensnetzwerk.
2. Von IPv6 + IPv4 zu einem reinen IPv6-Unternehmensnetzwerk.

In jedem Teil kann der Übergang in Phasen ausgeführt werden. In jeder Phase kann nur ein Subnetz des Netzwerks in die neue Netzwerkkonfiguration geändert werden. Daher ist eine DirectAccess-Bereitstellung mit mehreren Standorten erforderlich, um eine Hybrid Bereitstellung zu unterstützen, bei der beispielsweise einige Einstiegspunkte zu einem reinen IPv4-Subnetz gehören und andere zu einem IPv6-und IPv4-Subnetz gehören. Außerdem dürfen Konfigurationsänderungen während der Übergangsprozesse die Client Konnektivität über DirectAccess nicht unterbrechen.

## Übergang von einer reinen IPv4-zu einem IPv6-und IPv4-Unternehmensnetzwerk

Beim Hinzufügen von IPv6-Adressen zu einem reinen IPv4-Unternehmensnetzwerk können Sie einem bereits bereitgestellten DirectAccess-Server eine IPv6-Adresse hinzufügen. Außerdem empfiehlt es sich, einen Einstiegspunkt oder Knoten einem Cluster mit Lastenausgleich mit IPv4-und IPv6-Adressen für die DirectAccess-Bereitstellung hinzuzufügen.

Der Remote Zugriff ermöglicht Ihnen das Hinzufügen von Servern mit IPv4-und IPv6-Adressen zu einer Bereitstellung, die ursprünglich ausschließlich mit IPv4-Adressen konfiguriert wurde. Diese Server werden als reine IPv4-Server hinzugefügt, und ihre IPv6-Adressen werden von DirectAccess ignoriert. Folglich kann Ihre Organisation die Vorteile der systemeigenen IPv6-Konnektivität auf diesen neuen Servern nicht nutzen.

Um die Bereitstellung in eine IPv6-und IPv4-Bereitstellung umzuwandeln und die systemeigenen IPv6-Funktionen zu nutzen, müssen Sie DirectAccess neu installieren. Informationen zur Aufrechterhaltung der Client Konnektivität während der erneuten Installation finden Sie unter Übergang von einer reinen IPv4-Bereitstellung zu einer reinen IPv6-Bereitstellung mithilfe von Dual DirectAccess-bereit Stellungen.

### NOTE

Wie bei einem reinen IPv4-Netzwerk muss die Adresse des DNS-Servers, der zum Auflösen von Client-DNS-Anforderungen verwendet wird, mit der DNS64 konfiguriert werden, die auf RAS-Servern selbst und nicht mit einem Unternehmens-DNS bereitgestellt wird.

## Übergang von IPv6 und IPv4 zu einem reinen IPv6-Unternehmensnetzwerk

DirectAccess ermöglicht das Hinzufügen von nur-IPv6-Einstiegspunkten, wenn der erste RAS-Server in der Bereitstellung ursprünglich entweder IPv4-und IPv6-Adressen oder nur eine IPv6-Adresse enthielt. Das heißt, Sie können in einem einzigen Schritt nicht von einem reinen IPv4-Netzwerk zu einem reinen IPv6-Netzwerk wechseln, ohne DirectAccess erneut zu installieren. Informationen zum direkten Übergang von einem reinen IPv4-Netzwerk zu einem reinen IPv6-Netzwerk finden Sie unter Übergang von einer reinen IPv4-Bereitstellung zu einer reinen IPv6-Bereitstellung mithilfe von Dual DirectAccess-bereit Stellungen.

Nachdem Sie den Übergang von einer reinen IPv4-Bereitstellung zu einer IPv6-und IPv4-Bereitstellung abgeschlossen haben, können Sie zu einem reinen IPv6-Netzwerk wechseln. Beachten Sie während und nach der Umstellung Folgendes:

- Wenn alle IPv4-Back-End-Server im Unternehmensnetzwerk verbleiben, sind Sie für Clients, die über die reinen IPv6-Einstiegspunkte verbunden sind, nicht erreichbar.
- Beim Hinzufügen von reinen IPv6-Einstiegspunkten zu einer IPv4-und IPv6-Bereitstellung werden DNS64

und NAT64 auf den neuen Servern nicht aktiviert. Clients, die eine Verbindung mit diesen Einstiegspunkten herstellen, werden automatisch für die Verwendung der DNS-Server des Unternehmens konfiguriert.

- Wenn Sie IPv4-Adressen von einem bereitgestellten Server löschen müssen, müssen Sie den Server aus der DirectAccess-Bereitstellung entfernen, die zugehörige IPv4-Unternehmensnetzwerk Adresse entfernen und Sie der Bereitstellung wieder hinzufügen.

Zur Unterstützung der Client Konnektivität mit dem Unternehmensnetzwerk müssen Sie sicherstellen, dass der Netzwerkadressen Server durch das Unternehmens-DNS in seine IPv6-Adresse aufgelöst werden kann. Eine zusätzliche IPv4-Adresse kann ebenfalls festgelegt werden, ist jedoch nicht erforderlich.

### **Übergang von einer reinen IPv4-zu einer reinen IPv6-Bereitstellung mithilfe von Dual DirectAccess-bereit Stellungen**

Der Übergang von einem reinen IPv4-zu einem reinen IPv6-Unternehmensnetzwerk kann nicht durchgeführt werden, ohne dass die DirectAccess-Bereitstellung neu installiert wird. Um die Client Konnektivität während des Übergangs aufrechtzuerhalten, können Sie eine andere DirectAccess-Bereitstellung verwenden. Die duale Bereitstellung ist erforderlich, wenn die erste Übergangsphase abgeschlossen ist (nur-IPv4-Netzwerk, das auf IPv4 + IPv6 aktualisiert wurde), und Sie beabsichtigen, sich für einen zukünftigen Übergang zu einem reinen IPv6-Unternehmensnetzwerk zu entscheiden, um die Vorteile der systemeigenen IPv6-Konnektivität zu nutzen. Die duale Bereitstellung wird in den folgenden allgemeinen Schritten beschrieben:

1. Installieren Sie eine zweite DirectAccess-Bereitstellung. Sie können DirectAccess auf neuen Servern installieren oder Server aus der ersten Bereitstellung entfernen und für die zweite Bereitstellung verwenden.

#### **NOTE**

Stellen Sie beim Installieren einer zusätzlichen DirectAccess-Bereitstellung neben einer aktuellen Bereitstellung sicher, dass keine zwei Einstiegspunkte dasselbe Client Präfix verwenden.

Wenn Sie DirectAccess mithilfe des Assistenten für erste Schritte oder mit dem-Cmdlet `Install-RemoteAccess` installieren, legt der Remote Zugriff das Client Präfix des ersten Einstiegs Punkts in der Bereitstellung automatisch auf einen Standardwert < IPv6-Subnetz\_Präfix >: 1000::/64 fest. Bei Bedarf müssen Sie das Präfix ändern.

2. Entfernen Sie die ausgewählten Client Sicherheitsgruppen aus der ersten Bereitstellung.
3. Fügen Sie die Client Sicherheitsgruppen der zweiten Bereitstellung hinzu.

#### **IMPORTANT**

Um die Client Konnektivität während des gesamten Vorgangs aufrechtzuerhalten, müssen Sie die Sicherheitsgruppen der zweiten Bereitstellung sofort nach dem Entfernen aus der ersten Bereitstellung hinzufügen. Dadurch wird sichergestellt, dass Clients nicht mit zwei oder NULL DirectAccess-GPOs aktualisiert werden. Nachdem Sie das Client-Gruppenrichtlinien Objekt abgerufen und aktualisiert haben, wird die zweite Bereitstellung von den Clients verwendet.

4. Optional: Entfernen Sie die DirectAccess-Einstiegspunkte aus der ersten Bereitstellung, und fügen Sie diese Server als neue Einstiegspunkte in der zweiten Bereitstellung hinzu.

Wenn Sie den Übergang abgeschlossen haben, können Sie die erste DirectAccess-Bereitstellung deinstallieren. Beim Deinstallieren von können die folgenden Probleme auftreten:

- Wenn die Bereitstellung so konfiguriert wurde, dass nur Clients auf mobilen Computern unterstützt werden, wird der WMI-Filter gelöscht. Wenn die Client Sicherheitsgruppen der zweiten Bereitstellung Desktop Computer enthalten, werden Desktop Computer vom DirectAccess-Client-Gruppenrichtlinien Objekt nicht gefiltert und möglicherweise Probleme verursacht. Wenn ein Filter für mobile Computer erforderlich ist, erstellen Sie ihn neu, indem Sie die Anweisungen unter [Erstellen von WMI-Filters für das GPO](#)befolgen.

- Wenn beide bereit Stellungen ursprünglich in derselben Active Directory Domäne erstellt wurden, wird der DNS-Test Eintrag, der auf "localhost" verweist, gelöscht und kann zu Problemen mit der Client Konnektivität führen. Beispielsweise können Clients eine Verbindung über IP-HTTPS anstelle von Teredo herstellen oder zwischen DirectAccess-Einstiegspunkten für mehrere Standorte wechseln. In diesem Fall müssen Sie dem Unternehmens-DNS den folgenden DNS-Eintrag hinzufügen:

- Zone: Domänen Name
- Name: DirectAccess-corpconnectivityhost
- IP-Adresse::: 1
- Typ: AAAA

# Konfigurieren einer Bereitstellung mit mehreren Standorten

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 kombiniert DirectAccess-und RAS-VPN (RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle. Diese Übersicht bietet eine Einführung in die Konfigurationsschritte, die erforderlich sind, um eine einzelne Bereitstellung von Windows Server 2016 oder Windows Server 2012 Remote Access für mehrere Standorte bereitzustellen.

- Schritt 1: bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) Installieren und konfigurieren Sie einen einzelnen Remote Zugriffs Server. Die Bereitstellung für mehrere Standorte erfordert, dass Sie einen einzelnen Server installieren, bevor Sie eine Bereitstellung für mehrere Standorte konfigurieren.
- **Schritt 2: Konfigurieren der Infrastruktur für mehrere Standorte** Für eine Bereitstellung mit mehreren Standorten müssen Sie zusätzliche Active Directory Standorte und Domänen Controller konfigurieren. Weitere Sicherheitsgruppen und Gruppenrichtlinie Objekte (GPOs) sind ebenfalls erforderlich, wenn Sie nicht automatisch konfigurierte Gruppenrichtlinien Objekte verwenden.
- **Schritt 3: Konfigurieren der Bereitstellung für mehrere Standorte:** installieren Sie die Remote Zugriffs Rolle auf zusätzlichen Remote Zugriffs Servern, aktivieren Sie die Bereitstellung für mehrere Standorte, und konfigurieren Sie die zusätzlichen Server als Einstiegspunkte für die Bereitstellung.
- **Schritt 4: Überprüfen der Bereitstellung für mehrere Standorte**

# Schritt 1 Implementieren einer einzelnen Server Bereitstellung für den Remote Zugriff

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Konfigurationsschritt zum Bereitstellen des Remote Zugriffs in einer Topologie mit mehreren Standorten ist die Implementierung einer erweiterten Bereitstellung mit einem einzelnen Server und das Hinzufügen von Servern zu jedem Multisite-Einstiegspunkt.

## Implementieren einer Bereitstellung auf einem einzelnen Server

Bevor Sie eine Bereitstellung für mehrere Standorte konfigurieren können, müssen Sie wie unter Bereitstellen eines [einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) beschrieben eine erweiterte Bereitstellung für den Remote Zugriff mit einem Server konfigurieren.

## Siehe auch

- [Schritt 2: Konfigurieren der Infrastruktur für mehrere Standorte](#)

# Schritt 2 Konfigurieren der Infrastruktur für mehrere Standorte

09.04.2020 • 30 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2012 R2, Windows Server 2012

Zum Konfigurieren einer Bereitstellung mit mehreren Standorten sind einige Schritte erforderlich, um die Einstellungen für die Netzwerkinfrastruktur zu ändern. Dazu gehören: Konfigurieren zusätzlicher Active Directory Standorte und Domänen Controller, Konfigurieren zusätzlicher Sicherheitsgruppen und Konfigurieren von Gruppenrichtlinie Objekte (GPOs), wenn Sie keine automatisch konfigurierten GPOs verwenden.

AUFGABE	BESCHREIBUNG
2.1. Zusätzliche Active Directory Standorte konfigurieren	Konfigurieren Sie zusätzliche Active Directory Standorte für die Bereitstellung.
2.2. Zusätzliche Domänen Controller konfigurieren	Konfigurieren Sie zusätzliche Active Directory Domänen Controller nach Bedarf.
2.3. Konfigurieren von Sicherheitsgruppen	Konfigurieren Sie Sicherheitsgruppen für alle Windows 7-Client Computer.
2.4. Konfigurieren der Gruppenrichtlinienobjekte	Konfigurieren Sie zusätzliche Gruppenrichtlinie Objekte nach Bedarf.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## 2.1. Zusätzliche Active Directory Standorte konfigurieren

Alle Einstiegspunkte können sich an einer einzigen Active Directory Site befinden. Daher ist mindestens eine Active Directory Site für die Implementierung von Remote Zugriffs Servern in einer Konfiguration mit mehreren Standorten erforderlich. Verwenden Sie dieses Verfahren, wenn Sie den ersten Active Directory Standort erstellen müssen oder wenn Sie zusätzliche Active Directory Standorte für die Bereitstellung mit mehreren Standorten verwenden möchten. Verwenden Sie das Snap-in Active Directory Sites und Dienste, um neue Standorte im Netzwerk Ihrer Organisation zu erstellen.

Zum Ausführen dieses Verfahrens ist mindestens die Mitgliedschaft in der Gruppe "Organisations- Admins " in der Gesamtstruktur oder in der Gruppe " Domänen-Admins " in der Stamm Domäne der Gesamtstruktur oder einer gleichwertigen Gruppe erforderlich. Ausführliche Informationen zur Verwendung der entsprechenden Konten und Gruppenmitgliedschaften finden Sie unter [lokale und Domänen Standard Gruppen](#).

Weitere Informationen finden Sie unter [Hinzufügen einer Site zur Gesamtstruktur](#).

### So konfigurieren Sie zusätzliche Active Directory Standorte

1. Klicken Sie auf dem primären Domänen Controller auf Start, und klicken Sie dann auf Active Directory Websites und Dienste.

2. Klicken Sie in der Konsole Active Directory Standorte und Dienste in der Konsolen Struktur mit der rechten Maustaste auf **Standorte**, und klicken Sie dann auf **neuer Standort**.
3. Geben Sie im Dialogfeld **Neues Objekt-Standort** im Feld **Name** einen Namen für den neuen Standort ein.
4. Klicken Sie unter **Linkname** auf ein Standort Verknüpfungs Objekt, und klicken Sie dann zweimal auf **OK**.
5. Erweitern Sie in der Konsolen Struktur **Standorte**, klicken Sie mit der rechten Maustaste auf **Subnetze**, und klicken Sie dann auf **Neues Subnetz**.
6. Geben Sie im Dialogfeld **Neues Objekt-Subnetz** unter **Präfix** das IPv4-oder IPv6-Subnetzpräfix ein, klicken Sie in der Liste **Wählen Sie ein Standort Objekt für dieses Präfix aus** auf die Site, die diesem Subnetz zugeordnet werden soll, und klicken Sie dann auf **OK**.
7. Wiederholen Sie die Schritte 5 und 6, bis Sie alle Subnetze erstellt haben, die für die Bereitstellung erforderlich sind.
8. Schließen Sie Active Directory Websites und Dienste.

#### *Befehle in Windows PowerShell*

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

So installieren Sie die Windows-Funktion "Active Directory-Modul für Windows PowerShell":

```
Install-WindowsFeature "Name RSAT-AD-PowerShell"
```

oder fügen Sie das "Active Directory PowerShell-Snap-in" über OptionalFeatures hinzu.

Wenn Sie die folgenden Cmdlets unter Windows 7 oder Windows Server 2008 R2 ausführen, muss das Active Directory PowerShell-Modul importiert werden:

```
Import-Module ActiveDirectory
```

So konfigurieren Sie eine Active Directory Site mit dem Namen "Second-Site" unter Verwendung der integrierten DEFAULTIPSITELINK:

```
New-ADReplicationSite -Name "Second-Site"
Set-ADReplicationSiteLink -Identity "DEFAULTIPSITELINK" -sitesIncluded @{Add="Second-Site"}
```

So konfigurieren Sie IPv4-und IPv6-Subnetze für den zweiten Standort:

```
New-ADReplicationSubnet -Name "10.2.0.0/24" -Site "Second-Site"
New-ADReplicationSubnet -Name "2001:db8:2::/64" -Site "Second-Site"
```

## 2.2. Zusätzliche Domänen Controller konfigurieren

Zum Konfigurieren einer Bereitstellung mit mehreren Standorten in einer einzelnen Domäne empfiehlt es sich, mindestens einen beschreibbaren Domänen Controller für jeden Standort in der Bereitstellung zu haben.

Um dieses Verfahren auszuführen, müssen Sie mindestens Mitglied der Gruppe "Domänen-Admins" in der Domäne sein, in der der Domänen Controller installiert wird.

Weitere Informationen finden Sie unter [Installieren eines zusätzlichen Domänen Controllers](#).

### So konfigurieren Sie zusätzliche Domänen Controller

1. Klicken Sie auf dem Server, der als Domänen Controller fungieren soll, in **Server-Manager** auf dem **Dashboard** auf **Rollen und Features hinzufügen**.
2. Klicken Sie dreimal auf **weiter**, um zum Bildschirm für die Server Rollenauswahl zu gelangen.
3. Wählen Sie auf der Seite **Server Rollen auswählen** die Option **Active Directory Domain Services** aus. Klicken Sie bei entsprechender Aufforderung auf **Features hinzufügen**, und klicken Sie dann dreimal auf **weiter**.
4. Klicken Sie auf der Seite **Bestätigung** auf **Installieren**.
5. Wenn die Installation erfolgreich abgeschlossen wurde, klicken Sie auf **Server zu einem Domänen Controller** herauf Stufen.
6. Klicken Sie im Konfigurations-Assistenten für Active Directory Domain Services auf der Seite **Bereitstellungs Konfiguration** auf **Domänen Controller einer vorhandenen Domäne hinzufügen**.
7. Geben Sie unter **Domänen** Domänen Namen ein. beispielsweise Corp.contoso.com.
8. Klicken Sie unter **Geben Sie die Anmelde Informationen an, um diesen Vorgang auszuführen, auf ändern**. Geben Sie im Dialogfeld **Windows-Sicherheit** den Benutzernamen und das Kennwort für ein Konto an, mit dem der zusätzliche Domänen Controller installiert werden kann. Zum Installieren eines zusätzlichen Domänencontrollers müssen Sie ein Mitglied der Gruppe Organisations-Admins oder Domänen-Admins sein. Klicken Sie nach Eingabe der Anmeldeinformationen auf **Weiter**.
9. Gehen Sie auf der Seite **Domänen Controller Optionen** wie folgt vor:

- a. Nehmen Sie folgende Auswahl vor:

- **Domain Name System (DNS)-Server**: diese Option ist standardmäßig ausgewählt, sodass der Domänen Controller als Domain Name System Server (DNS) fungieren kann. Falls der Domänencontroller nicht als DNS-Server verwendet werden soll, können Sie diese Option deaktivieren.

Wenn die DNS-Server Rolle nicht auf dem PDC-Emulator (primärer Domänen Controller) in der Stamm Domäne der Gesamtstruktur installiert ist, ist die Option zum Installieren des DNS-Servers auf einem zusätzlichen Domänen Controller nicht verfügbar. Um dieses Problem zu umgehen, können Sie die DNS-Server Rolle vor oder nach der AD DS Installation installieren.

#### NOTE

Wenn Sie die Option zum Installieren des DNS-Servers auswählen, erhalten Sie möglicherweise eine Meldung mit dem Hinweis, dass keine DNS-Delegierung für den DNS-Server erstellt werden konnte und dass Sie manuell eine DNS-Delegierung an den DNS-Server erstellen sollten, um eine zuverlässige Namensauflösung sicherzustellen. Wenn Sie einen zusätzlichen Domänen Controller in der Stamm Domäne der Gesamtstruktur oder in einer Struktur Stamm Domäne installieren, müssen Sie keine DNS-Delegierung erstellen. Klicken Sie in diesem Fall auf **Ja**, und ignorieren Sie die Meldung.

- **Globaler Katalog (GC)** : diese Option ist standardmäßig ausgewählt. Damit werden dem Domänencontroller die schreibgeschützten Verzeichnispartitionen des globalen Katalogs hinzugefügt. Außerdem wird die Suchfunktion für den globalen Katalog aktiviert.
- **Schreib geschützter Domänen Controller (RODC)** : diese Option ist standardmäßig nicht

ausgewählt. Der zusätzliche Domänen Controller ist schreibgeschützt. Das heißt, der Domänen Controller wird zu einem RODC.

- b. Wählen Sie unter **Website Name** einen Standort aus der Liste aus.
  - c. Geben Sie unter **Kennwort** und **Kennwort bestätigen** ein Kennwort für den **Verzeichnisdienst-Wiederherstellungs Modus (Directory Services Restore Mode, DSRM)** ein, und klicken Sie dann auf **weiter**. Dieses Kennwort muss verwendet werden, um AD DS in DSRM für Aufgaben zu starten, die offline ausgeführt werden müssen.
10. Aktivieren Sie auf der Seite **DNS-Optionen** das Kontrollkästchen **DNS-Delegierung aktualisieren**, wenn Sie die DNS-Delegierung während der Rollen Installation aktualisieren möchten, und klicken Sie dann auf **weiter**.
11. Geben Sie auf der Seite **zusätzliche Optionen** die Volumes und Ordner Orte für die Datenbankdatei, die Verzeichnisdienst-Protokolldateien und die Dateien des System Volume (SYSVOL) ein, oder navigieren Sie zu diesen. Geben Sie gegebenenfalls Replikations Optionen an, und klicken Sie dann auf **weiter**.
12. Überprüfen Sie die Installationsoptionen auf der Seite **Optionen prüfen**, und klicken Sie dann auf **weiter**.
13. Klicken Sie nach der Überprüfung der Voraussetzungen auf der Seite **Voraussetzungs Prüfung** auf **Installieren**.
14. Warten Sie, bis der Assistent die Konfiguration abgeschlossen hat, und klicken Sie dann auf **Schließen**.
15. Starten Sie den Computer neu, wenn er nicht automatisch neu gestartet wurde.

## 2.3. Konfigurieren von Sicherheitsgruppen

Für eine Bereitstellung mit mehreren Standorten ist eine zusätzliche Sicherheitsgruppe für Windows 7-Client Computer für jeden Einstiegspunkt in der Bereitstellung erforderlich, der den Zugriff auf Windows 7-Client Computer ermöglicht. Wenn mehrere Domänen mit Windows 7-Client Computern vorhanden sind, empfiehlt es sich, in jeder Domäne eine Sicherheitsgruppe für denselben Einstiegspunkt zu erstellen. Alternativ kann eine universelle Sicherheitsgruppe verwendet werden, die die Client Computer aus beiden Domänen enthält. Wenn Sie in einer Umgebung mit zwei Domänen z. b. den Zugriff auf Windows 7-Client Computer in den Einstiegspunkten 1 und 3 zulassen möchten, aber nicht auf Einstiegspunkt 2, dann erstellen Sie zwei neue Sicherheitsgruppen, die die Windows 7-Client Computer für jeden Einstiegspunkt in jedem der Gebiete.

### So konfigurieren Sie zusätzliche Sicherheitsgruppen

1. Klicken Sie auf dem primären Domänen Controller auf **Start**, und klicken Sie dann auf **Active Directory Benutzer und Computer**.
2. Klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf den Ordner, in dem Sie eine neue Gruppe hinzufügen möchten, z. b. Corp.contoso.com/users. Zeigen Sie auf **Neu**, und klicken Sie dann auf **Gruppe**.
3. Geben Sie im Dialogfeld **Neues Objekt-Gruppe** unter **Gruppenname** den Namen der neuen Gruppe ein, z. b. Win7\_Clients\_EntryPoint1.
4. Klicken Sie unter **Gruppenbereich** auf **universell**, klicken Sie unter **Gruppentyp** auf **Sicherheit**, und klicken Sie dann auf **OK**.
5. Wenn Sie der neuen Sicherheitsgruppe Computer hinzufügen möchten, doppelklicken Sie auf die Sicherheitsgruppe, und klicken Sie im Dialogfeld **Eigenschaften von < Group\_Name >** auf die Registerkarte **Mitglieder**.
6. Auf der Registerkarte **Mitglieder** klicken Sie auf **Hinzufügen**.
7. Wählen Sie die Windows 7-Computer aus, die dieser Sicherheitsgruppe hinzugefügt werden sollen, und

klicken Sie auf OK.

8. Wiederholen Sie dieses Verfahren, um eine Sicherheitsgruppe für jeden Einstiegspunkt nach Bedarf zu erstellen.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

So installieren Sie die Windows-Funktion "Active Directory-Modul für Windows PowerShell":

```
Install-WindowsFeature "Name RSAT-AD-PowerShell
```

oder fügen Sie das "Active Directory PowerShell-Snap-in" über OptionalFeatures hinzu.

Wenn Sie die folgenden Cmdlets unter Windows 7 oder Windows Server 2008 R2 ausführen, muss das Active Directory PowerShell-Modul importiert werden:

```
Import-Module ActiveDirectory
```

So konfigurieren Sie eine Sicherheitsgruppe mit dem Namen Win7\_Clients\_EntryPoint1 und zum Hinzufügen eines Client Computers mit dem Namen CLIENT2:

```
New-ADGroup -GroupScope universal -Name Win7_Clients_EntryPoint1  
Add-ADGroupMember -Identity Win7_Clients_EntryPoint1 -Members CLIENT2$
```

## 2.4. Konfigurieren der Gruppenrichtlinienobjekte

Für eine Remote Zugriffs Bereitstellung mit mehreren Standorten sind die folgenden Gruppenrichtlinie Objekte erforderlich:

- Ein Gruppenrichtlinien Objekt für jeden Einstiegspunkt für den Remote Zugriffs Server.
- Ein GPO für alle Windows 8-Client Computer für jede Domäne.
- Ein GPO in jeder Domäne, die Windows 7-Client Computer für jeden Einstiegspunkt enthält, der für die Unterstützung von Windows 7-Clients konfiguriert ist.

#### **NOTE**

Wenn Sie über keine Windows 7-Client Computer verfügen, müssen Sie keine Gruppenrichtlinien Objekte für Windows 7-Computer erstellen.

Wenn Sie den Remote Zugriff konfigurieren, erstellt der Assistent automatisch die erforderlichen Gruppenrichtlinie Objekte, wenn Sie nicht bereits vorhanden sind. Wenn Sie nicht über die erforderlichen Berechtigungen zum Erstellen von Gruppenrichtlinie Objekten verfügen, müssen Sie vor dem Konfigurieren des Remote Zugriffs erstellt werden. Der DirectAccess-Administrator muss über vollständige Berechtigungen für die Gruppenrichtlinien Objekte verfügen (Bearbeiten und Ändern von Sicherheit + löschen).

## **IMPORTANT**

Nachdem Sie die Gruppenrichtlinien Objekte für den Remote Zugriff manuell erstellt haben, müssen Sie dem Domänen Controller am Active Directory Standort, der dem RAS-Server zugeordnet ist, ausreichend Zeit für die Active Directory- und DFS-Replikation gewähren. Wenn der Remote Zugriff die Gruppenrichtlinie Objekte automatisch erstellt hat, ist keine Wartezeit erforderlich.

Informationen zum Erstellen von Gruppenrichtlinie Objekten finden Sie unter [Erstellen und Bearbeiten eines Gruppenrichtlinie Objekts](#).

## **Wartung und Ausfall von Domänen Controllern**

Wenn ein Domänen Controller, auf dem der PDC-Emulator ausgeführt wird, oder Domänen Controller, die Server-Gruppenrichtlinien Objekte verwalten, Ausfallzeiten auftreten, ist es nicht möglich, die Konfiguration des Remote Zugriffs zu laden. Dies hat keine Auswirkung auf die Client Konnektivität, wenn andere Domänen Controller verfügbar sind.

Wenn Sie die Remote Zugriffs Konfiguration laden oder ändern möchten, können Sie die PDC-Emulatorrolle auf einen anderen Domänen Controller für den Client oder die Anwendungsserver-Gruppenrichtlinien Objekte übertragen. Ändern Sie für Server-Gruppenrichtlinien Objekte die Domänen Controller, die die Server-Gruppenrichtlinien Objekte verwalten.

## **IMPORTANT**

Dieser Vorgang kann nur von einem Domänen Administrator ausgeführt werden. Die Auswirkungen der Änderung des primären Domänen Controllers sind nicht auf den Remote Zugriff beschränkt. Verwenden Sie daher beim Übertragen der PDC-Emulatorrolle Vorsicht.

## **NOTE**

Vergewissern Sie sich vor dem Ändern der Domänen Controller Zuordnung, dass alle GPOs in der Remote Zugriffs Bereitstellung auf allen Domänen Controllern in der Domäne repliziert wurden. Wenn das Gruppenrichtlinien Objekt nicht synchronisiert ist, können nach dem Ändern der Domänen Controller Zuordnung die aktuellen Konfigurationsänderungen verloren gehen. Dies kann zu einer beschädigten Konfiguration führen. Informationen zum Überprüfen der Gruppenrichtlinien Objekt-Synchronisierung finden [Sie unter Überprüfen des Gruppenrichtlinie](#)

## **So übertragen Sie die PDC-Emulatorrolle**

1. Geben Sie auf dem **Start** Bildschirm DSA. **msc**, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie im linken Bereich der Konsole Active Directory Benutzer und Computer mit der rechten Maustaste auf **Active Directory Benutzer und Computer**, und klicken Sie dann auf **Domänen Controller ändern**. Klicken Sie im Dialogfeld Verzeichnis Server ändern auf **diesen Domänen Controller oder AD LDS Instanz**, klicken Sie in der Liste auf den Domänen Controller, der als neuer Rollen Inhaber verwendet werden soll, und klicken Sie dann auf **OK**.

## **NOTE**

Sie müssen diesen Schritt ausführen, wenn Sie sich nicht auf dem Domänen Controller befinden, an den Sie die Rolle übertragen möchten. Führen Sie diesen Schritt nicht aus, wenn Sie bereits eine Verbindung mit dem Domänen Controller hergestellt haben, an den Sie die Rolle übertragen möchten.

3. Klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf **Active Directory Benutzer und Computer**, zeigen Sie auf **Alle Tasks**, und klicken Sie dann auf **Betriebs Master**.

4. Klicken Sie im Dialogfeld Betriebs Master auf die Registerkarte **PDC**, und klicken Sie dann auf **ändern**.

5. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie die Rolle übertragen möchten, und klicken Sie dann auf **Schließen**.

#### So ändern Sie den Domänen Controller, der Server-GPOs verwaltet

- Führen Sie das Windows PowerShell-Cmdlet [Set-Daentrypointdc](#) auf dem Remote Zugriffs Server aus, und geben Sie den nicht erreichbaren Domänen Controller Namen für den *existingdc*-Parameter an. Mit diesem Befehl wird die Domänen Controller Zuordnung für die Server-Gruppenrichtlinien Objekte der Einstiegspunkte geändert, die derzeit von diesem Domänen Controller verwaltet werden.
  - Gehen Sie folgendermaßen vor, um den nicht erreichbaren Domänen Controller "DC1.Corp.contoso.com" durch den Domänen Controller "DC2.Corp.contoso.com" zu ersetzen:

```
Set-DAEntryPointDC "ExistingDC 'dc1.corp.contoso.com' "NewDC 'dc2.corp.contoso.com' "ErrorAction Inquire
```

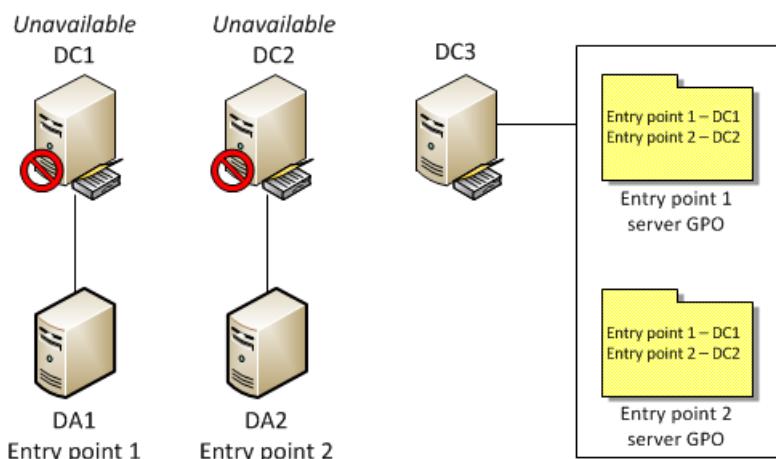
- Führen Sie die folgenden Schritte aus, um den nicht erreichbaren Domänen Controller "DC1.Corp.contoso.com" durch einen Domänen Controller am nächstgelegenen Active Directory Standort zum RAS-Server "da1.Corp.contoso.com" zu ersetzen:

```
Set-DAEntryPointDC "ExistingDC 'dc1.corp.contoso.com' "ComputerName 'DA1.corp.contoso.com' "ErrorAction Inquire
```

#### Ändern von mindestens zwei Domänen Controllern, die Server-Gruppenrichtlinien Objekte verwalten

In einer minimalen Anzahl von Fällen sind mindestens zwei Domänen Controller, die Server-Gruppenrichtlinien Objekte verwalten, nicht verfügbar. Wenn dies auftritt, sind weitere Schritte erforderlich, um die Domänen Controller Zuordnung für die Server-Gruppenrichtlinien Objekte zu ändern.

Domänen Controller-Zuordnungs Informationen werden sowohl in der Registrierung der RAS-Server als auch in allen Server-GPOs gespeichert. Im folgenden Beispiel gibt es zwei Einstiegspunkte mit zwei Remote Zugriffs Servern: "da1" in "Entry Point 1" und "da2" in "Entry Point 2". Das Server-GPO von "Einstiegspunkt 1" wird auf dem Domänen Controller "DC1" verwaltet, während das Server-Gruppenrichtlinien Objekt "Einstiegspunkt 2" auf dem Domänen Controller "DC2" verwaltet wird. "DC1" und "DC2" sind nicht verfügbar. Ein Dritter Domänen Controller ist weiterhin in der Domäne "DC3" verfügbar, und die Daten von "DC1" und "DC2" wurden bereits in "DC3" repliziert.



#### So ändern Sie mindestens zwei Domänen Controller, die Server-Gruppenrichtlinien Objekte verwalten

- Führen Sie den folgenden Befehl aus, um den nicht verfügbaren Domänen Controller "DC2" durch den Domänen Controller "DC3" zu ersetzen:

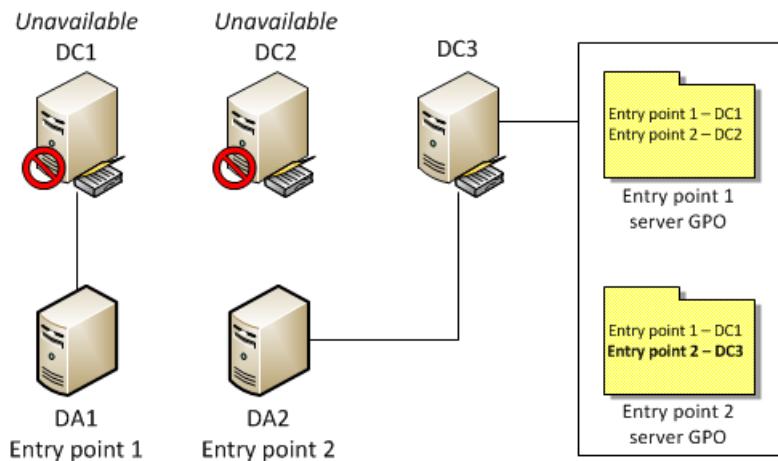
```
Set-DAEntryPointDC "ExistingDC 'DC2' "NewDC 'DC3' "ComputerName 'DA2' "ErrorAction Continue
```

Mit diesem Befehl wird die Domänen Controller Zuordnung für das Server-Gruppenrichtlinien Objekt "Entry Point 2" in der Registrierung von da2 und im Server-Gruppenrichtlinien Objekt "Entry Point 2" aktualisiert. Allerdings wird das Server-Gruppenrichtlinien Objekt "Einstiegspunkt 1" nicht aktualisiert, da der Domänen Controller, der ihn verwaltet, nicht verfügbar ist.

**TIP**

Dieser Befehl verwendet den Continue-Wert für den *ErrorAction* -Parameter, der das Server-GPO "Entry Point 2" aktualisiert, obwohl das Server-Gruppenrichtlinien Objekt "Einstiegspunkt 1" nicht aktualisiert werden konnte.

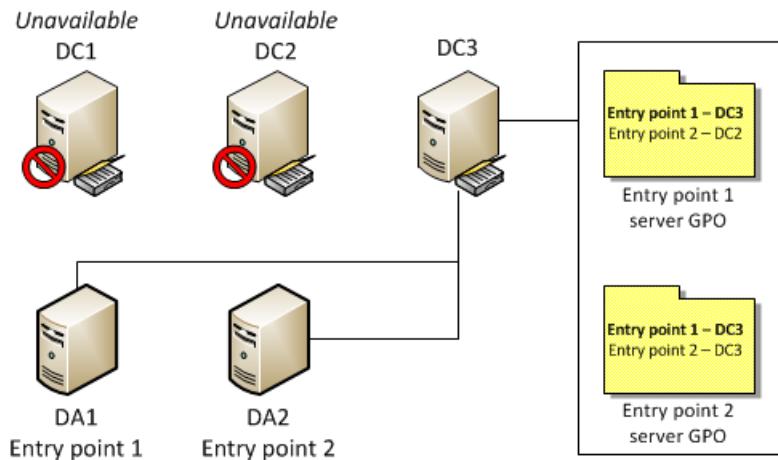
Die resultierende Konfiguration ist in der folgenden Abbildung dargestellt.



2. Führen Sie den folgenden Befehl aus, um den nicht verfügbaren Domänen Controller "DC1" durch den Domänen Controller "DC3" zu ersetzen:

```
Set-DAEntryPointDC "ExistingDC 'DC1' "NewDC 'DC3' "ComputerName 'DA2' "ErrorAction Continue
```

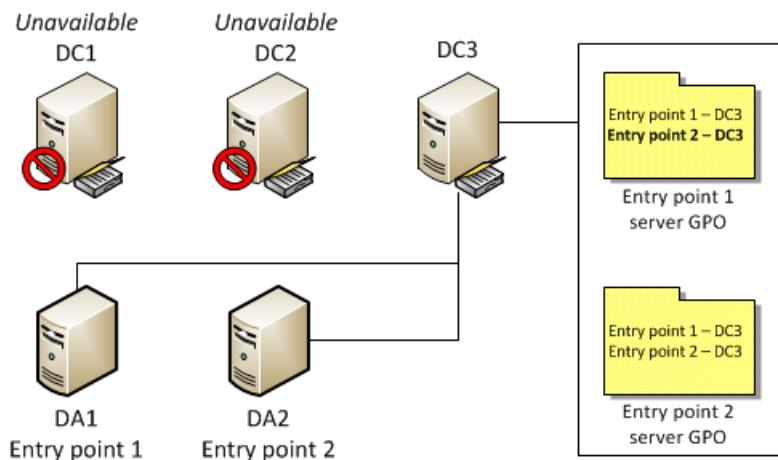
Mit diesem Befehl wird die Domänen Controller Zuordnung für das Server-Gruppenrichtlinien Objekt "Entry Point 1" in der Registrierung von da1 und in den Server-Gruppenrichtlinien Objekten "Entry Point 1" und "Entry Point 2" aktualisiert. Die resultierende Konfiguration ist in der folgenden Abbildung dargestellt.



3. Um die Domänen Controller Zuordnung für das Server-Gruppenrichtlinien Objekt "Entry Point 2" im Server-Gruppenrichtlinien Objekt "Einstiegspunkt 1" zu synchronisieren, führen Sie den Befehl aus, um "DC2" durch "DC3" zu ersetzen, und geben Sie den Remote Zugriffs Server an, dessen Server-GPO nicht synchronisiert ist, in diesem Fall "da1" für den *Computername* -Parameter

```
Set-DAEntryPointDC "ExistingDC 'DC2' "NewDC 'DC3' "ComputerName 'DA1' "ErrorAction Continue
```

Die endgültige Konfiguration ist in der folgenden Abbildung dargestellt.



### Optimierung der Konfigurations Verteilung

Wenn Sie Konfigurationsänderungen vornehmen, werden die Änderungen erst angewendet, nachdem die Server-Gruppenrichtlinien Objekte an die RAS-Server weitergegeben wurden. Um die Konfigurations Verteilung zu verkürzen, wählt der Remote Zugriff automatisch einen beschreibbaren Domänen Controller aus, der dem RAS-Server am nächsten liegt, wenn das zugehörige Server-Gruppenrichtlinien Objekt erstellt wird.

In einigen Szenarien kann es erforderlich sein, den Domänen Controller, von dem ein Server-Gruppenrichtlinien Objekt verwaltet wird, manuell zu ändern, um die Konfigurationszeit für die Verteilung zu optimieren:

- Es waren keine beschreibbaren Domänen Controller an der Active Directory Site eines RAS-Servers zum Zeitpunkt des Hinzufügens als Einstiegspunkt vorhanden. Ein Beschreibbarer Domänen Controller wird jetzt der Active Directory Site des RAS-Servers hinzugefügt.
- Durch eine Änderung der IP-Adresse oder durch Änderungen an Active Directory Standorten und Subnetzen konnte der RAS-Server möglicherweise an einen anderen Active Directory Standort verschoben werden.
- Die Domänen Controller Zuordnung für einen Einstiegspunkt wurde manuell aufgrund von Wartungsarbeiten auf einem Domänen Controller geändert, und der Domänen Controller ist nun wieder online.

Führen Sie in diesen Szenarien das PowerShell-Cmdlet `Set-DAEntryPointDC` auf dem RAS-Server aus, und geben Sie mit dem Parameter *entrypointname* den Namen des Einstiegs Punkts an, den Sie optimieren möchten. Dies sollten Sie nur tun, nachdem die GPO-Daten des Domänen Controllers, der das Server-GPO derzeit speichert, bereits vollständig auf dem gewünschten neuen Domänen Controller repliziert wurden.

#### NOTE

Vergewissern Sie sich vor dem Ändern der Domänen Controller Zuordnung, dass alle GPOs in der Remote Zugriffs Bereitstellung auf allen Domänen Controllern in der Domäne repliziert wurden. Wenn das Gruppenrichtlinien Objekt nicht synchronisiert ist, können nach dem Ändern der Domänen Controller Zuordnung die aktuellen Konfigurationsänderungen verloren gehen. Dies kann zu einer beschädigten Konfiguration führen. Informationen zum Überprüfen der Gruppenrichtlinien Objekt-Synchronisierung finden Sie unter [Überprüfen des Gruppenrichtlinie](#)

Führen Sie einen der folgenden Schritte aus, um die Konfigurations Verteilung zu optimieren:

- Führen Sie den folgenden Befehl aus, um das Server-Gruppenrichtlinien Objekt des Einstiegs Punkts "Einstiegspunkt 1" auf einem Domänen Controller am nächstgelegenen Active Directory Standort zum

RAS-Server "da1.Corp.contoso.com" zu verwalten:

```
Set-DAEntryPointDC "EntryPointName 'Entry point 1' "ComputerName 'DA1.corp.contoso.com' "ErrorAction  
Inquire
```

- Führen Sie den folgenden Befehl aus, um das Server-Gruppenrichtlinien Objekt des Einstiegs Punkts "Einstiegspunkt 1" auf dem Domänen Controller "DC2.Corp.contoso.com" zu verwalten:

```
Set-DAEntryPointDC "EntryPointName 'Entry point 1' "NewDC 'dc2.corp.contoso.com' "ComputerName  
'DA1.corp.contoso.com' "ErrorAction Inquire
```

#### NOTE

Wenn Sie den einem bestimmten Einstiegspunkt zugeordneten Domänen Controller ändern, müssen Sie einen Remote Zugriffs Server angeben, der Mitglied dieses Einstiegs Punkts für den *Computername*-Parameter ist.

## Siehe auch

- [Schritt 3: Konfigurieren der Bereitstellung für mehrere Standorte](#)
- [Schritt 1: Implementieren einer Remote Zugriffs Bereitstellung für einen einzelnen Server](#)

# Schritt 3 Konfigurieren der Bereitstellung für mehrere Standorte

09.04.2020 • 37 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Führen Sie nach dem Konfigurieren der Infrastruktur für mehrere Standorte die folgenden Schritte aus, um die Bereitstellung des Remote Zugriffs für mehrere Standorte einzurichten.

AUFGABE	BESCHREIBUNG
3.1. Konfigurieren von Remote Zugriffs Servern	Konfigurieren Sie zusätzliche Remote Zugriffs Server, indem Sie IP-Adressen einrichten, Sie der Domäne hinzufügen und die Remote Zugriffs Rolle installieren.
3.2. Gewähren des Administrator Zugriffs	Erteilen Sie dem DirectAccess-Administrator Berechtigungen für die zusätzlichen Remote Zugriffs Server.
3.3. Konfigurieren von IP-HTTPS für eine Bereitstellung mit mehreren Standorten	Konfigurieren des IP-HTTPS-Zertifikats, das in einer Bereitstellung für mehrere Standorte verwendet wird.
3.4. Konfigurieren des Netzwerkadressen Servers für eine Bereitstellung mit mehreren Standorten	Konfigurieren des Netzwerkadressen Server-Zertifikats, das bei einer Bereitstellung mit mehreren Standorten verwendet wird
3.5. Konfigurieren von DirectAccess-Clients für eine Bereitstellung mit mehreren Standorten	Entfernen Sie Windows 7-Client Computer aus Windows 8-Sicherheitsgruppen.
3.6. Aktivieren der Bereitstellung für mehrere Standorte	Aktivieren Sie die Bereitstellung für mehrere Standorte auf dem ersten Remote Zugriffs Server.
3.7. Hinzufügen von Einstiegspunkten zur Bereitstellung für mehrere Standorte	Fügen Sie der Bereitstellung für mehrere Standorte zusätzliche Einstiegspunkte hinzu.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## 3.1. Konfigurieren von Remote Zugriffs Servern

### So installieren Sie die Remotezugriffsrolle

1. Stellen Sie sicher, dass jeder RAS-Server mit der richtigen Bereitstellungs Topologie (Edge, hinter einer NAT, einer einzelnen Netzwerkschnittstelle) und entsprechenden Routen konfiguriert ist.
2. Konfigurieren Sie die IP-Adressen auf jedem RAS-Server entsprechend der Standort Topologie und dem IP-Addressierungs Schema Ihrer Organisation.
3. Verknüpfen Sie jeden RAS-Server mit einer Active Directory Domäne.
4. Klicken Sie in der Server-Manager-Konsole im Dashboard auf Rollen und Features hinzufügen.

5. Klicken Sie dreimal auf **Weiter**, um zur Anzeige für die Serverrollenauswahl zu gelangen.
6. Wählen Sie im Dialogfeld **Server Rollen auswählen** die Option **Remote Zugriff** aus, und klicken Sie dann auf **weiter**.
7. Klicken Sie drei Mal auf **weiter**.
8. Wählen Sie im Dialogfeld **Rollen Dienste auswählen** die Option **DirectAccess und VPN (RAS)** aus, und klicken Sie dann auf **Features hinzufügen**.
9. Wählen Sie **Routing, webanwendungsproxy** aus, klicken Sie auf **Features hinzufügen** und dann auf **weiter**.
10. Klicken Sie auf **Weiter** und dann auf **Installieren**.
11. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.

#### **Befehle in Windows PowerShell**

Die Schritte 1-3 müssen manuell ausgeführt werden und werden nicht mithilfe dieses Windows PowerShell-Cmdlets ausgeführt.

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

## 3.2. Gewähren des Administrator Zugriffs

### **So erteilen Sie Administrator Berechtigungen**

1. Geben Sie auf dem Remote Zugriffs Server im zusätzlichen Einstiegspunkt Folgendes ein: **Computer Verwaltung**, und drücken Sie dann die **Eingabe** Taste.
2. Klicken Sie im linken Bereich auf **lokale Benutzer und Gruppen**.
3. Doppelklicken Sie auf **Gruppen**, und doppelklicken Sie dann auf **Administratoren**.
4. Klicken Sie im Dialogfeld **Administrator Eigenschaften** auf **Hinzufügen**, und klicken Sie im Dialogfeld **Benutzer, Computer, Dienst Konten oder Gruppen auswählen** auf **Speicher Orte**.
5. Klicken Sie im Dialogfeld **Speicher Orte** in der Struktur **Speicherort** auf den Speicherort, der das Benutzerkonto des DirectAccess-Administrators enthält, und klicken Sie dann auf **OK**.
6. Geben Sie unter **Geben Sie die zu ausgewählenden Objektnamenein** den Benutzernamen des DirectAccess-Administrators ein, und klicken Sie dann zweimal auf **OK**.
7. Klicken Sie im Dialogfeld **Administrator Eigenschaften** auf **OK**.
8. Schließen Sie das Fenster Computerverwaltung.
9. Wiederholen Sie diesen Vorgang auf allen RAS-Servern, die Teil der Bereitstellung für mehrere Standorte sein werden.

## 3.3. Konfigurieren von IP-HTTPS für eine Bereitstellung mit mehreren Standorten

Auf jedem Remote Zugriffs Server, der der Bereitstellung für mehrere Standorte hinzugefügt wird, ist ein SSL-

Zertifikat erforderlich, um die HTTPS-Verbindung mit dem IP-HTTPS-Webserver zu überprüfen. Zum Ausführen dieses Verfahrens ist mindestens die Mitgliedschaft in der lokalen Gruppe **Administratoren** oder eine gleichwertige Berechtigung erforderlich.

**So erhalten Sie ein IP-HTTPS-Zertifikat**

1. Auf jedem RAS-Server: Geben Sie auf dem **Start** Bildschirm **MMC**ein, und drücken Sie dann die **EINGABETASTE**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie im Menü **Datei** auf **Snap-Ins hinzufügen bzw. entfernen**.
3. Klicken Sie auf **Zertifikate, Hinzufügen, Computerkonto** und **Weiter**. Wählen Sie **Lokaler Computer** aus, klicken Sie auf **Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
6. Klicken Sie zweimal auf **Weiter**.
7. Klicken Sie auf der Seite **Zertifikate anfordern** auf die Vorlage **Webserver Zertifikat**, und klicken Sie dann auf **Weitere Informationen sind erforderlich, um sich für dieses Zertifikat zu registrieren**.

Wenn die Vorlage für das Webserver Zertifikat nicht angezeigt wird, stellen Sie sicher, dass das Remote Zugriffs Server-Computer Konto über die Berechtigung "registrieren" für die Webserver-Zertifikat Vorlage verfügt. Weitere Informationen finden Sie unter [Konfigurieren von Berechtigungen für die Webserver-Zertifikat Vorlage](#).

8. Wählen Sie im Dialogfeld **Zertifikat Eigenschaften auf der Register Karte Antragsteller** unter **Antragsteller Name** für **Typ** die Option **allgemeiner Name** aus.
9. Geben Sie unter **Wert** den voll qualifizierten Domänen Namen (FQDN) des Internet namens des Remote Zugriffs Servers (z. b. Europe.contoso.com) ein, und klicken Sie dann auf **Hinzufügen**.
10. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
11. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, dass ein neues Zertifikat mit dem vollqualifizierten Domänennamen unter **Serverauthentifizierung** mit der Option **Beabsichtigte Zwecke** registriert wurde.
12. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und klicken Sie anschließend auf **Eigenschaften**.
13. Geben Sie unter **Anzeigename** die Zeichenfolge **IP-HTTPS-Zertifikat** ein, und klicken Sie dann auf **OK**.

**TIP**

Die Schritte 12 und 13 sind optional, erleichtern Ihnen jedoch die Auswahl des Zertifikats für IP-HTTPS beim Konfigurieren des Remote Zugriffs.

14. Wiederholen Sie diesen Vorgang auf allen RAS-Servern in Ihrer Bereitstellung.

### 3,4. Konfigurieren des Netzwerkadressen Servers für eine Bereitstellung mit mehreren Standorten

Wenn Sie beim Einrichten des ersten Servers die Netzwerkadressen Server-Website auf dem RAS-Server eingerichtet haben, muss jeder neue RAS-Server, den Sie hinzufügen, mit einem Webserver Zertifikat konfiguriert

werden, das den gleichen Antragsteller Namen hat, den Sie ausgewählt haben. der Netzwerkadressen Server für den ersten Server. Jeder Server benötigt ein Zertifikat, um die Verbindung mit dem Netzwerkadressen Server zu authentifizieren, und Client Computer im internen Netzwerk müssen in der Lage sein, den Namen der Website in DNS aufzulösen.

#### **So installieren Sie ein Zertifikat für den Netzwerk Speicherort**

1. Auf dem Remote Zugriffs Server: Geben Sie auf dem **Start** Bildschirm **MMC**ein, und drücken Sie dann die **EINGABETASTE**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie im Menü **Datei** auf **Snap-Ins hinzufügen bzw. entfernen**.
3. Klicken Sie auf **Zertifikate, Hinzufügen, Computerkonto** und **Weiter**. Wählen Sie **Lokaler Computer** aus, klicken Sie auf **Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.

#### **NOTE**

Sie können auch das Zertifikat importieren, das für den Netzwerkadressen Server für den ersten RAS-Server verwendet wurde.

6. Klicken Sie zweimal auf **Weiter**.
7. Klicken Sie auf der Seite **Zertifikate anfordern** auf die Vorlage **Webserver Zertifikat**, und klicken Sie dann auf **Weitere Informationen sind erforderlich, um sich für dieses Zertifikat zu registrieren**.

Wenn die Vorlage für das Webserver Zertifikat nicht angezeigt wird, stellen Sie sicher, dass das Remote Zugriffs Server-Computer Konto über die Berechtigung "registrieren" für die Webserver-Zertifikat Vorlage verfügt. Weitere Informationen finden Sie unter [Konfigurieren von Berechtigungen für die Webserver-Zertifikat Vorlage](#).

8. Wählen Sie im Dialogfeld **Zertifikat Eigenschaften auf der Register Karte Antragsteller** unter **Antragsteller Name** für **Typ** die Option **allgemeiner Name** aus.
9. Geben Sie unter **Wert** den voll qualifizierten Domänen Namen (FQDN) ein, der für das Netzwerkadressen Server-Zertifikat des ersten Remote Zugriffs Servers (z. b. `nls.Corp.contoso.com`) konfiguriert wurde, und klicken Sie dann auf **Hinzufügen**.
10. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
11. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, dass ein neues Zertifikat mit dem vollqualifizierten Domänennamen unter **Serverauthentifizierung** mit der Option **Beabsichtigte Zwecke** registriert wurde.
12. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und klicken Sie anschließend auf **Eigenschaften**.
13. Geben Sie unter **Anzeigenamen** den Namen **Netzwerkadressenzertifikat** ein, und klicken Sie dann auf **OK**.

**TIP**

Die Schritte 12 und 13 sind optional, erleichtern es Ihnen jedoch, das Zertifikat für den Netzwerk Speicherort beim Konfigurieren des Remote Zugriffs auszuwählen.

14. Wiederholen Sie diesen Vorgang auf allen RAS-Servern in Ihrer Bereitstellung.

**So erstellen Sie DNS-Einträge für den Netzwerkadressen Server**

1. Auf dem DNS-Server: Geben Sie auf dem **Start** Bildschirm **dnsmgmt. mscein**, und drücken Sie dann die **EINGABETASTE**.
2. Öffnen Sie im linken Bereich der **DNS-Manager**-Konsole die Forward-Lookupzone für das interne Netzwerk. Klicken Sie mit der rechten Maustaste auf die relevante Zone, und klicken Sie auf **neuer Host (A oder AAAA)**
3. Geben Sie im Dialogfeld **neuer Host** in das Feld **Name (verwendet übergeordneter Domänen Name wenn leer)** den Namen ein, der für den Netzwerkadressen Server für den ersten RAS-Server verwendet wurde. Geben Sie im Feld **IP-Adresse** die IPv4-Adresse des Remote Zugriffs Servers ein, und klicken Sie dann auf **Host hinzufügen**. Klicken Sie im Dialogfeld **DNS** auf **OK**.
4. Geben Sie im Dialogfeld **neuer Host** in das Feld **Name (verwendet übergeordneter Domänen Name wenn leer)** den Namen ein, der für den Netzwerkadressen Server für den ersten RAS-Server verwendet wurde. Geben Sie im Feld **IP-Adresse** die IPv6-Adresse des Remote Zugriffs Servers ein, und klicken Sie dann auf **Host hinzufügen**. Klicken Sie im Dialogfeld **DNS** auf **OK**.
5. Wiederholen Sie die Schritte 3 und 4 für jeden RAS-Server in der Bereitstellung.
6. Klicken Sie auf **Fertig**.
7. Wiederholen Sie dieses Verfahren, bevor Sie Server als zusätzliche Einstiegspunkte in der Bereitstellung hinzufügen.

### 3.5. Konfigurieren von DirectAccess-Clients für eine Bereitstellung mit mehreren Standorten

DirectAccess-Windows-Client Computer müssen Mitglieder der Sicherheitsgruppe (n) sein, die ihre DirectAccess-Zuordnung definieren. Vor der Aktivierung mehrerer Standorte können diese Sicherheitsgruppen sowohl Windows 8-Clients als auch Windows 7-Clients enthalten (sofern der entsprechende Modus "Downlevel" ausgewählt wurde). Wenn die Funktion für mehrere Standorte aktiviert ist, werden vorhandene Client Sicherheitsgruppen im Einzel Server Modus nur für Windows 8 in die Sicherheitsgruppe (n) konvertiert. Nachdem Multisite aktiviert ist, müssen DirectAccess-Windows 7-Client Computer in die entsprechenden dedizierten Windows 7-Client Sicherheitsgruppen (die bestimmten Einstiegspunkten zugeordnet sind) verschoben werden, oder Sie können keine Verbindung über DirectAccess herstellen. Die Windows 7-Clients müssen zunächst aus den vorhandenen Sicherheitsgruppen entfernt werden, die jetzt Windows 8-Sicherheitsgruppen sind. Vorsicht: Windows 7-Client Computer, die Mitglieder von Windows 7-und Windows 8-Client Sicherheitsgruppen sind, verlieren die Remote Konnektivität, und Windows 7-Clients ohne installiertes SP1 verlieren auch die Unternehmens Konnektivität. Daher müssen alle Windows 7-Client Computer aus Windows 8-Sicherheitsgruppen entfernt werden.

**Entfernen von Windows 7-Clients aus Windows 8-Sicherheitsgruppen**

1. Klicken Sie auf dem primären Domänen Controller auf **Start**, und klicken Sie dann auf **Active Directory Benutzer und Computer**.
2. Wenn Sie Computer aus der Sicherheitsgruppe entfernen möchten, doppelklicken Sie auf die Sicherheitsgruppe, und klicken Sie im Dialogfeld **Eigenschaften von < Group\_Name >** auf die Registerkarte **Mitglieder**.

3. Wählen Sie den Windows 7-Client Computer aus, und klicken Sie auf **Entfernen**.
4. Wiederholen Sie dieses Verfahren, um die Windows 7-Client Computer aus den Windows 8-Sicherheitsgruppen zu entfernen.

#### **IMPORTANT**

Wenn Sie eine Remote Zugriffs Konfiguration für mehrere Standorte aktivieren, verlieren alle Client Computer (Windows 7 und Windows 8) Remote Verbindungen, bis Sie direkt oder per VPN eine Verbindung mit dem Unternehmensnetzwerk herstellen können, um Ihre Gruppenrichtlinien zu aktualisieren. Dies trifft zu, wenn Sie die Funktionalität für mehrere Standorte zum ersten Mal aktivieren, und auch wenn Sie mehrere Websites deaktivieren.

## 3.6. Aktivieren der Bereitstellung für mehrere Standorte

Um eine Bereitstellung für mehrere Standorte zu konfigurieren, aktivieren Sie die Funktion für mehrere Standorte auf dem vorhandenen Remote Zugriffs Server. Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie mehrere Standorte in der Bereitstellung aktivieren:

1. Globale Load Balancer-Einstellungen und IP-Adressen, wenn Sie einen Lastenausgleich für DirectAccess-Clientverbindungen über alle Einstiegspunkte in der Bereitstellung ausführen möchten.
2. Die Sicherheitsgruppen, die Windows 7-Client Computer für den ersten Einstiegspunkt in der Bereitstellung enthalten, wenn Sie den Remote Zugriff für Windows 7-Client Computer aktivieren möchten.
3. Gruppenrichtlinie Objektnamen, wenn Sie nicht standardmäßige Gruppenrichtlinie Objekte verwenden müssen, die auf Windows 7-Client Computern für den ersten Einstiegspunkt in der Bereitstellung angewendet werden, wenn Sie Unterstützung für Windows 7-Client Computer benötigen.

#### **So aktivieren Sie eine Konfiguration für mehrere Standorte**

1. Auf dem vorhandenen RAS-Server: Geben Sie auf dem Start Bildschirm **ramgmtui.exe**, und drücken Sie dann die EINGABETASTE. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remote Zugriffs-Verwaltungskonsole auf **Konfiguration**, und klicken Sie dann im Bereich **Tasks** auf **Multisite aktivieren**.
3. Klicken Sie im Assistenten zum **Aktivieren der Bereitstellung für mehrere Standorte** auf der Seite **Vorbemerkungen** auf **weiter**.
4. Geben Sie auf der Seite **Bereitstellungs Name** unter **Name** der Bereitstellung für **mehrere Standorte** einen Namen für die Bereitstellung ein. Geben Sie unter **Name des ersten Einstiegs Punkt** einen Namen ein, um den ersten Einstiegspunkt zu identifizieren, der der aktuelle RAS-Server ist, und klicken Sie dann auf **weiter**.
5. Führen Sie auf der Seite **Einstiegspunkt Auswahl** einen der folgenden Schritte aus:
  - Klicken Sie auf **Einstiegspunkte automatisch zuweisen, und lassen Sie Clients die Option manuell auswählen**, um Client Computer automatisch an den am besten geeigneten Einstiegspunkt weiterzuleiten, während gleichzeitig Client Computer einen Einstiegspunkt manuell auswählen können. Die Auswahl für den manuellen Einstiegspunkt ist nur für Windows 8-Computer verfügbar. Klicken Sie auf **Weiter**.
  - Klicken Sie auf **Einstiegspunkte automatisch zuweisen**, um Client Computer automatisch an den am besten geeigneten Einstiegspunkt weiterzuleiten, und klicken Sie dann auf **weiter**.
6. Führen Sie auf der Seite **Globaler Lastenausgleich** einen der folgenden Schritte aus:

- Klicken Sie auf **Nein, verwenden Sie keinen globalen Lastenausgleich**, wenn Sie keinen globalen Lastenausgleich verwenden möchten, und klicken Sie dann auf **weiter**.

**NOTE**

Wenn Sie diese Option auswählen, wird automatisch eine Verbindung mit dem nächstgelegenen Einstiegspunkt hergestellt.

- Klicken Sie auf **Ja, globalen Lastenausgleich verwenden**, Wenn Sie den Datenverkehr Global zwischen allen Einstiegspunkten gleichmäßig verteilen möchten. Geben Sie unter **Geben Sie den globalen Lastenausgleich- FQDN ein, der von allen Einstiegspunkten verwendet werden soll**, den globalen Lasten Ausgleichs-FQDN ein, und geben Sie unter **Geben Sie die globale Lasten Ausgleichs-IP-Adresse für diesen Einstiegspunkt ein**, der den ersten RAS-Server enthält, und klicken Sie dann auf **weiter**.

7. Führen Sie auf der Seite **Client Unterstützung** einen der folgenden Schritte aus:

- Um den Zugriff auf Client Computer unter Windows 8 oder höher einzuschränken, klicken Sie auf **Zugriff auf Client Computer mit Windows 8 oder höher beschränken**, und klicken Sie dann auf **weiter**.
- Damit Client Computer mit Windows 7 auf diesen Einstiegspunkt zugreifen können, klicken Sie auf **Client Computern, auf denen Windows 7 ausgeführt wird, auf diesen Einstiegspunkt zugreifen**, und klicken Sie auf **Hinzufügen**. Wählen Sie im Dialogfeld **Gruppen auswählen** die Sicherheitsgruppen aus, die die Windows 7-Client Computer enthalten, klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.

8. Akzeptieren Sie auf der Seite **Client-Gruppenrichtlinien Objekt- Einstellungen** das Standard-Gruppenrichtlinien Objekt für Windows 7-Client Computer für diesen Einstiegspunkt, geben Sie den Namen des Gruppenrichtlinien Objekts ein, das automatisch erstellt werden soll, oder klicken Sie auf **Durchsuchen**, um das Gruppenrichtlinien Objekt für Windows 7-Client Computer zu suchen, und klicken Sie auf **weiter**.

**NOTE**

- Die Seite **Einstellungen für das Client -Gruppenrichtlinien Objekt** wird nur angezeigt, wenn Sie den Einstiegspunkt so konfigurieren, dass Windows 7-Client Computer auf den Einstiegspunkt zugreifen können.
- Optional können Sie auf **GPOs** überprüfen klicken, um sicherzustellen, dass Sie über die entsprechenden Berechtigungen für das ausgewählte Gruppenrichtlinien Objekt oder GPOs für diesen Einstiegspunkt verfügen. Wenn das GPO nicht vorhanden ist und automatisch erstellt wird, sind Create-und Link-Berechtigungen erforderlich. Wenn die Gruppenrichtlinien Objekte manuell erstellt wurden, sind die Berechtigungen bearbeiten, Sicherheit ändern und Löschen erforderlich.

9. Klicken Sie auf der Seite **Zusammenfassung** auf **Commit**.

10. Klicken Sie im Dialogfeld **Bereitstellung für mehrere Standorte** aktivieren auf **Schließen**, und klicken Sie dann im Assistenten zum Aktivieren der Bereitstellung für mehrere Standorte auf **Schließen**.

 **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

So aktivieren Sie eine Bereitstellung mit mehreren Standorten mit dem Namen "Configuration Manager" auf dem ersten Einstiegspunkt mit dem Namen "EDGE1-US". Mithilfe der Bereitstellung können Clients den Einstiegspunkt

manuell auswählen und keinen globalen Lastenausgleich verwenden.

```
Enable-DAMultiSite -Name 'Contoso' -EntryPointName 'Edge1-US' -ManualEntryPointSelectionAllowed 'Enabled'
```

Um Windows 7-Client Computern den Zugriff über den ersten Einstiegspunkt über die Sicherheitsgruppe zu gestatten, DA\_Clients\_US und die Verwendung des GPO-DA\_W7\_Clients\_GPO\_US.

```
Add-DAClient -EntryPointName 'Edge1-US' -DownlevelSecurityGroupNameList @('corp.contoso.com\DA_Clients_US') -  
DownlevelGpoName @('corp.contoso.com\DA_W7_Clients_GPO_US')
```

### 3,7. Hinzufügen von Einstiegspunkten zur Bereitstellung für mehrere Standorte

Nachdem Sie mehrere Standorte in der Bereitstellung aktiviert haben, können Sie mithilfe des Assistenten zum Hinzufügen eines Einstiegs Punkts weitere Einstiegspunkte hinzufügen. Stellen Sie vor dem Hinzufügen von Einstiegspunkten sicher, dass Sie über die folgenden Informationen verfügen:

- Globale Load Balancer-IP-Adressen für jeden neuen Einstiegspunkt, wenn Sie einen globalen Lastenausgleich verwenden.
- Die Sicherheitsgruppen, die Windows 7-Client Computer für jeden Einstiegspunkt enthalten, der hinzugefügt wird, wenn Sie den Remote Zugriff für Windows 7-Client Computer aktivieren möchten.
- Gruppenrichtlinie Objektnamen, wenn Sie nicht standardmäßige Gruppenrichtlinie Objekte verwenden müssen, die für jeden hinzu zufügenden Einstiegspunkt auf Windows 7-Client Computern angewendet werden, wenn Sie Unterstützung für Windows 7-Client Computer benötigen.
- Wenn IPv6 im Netzwerk der Organisation bereitgestellt wird, müssen Sie das IP-HTTPS-Präfix für den neuen Einstiegspunkt vorbereiten.

#### So fügen Sie Ihrer Bereitstellung für mehrere Standorte Einstiegspunkte hinzu

1. Auf dem vorhandenen RAS-Server: Geben Sie auf dem Start Bildschirm **ramgmtui.exe**, und drücken Sie dann die EINGABETASTE. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remote Zugriffs-Verwaltungskonsole auf **Konfiguration**, und klicken Sie dann im Bereich **Tasks** auf **Einstiegspunkt hinzufügen**.
3. Geben Sie im Assistenten zum Hinzufügen von Einstiegspunkten auf der Seite **Einstiegspunkt Details** unter **RAS-Server** den voll qualifizierten Domänen Namen (FQDN) des hinzu zufügenden Servers ein. Geben Sie unter **Einstiegspunkt Name** den Namen des Einstiegs Punkts ein, und klicken Sie dann auf **weiter**.
4. Geben Sie auf der Seite **globale Einstellungen für den Lastenausgleich** die globale IP-Adresse für den Lastenausgleich dieses Einstiegs Punkts ein, und klicken Sie dann auf **weiter**.

#### NOTE

Die Seite **globale Einstellungen für den Lastenausgleich** wird nur angezeigt, wenn die Konfiguration für mehrere Standorte einen globalen Load Balancer verwendet.

5. Klicken Sie auf der Seite **Netzwerktopologie** auf die Topologie, die der Netzwerktopologie des RAS-Servers entspricht, den Sie hinzufügen, und klicken Sie dann auf **weiter**.

6. Geben Sie auf der Seite **Netzwerkname oder IP-Adresse** in **Geben Sie den öffentlichen Namen oder die IP-Adresse ein, die von Clients zum Herstellen einer Verbindung mit dem RAS-Server verwendet wird.** Der öffentliche Name entspricht dem Antragsteller Namen des IP-HTTPS-Zertifikats. Bei der Implementierung der edgenetzwerktopologie ist die IP-Adresse die Adresse des externen Adapters des RAS-Servers. Klicken Sie auf **Weiter**.

7. Führen Sie auf der Seite **Netzwerkadapter** einen der folgenden Schritte aus:

- Wenn Sie eine Topologie mit zwei Netzwerkadapters bereitstellen, wählen Sie in **externer Adapter** den Adapter aus, der mit dem externen Netzwerk verbunden ist. Wählen Sie unter **interner Adapter** den Adapter aus, der mit dem internen Netzwerk verbunden ist.
- Wenn Sie eine Topologie mit einem Netzwerkadapter bereitstellen, wählen Sie unter **Netzwerkadapter** den Adapter aus, der mit dem internen Netzwerk verbunden ist.

8. Klicken Sie auf der Seite **Netzwerkadapter** unter **Wählen Sie das Zertifikat zum Authentifizieren von IP-HTTPS-Verbindungen auswählen** auf **Durchsuchen**, um das IP-HTTPS-Zertifikat zu suchen und auszuwählen. Klicken Sie auf **Weiter**.

9. Wenn IPv6 im Unternehmensnetzwerk konfiguriert ist, geben Sie auf der Seite **Präfix Konfiguration** unter **IPv6-Präfix, das Client Computern zugewiesen ist** ein IP-HTTPS-Präfix ein, um den DirectAccess-Client Computern IPv6-Adressen zuzuweisen, und klicken Sie auf **weiter**.

10. Führen Sie auf der Seite **Client Unterstützung** einen der folgenden Schritte aus:

- Um den Zugriff auf Client Computer unter Windows 8 oder höher einzuschränken, klicken Sie auf **Zugriff auf Client Computer mit Windows 8 oder höher beschränken**, und klicken Sie dann auf **weiter**.
- Damit Client Computer mit Windows 7 auf diesen Einstiegspunkt zugreifen können, klicken Sie auf **Client Computern, auf denen Windows 7 ausgeführt wird, auf diesen Einstiegspunkt zugreifen**, und klicken Sie auf **Hinzufügen**. Wählen Sie im Dialogfeld **Gruppen auswählen** die Sicherheitsgruppen aus, die die Windows 7-Client Computer enthalten, von denen eine Verbindung mit diesem Einstiegspunkt hergestellt werden soll, klicken Sie auf **OK**, und klicken Sie **dann auf weiter**.

11. Akzeptieren Sie auf der Seite **Client-Gruppenrichtlinien Objekt- Einstellungen** das Standard-Gruppenrichtlinien Objekt für Windows 7-Client Computer für diesen Einstiegspunkt, geben Sie den Namen des GPO ein, das Sie automatisch erstellen möchten, oder klicken Sie auf **Durchsuchen**, um das Gruppenrichtlinien Objekt für Windows 7-Client Computer zu suchen, und klicken Sie auf **weiter**.

**NOTE**

- Die Seite **Einstellungen für das Client -Gruppenrichtlinien Objekt** wird nur angezeigt, wenn Sie den Einstiegspunkt so konfigurieren, dass Windows 7-Client Computer auf den Einstiegspunkt zugreifen können.
- Optional können Sie auf **GPOs** überprüfen klicken, um sicherzustellen, dass Sie über die entsprechenden Berechtigungen für das ausgewählte Gruppenrichtlinien Objekt oder GPOs für diesen Einstiegspunkt verfügen. Wenn das GPO nicht vorhanden ist und automatisch erstellt wird, sind Create-und Link-Berechtigungen erforderlich. Wenn die Gruppenrichtlinien Objekte manuell erstellt wurden, sind die Berechtigungen bearbeiten, Sicherheit ändern und Löschen erforderlich.

12. Akzeptieren Sie auf der Seite **Server-GPO-Einstellungen** das Standard-Gruppenrichtlinien Objekt für diesen RAS-Server, geben Sie den Namen des GPO ein, das Sie automatisch erstellen möchten, oder klicken Sie auf **Durchsuchen**, um das Gruppenrichtlinien Objekt für diesen Server zu suchen, und klicken Sie dann auf **weiter**.

13. Klicken Sie auf der Seite **Netzwerkadressen Server** auf **Durchsuchen**, um das Zertifikat für die Netzwerkadressen Server-Website auszuwählen, die auf dem Remote Zugriffs Server ausgeführt wird, und klicken Sie dann auf **weiter**.

**NOTE**

Die Seite **Netzwerkadressen Server** wird nur angezeigt, wenn die Netzwerkadressen Server-Website auf dem Remote Zugriffs Server ausgeführt wird.

14. Überprüfen Sie auf der Seite **Zusammenfassung** die Einstellungen für den Einstiegspunkt, und klicken Sie dann auf **Commit**.
15. Klicken Sie im Dialogfeld **Einstiegspunkt hinzufügen** auf **Schließen**, und klicken Sie dann im Assistenten zum Hinzufügen von Einstiegspunkten auf **Schließen**.

**NOTE**

Wenn sich der hinzugefügte Einstiegspunkt in einer anderen Gesamtstruktur als die vorhandenen Einstiegspunkte oder Client Computer befindet, müssen Sie im Bereich **Tasks** auf **Verwaltungs Server aktualisieren** klicken, um die Domänen Controller und Configuration Manager in der neuen Gesamtstruktur zu ermitteln.

16. Wiederholen Sie dieses Verfahren aus Schritt 2 für jeden Einstiegspunkt, den Sie der Bereitstellung für mehrere Standorte hinzufügen möchten.

 **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

Um den Computer edge2 aus der corp2-Domäne als zweiten Einstiegspunkt mit dem Namen edge2-Europe hinzuzufügen. Die Einstiegspunkt Konfiguration lautet wie folgt: ein Client-IPv6-Präfix "2001: db8:2: 2000::/64", eine Connect to-Adresse (das IP-HTTPS-Zertifikat auf dem edge2-Computer) "edge2.contoso.com", ein Server-Gruppenrichtlinien Objekt mit dem Namen "DirectAccess-Serveereinstellungen-edge2-Europa" und die internen und externen Schnittstellen mit

```
Add-DAEntryPoint -RemoteAccessServer 'edge2.corp2.corp.contoso.com' -Name 'Edge2-Europe' -ClientIPv6Prefix  
'2001:db8:2:2000::/64' -ConnectToAddress 'Europe.contoso.com' -ServerGpoName  
'corp2.corp.contoso.com\DirectAccess Server Settings - Edge2-Europe' -InternetInterface 'Internet' -  
InternalInterface 'CorpNet2'
```

Um Windows 7-Client Computern den Zugriff auf den zweiten Einstiegspunkt über die Sicherheitsgruppe zu gestatten, DA\_Clients\_Europe und die Verwendung des GPO-DA\_W7\_Clients\_GPO\_Europe.

```
Add-DAClient -EntryPointName 'Edge2-Europe' -DownlevelGpoName @('corp.contoso.com\ DA_W7_Clients_GPO_Europe')  
-DownlevelSecurityGroupNameList @('corp.contoso.com\DA_Clients_Europe')
```

## Siehe auch

- [Schritt 2: Konfigurieren der Infrastruktur für mehrere Standorte](#)

# Schritt 4 Überprüfen der Bereitstellung für mehrere Standorte

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie überprüfen, ob Sie die Bereitstellung für den Remote Zugriff auf mehrere Standorte ordnungsgemäß

## So überprüfen Sie den Zugriff auf interne Ressourcen über die Bereitstellung für mehrere Standorte

1. Stellen Sie eine Verbindung von einem DirectAccess-Clientcomputer mit dem Unternehmensnetzwerk her, und rufen Sie die Gruppenrichtlinie ab.
2. Verbinden Sie den Clientcomputer mit dem externen Netzwerk, und versuchen Sie, auf interne Ressourcen zuzugreifen.

Sie sollten auf alle Unternehmensressourcen zugreifen können.

3. Testen Sie die Konnektivität über jeden Server in der Bereitstellung für mehrere Standorte, indem Sie alle außer einem der RAS-Server ausschalten oder die Verbindung mit dem externen Netzwerk trennen.  
Versuchen Sie auf dem Client Computer, auf Unternehmensressourcen zuzugreifen. Wiederholen Sie den Test auf einem anderen Server mit mehreren Standorten. Es kann bis zu 10 Minuten dauern, bis der Client Computer eine Verbindung mit dem neuen Einstiegspunkt herstellt. Dies liegt daran, dass die Überprüfung 10 Minuten für einen Einstiegspunkt deaktiviert wird, nachdem er als nicht erreichbar eingestuft wurde, um die Bandbreite und die Akku Lebensdauer zu optimieren. Alternativ dazu können Sie manuell zwischen den verschiedenen Einstiegspunkten wechseln, indem Sie den gewünschten Einstiegspunkt aus dem Kombinations Feld auswählen, das beim Ausführen von `daprop.exe` angezeigt wird.

Sie sollten in der Lage sein, über jeden Server mit mehreren Standorten auf alle Unternehmensressourcen zuzugreifen.

4. Verbinden Sie einen Windows 7-Client Computer mit dem Unternehmensnetzwerk, und rufen Sie die Gruppenrichtlinie ab.
5. Verbinden Sie den Windows 7-Client Computer mit dem externen Netzwerk, und versuchen Sie, auf interne Ressourcen zuzugreifen.

Sie sollten auf alle Unternehmensressourcen zugreifen können.

6. Testen Sie die Konnektivität für Windows 7-Clients über jeden Server in der Bereitstellung für mehrere Standorte, indem Sie auf die Konsole Active Directory Benutzer und Computer zugreifen und den Client Computer in die Sicherheitsgruppe verschieben, die den einzelnen Servern entspricht. Nachdem die Änderungen in der gesamten Domäne repliziert wurden, starten Sie den Client Computer neu, während Sie mit dem Unternehmensnetzwerk verbunden sind, um die neue Gruppenrichtlinie zu erhalten. Versuchen Sie, auf Unternehmensressourcen zuzugreifen. Wiederholen Sie den Test auf einem anderen Server mit mehreren Standorten.

Sie sollten in der Lage sein, über jeden Server mit mehreren Standorten auf alle Unternehmensressourcen zuzugreifen.

In einer Produktionsumgebung ist diese Methode möglicherweise aufgrund der Zeitspanne, die für die Replikation von Änderungen in der gesamten Domäne erforderlich ist, nicht möglich. Möglicherweise

möchten Sie die Replikation nach Möglichkeit erzwingen. Tests können auch von mehreren unterschiedlichen Windows 7-Client Computern durchgeführt werden, die bereits Mitglieder der verschiedenen Windows 7-Sicherheitsgruppen in der Bereitstellung für mehrere Standorte sind.

# Problembehandlung bei einer Bereitstellung für mehrere Standorte

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie die häufigsten Fehler beim Konfigurieren der Bereitstellung des Remotezugriffs für mehrere Standorte beheben.

- [Problembehandlung beim Aktivieren von Multisite](#)
- [Fehler beim Hinzufügen von Einstiegspunkten](#)
- [Problembehandlung beim Festlegen des Einstiegspunkt-Domänen Controllers](#)
- [Problembehandlung bei Webtest-URLs](#)
- [Problembehandlung bei allgemeinen Problemen](#)

# Behandeln von Problemen beim Aktivieren der Funktionen für mehrere Standorte

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zum Beheben von Problemen mit dem Befehl `Enable-DAMultisite`. Um sicherzustellen, dass sich der angezeigte Fehler auf das Aktivieren der Funktionen für mehrere Standorte bezieht, prüfen Sie, ob im Windows-Ereignisprotokoll die Ereignis-ID 10051 aufgeführt wird.

## Benutzerkonnektivitätsprobleme

Bei Benutzern treten möglicherweise Konnektivitätsprobleme auf, wenn Sie die Funktionen für mehrere Standorte aktivieren, aber die Konfiguration nicht richtig ist.

### Ursache

Bei einer Bereitstellung mit mehreren Standorten können Windows 10- und Windows 8-Client Computer zwischen verschiedenen Einstiegspunkten wechseln. Windows 7-Client Computer müssen einem bestimmten Einstiegspunkt in der Bereitstellung für mehrere Standorte zugeordnet werden. Falls sich Clientcomputer nicht in der richtigen Sicherheitsgruppe befinden, erhalten sie möglicherweise die falschen Gruppenrichtlinieneinstellungen.

### Lösung

DirectAccess erfordert mindestens eine Sicherheitsgruppe für alle Windows 10- und Windows 8-Client Computer. Es wird empfohlen, eine Sicherheitsgruppe für alle Windows 10- und Windows 8-Computer pro Domäne zu verwenden. DirectAccess erfordert auch eine Sicherheitsgruppe für Windows 7-Client Computer für jeden Einstiegspunkt. Jeder Clientcomputer sollte nur in eine Sicherheitsgruppe aufgenommen werden. Daher sollten Sie sicherstellen, dass die Sicherheitsgruppen für Windows 10- und Windows 8-Clients nur Computer enthalten, auf denen Windows 10 oder Windows 8 ausgeführt wird, und dass jeder Windows 7-Client Computer zu einer dedizierten Sicherheitsgruppe für den relevanten Einstiegspunkt gehört. Es sind keine Windows 10- oder Windows 8-Clients zu den Windows 7-Sicherheitsgruppen gehören.

Konfigurieren Sie die Windows 8-Sicherheitsgruppen auf der Seite **Gruppen auswählen** des Setup-Assistenten für den **DirectAccess-Client**. Konfigurieren Sie Windows 7-Sicherheitsgruppen auf der Seite **Client Unterstützung** des Assistenten zum **Aktivieren der Bereitstellung für mehrere Standorte** oder auf der Seite **Client Unterstützung** des Assistenten zum **Hinzufügen von Einstiegspunkten**.

## Kerberos-Proxyauthentifizierung

Der **Fehler wurde empfangen**. Die Kerberos-Proxy Authentifizierung wird in einer Bereitstellung mit mehreren Standorten nicht unterstützt. Sie müssen die Verwendung von Computerzertifikaten für IPsec-Benutzauthentifizierung aktivieren.

### Ursache

Die Computerzertifikatauthentifizierung muss vor dem Aktivieren der Funktionen für mehrere Standorte aktiviert werden.

### Lösung

So konfigurieren Sie die Computerzertifikatauthentifizierung:

1. Klicken Sie in der Remotezugriffs-Verwaltungskonsole im Detailbereich in Schritt 2 **RAS-Server** auf **Bearbeiten**.
2. Aktivieren Sie im Setup-Assistenten für den RAS-Server auf der Seite **Authentifizierung** das Kontrollkästchen **Computerzertifikate verwenden**, und wählen Sie die Stamm- oder Zwischenzertifizierungsstelle aus, von der Zertifikate in Ihrer Bereitstellung ausgestellt werden.

Verwenden Sie zum Aktivieren der Computer Zertifikat Authentifizierung mithilfe von Windows PowerShell das Cmdlet "`Set-DAServer`", und geben Sie den Parameter "`ipccrootcertificate`" an.

## IP-HTTPS-Zertifikate

Der **Fehler wurde empfangen**. Der DirectAccess-Server verwendet ein selbst signiertes IP-HTTPS-Zertifikat. Konfigurieren Sie IP-HTTPS für die Verwendung eines signierten Zertifikats von einer bekannten Zertifizierungsstelle.

### Ursache

Das IP-HTTPS-Zertifikat ist selbstsigniert. Sie können keine selbstsignierten Zertifikate in einer Bereitstellung für mehrere Standorte verwenden.

### Lösung

So wählen Sie ein IP-HTTPS-Zertifikat aus:

1. Klicken Sie in der Remotezugriffs-Verwaltungskonsole im Detailbereich in Schritt 2 **RAS-Server** auf **Bearbeiten**.
2. Stellen Sie sicher, dass im Setup-Assistenten für den RAS-Server auf der Seite **Netzwerkadapter** unter **Wählen Sie das Zertifikat aus, mit dem IP-HTTPS-Verbindungen authentifiziert werden**: das Kontrollkästchen **Selbstsigniertes Zertifikat verwenden, das von DirectAccess automatisch erstellt wurde** deaktiviert ist, und klicken Sie auf **Durchsuchen**, um ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat auszuwählen.

## Netzwerkadressenserver

### • Problem 1

Der **Fehler wurde empfangen**. DirectAccess ist für die Verwendung eines selbst signierten Zertifikats für den Netzwerkadressen Server konfiguriert. Konfigurieren Sie den Netzwerkadressenserver für die Verwendung eines signierten Zertifikats von einer Zertifizierungsstelle.

### Ursache

Der Netzwerkadressenserver wird auf dem RAS-Server bereitgestellt und verwendet ein selbstsigniertes Zertifikat. Sie können keine selbstsignierten Zertifikate in einer Bereitstellung für mehrere Standorte verwenden.

### Lösung

So wählen Sie ein Netzwerkadressenserver-Zertifikat aus:

1. Klicken Sie in der Remotezugriffs-Verwaltungskonsole im Detailbereich in Schritt 3 **Infrastrukturserver** auf **Bearbeiten**.
2. Stellen Sie sicher, dass im Assistenten zum Einrichten des Infrastrukturservers auf der Seite **Netzwerkadressenserver** unter **Der Netzwerkadressenserver wird auf dem RAS-Server bereitgestellt**: das Kontrollkästchen **Selbstsigniertes Zertifikat verwenden** deaktiviert ist, und klicken Sie auf **Durchsuchen**, um ein von einer Unternehmenszertifizierungsstelle ausgestelltes

Zertifikat auszuwählen.

- **Problem 2**

Der Fehler wurde empfangen. Zum Bereitstellen eines Clusters mit Netzwerk Lastenausgleich oder einer Bereitstellung mit mehreren Standorten müssen Sie ein Zertifikat für den Netzwerkadressen Server mit einem Antragsteller Namen abrufen, der sich vom internen Namen des RAS-Servers unterscheidet.

#### **Ursache**

Der Antragstellernname des für die Netzwerkadressenserver-Website verwendeten Zertifikats stimmt mit dem internen Namen des RAS-Servers überein. Dadurch werden Probleme bei der Namensauflösung verursacht.

#### **Lösung**

Fordern Sie ein Zertifikat mit einem Antragstellernamen an, der sich vom internen Namen des RAS-Servers unterscheidet.

So konfigurieren Sie den Netzwerkadressenserver:

1. Klicken Sie in der Remotezugriffs-Verwaltungskonsole im Detailbereich in Schritt 3 **Infrastrukturserver** auf **Bearbeiten**.
2. Klicken Sie im Assistenten zum Einrichten des Infrastrukturserver auf der Seite **Netzwerkadressenserver** unter **Der Netzwerkadressenserver wird auf dem RAS-Server bereitgestellt**. auf **Durchsuchen**, um das zuvor abgerufene Zertifikat auszuwählen. Das Zertifikat muss einen Antragstellernamen enthalten, der sich vom internen Namen des RAS-Servers unterscheidet.

## **Windows 7-Clientcomputer**

Die Warnung wurde empfangen. Beim Aktivieren von Multisite dürfen die für DirectAccess-Clients konfigurierten Sicherheitsgruppen keine Windows 7-Computer enthalten. Wählen Sie eine Sicherheitsgruppe aus, die die Clients für die einzelnen Einstiegspunkte enthält, damit Clientcomputer mit Windows 7 in einer Bereitstellung mit mehreren Standorten unterstützt werden.

#### **Ursache**

In der vorhandenen DirectAccess-Bereitstellung wurde die Windows 7-Client Unterstützung aktiviert.

#### **Lösung**

DirectAccess erfordert mindestens eine Sicherheitsgruppe für alle Windows 8-Client Computer und eine Sicherheitsgruppe für Windows 7-Client Computer für jeden Einstiegspunkt. Jeder Clientcomputer sollte nur in eine Sicherheitsgruppe aufgenommen werden. Daher sollten Sie sicherstellen, dass die Sicherheitsgruppe für Windows 8-Clients nur Computer enthält, auf denen Windows 8 ausgeführt wird, und dass jeder Windows 7-Client Computer zu einer einzelnen dedizierten Sicherheitsgruppe für den relevanten Einstiegspunkt gehört und keine Windows 8-Clients gehört zu den Windows 7-Sicherheitsgruppen.

## **Active Directory-Standort**

Der Fehler wurde empfangen. Der Server < server\_name > ist keinem Active Directory Standort zugeordnet.

#### **Ursache**

Von DirectAccess konnte der Active Directory-Standort nicht ermittelt werden. In der Konsole für Active Directory-Standorte und -Dienste können Sie die verschiedenen Subnetze für Ihr Netzwerk konfigurieren und die einzelnen Subnetze dem relevanten Active Directory-Standort zuweisen. Dieser Fehler kann auftreten, wenn die IP-Adresse

des RAS-Servers zu keinem der Subnetze gehört oder wenn das Subnetz, zu dem die IP-Adresse gehört, keinem Active Directory-Standort zugeordnet ist.

## Lösung

Überprüfen Sie, ob dies das Problem ist, indem Sie den Befehl `nlttest /dsgetsite` auf dem RAS-Server ausführen. Ist dies das Problem, wird vom Befehl ERROR\_NO\_SITENAME zurückgegeben. Stellen Sie zum Beheben des Problems sicher, dass auf dem Domänencontroller ein Subnetz vorhanden ist, das die interne Server-IP-Adresse enthält und einem Active Directory-Standort zugeordnet ist.

## Server-GPO-Einstellungen werden gespeichert

Der **Fehler wurde empfangen**. Fehler beim Speichern der Remote Zugriffs Einstellungen auf dem GPO-< GPO\_name >.

## Ursache

Änderungen am Server-GPO konnten aufgrund von Konnektivitätsproblemen oder einer Freigabe Verletzung in der Datei "Registry. Pol" nicht gespeichert werden, z. B. Wenn ein anderer Benutzer die Datei gesperrt hat.

## Lösung

Stellen Sie sicher, dass Konnektivität zwischen dem RAS-Server und dem Domänencontroller besteht. Besteht Konnektivität, überprüfen Sie auf dem Domänencontroller, ob die Datei %amp;quot;registry.pol%amp;quot; durch einen anderen Benutzer gesperrt ist, und beenden Sie ggf. diese Benutzersitzung, um die Datei zu entsperren.

## Interner Fehler.

Der **Fehler wurde empfangen**. Interner Fehler.

## Ursache

Dieser Fehler wird möglicherweise durch eine unerwartete Konfiguration der Einstiegspunkttabelle im Client-Gruppenrichtlinienobjekt verursacht. Dies kann passieren, wenn der Administrator DirectAccess-Client-Cmdlets zum Bearbeiten der Einstiegspunkttabelle im Client-Gruppenrichtlinienobjekt verwendet.

## Lösung

Überprüfen Sie die Konfiguration der Einstiegspunkttabelle in allen Client-Gruppenrichtlinienobjekten, und beheben Sie alle Inkonsistenzen in der Konfiguration für mehrere Standorte zwischen den verschiedenen Instanzen der Client-Gruppenrichtlinienobjekte und der DirectAccess-Konfiguration. Verwenden Sie das `Get-DaEntryPointTableItem`-Cmdlet mit dem Namen des Client-Gruppenrichtlinienobjekts, um die Einstiegspunkttabelle für den Client abzurufen. Verwenden Sie das `Get-NetIPHttpsConfiguration`-Cmdlet, um alle IP-HTTPS-Profil für alle Einstiegspunkte abzurufen.

Weitere Informationen finden Sie unter [DirectAccess-Client-Cmdlets in Windows PowerShell](#).

# Beheben von Problemen beim Hinzufügen von Einstiegspunkten

09.04.2020 • 19 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zum Beheben von Problemen mit dem Befehl `Add-DAEntryPoint`. Um sicherzustellen, dass sich der angezeigte Fehler auf das Hinzufügen eines Einstiegspunkts bezieht, prüfen Sie, ob im Windows-Ereignisprotokoll die Ereignis-ID 10067 aufgeführt wird.

## Fehlender RemoteAccessServer-Parameter

Der **Fehler wurde empfangen**. Sie müssen einen Wert für den Parameter "remoteaccessserver" angeben.

### Ursache

Wenn Sie einer Bereitstellung für mehrere Standorte einen neuen Einstiegspunkt hinzufügen, müssen Sie den Parameter *RemoteAccessServer* angeben. Hierbei handelt es sich um den Namen des Servers, den Sie als neuen Einstiegspunkt hinzufügen möchten.

### Lösung

Führen Sie den Befehl aus, und geben Sie für den Parameter *RemoteAccessServer* den Namen des Servers an, der als Einstiegspunkt hinzugefügt werden soll.

## Nicht konfigurierter Remotezugriff

Der **Fehler wurde empfangen**. Der Remote Zugriff ist auf < server\_name > nicht konfiguriert. Geben Sie den Namen eines Servers an, der zu einer Bereitstellung für mehrere Standorte gehört.

### Ursache

Remotezugriff ist auf dem Computer, der durch den Parameter *ComputerName* definiert wird, oder auf dem Computer, auf dem Sie den Befehl ausführen, nicht konfiguriert.

Wenn Sie einer Bereitstellung für mehrere Standorte einen neuen Einstiegspunkt hinzufügen, müssen Sie zwei Parameter angeben: *ComputerName* und *RemoteAccessServer*. *ComputerName* ist der Name eines Servers, der bereits zu der Bereitstellung für mehrere Standorte gehört. *RemoteAccessServer* ist der Name des Servers, den Sie als neuen Einstiegspunkt hinzufügen möchten. Bei der Ausführung auf einem Computer, der bereits zu der Bereitstellung für mehrere Standorte gehört, ist der Parameter `&quot;ComputerName&quot;` nicht erforderlich.

### Lösung

Führen Sie den Befehl aus, und geben Sie für den Parameter *ComputerName* den Namen des Servers an, der bereits so konfiguriert ist, dass er zu der Bereitstellung für mehrere Standorte gehört. Alternativ können Sie den Befehl auf einem Computer ausführen, der zu der Bereitstellung für mehrere Standorte gehört.

## Nicht aktivierte Funktionen für mehrere Standorte

Der **Fehler wurde empfangen**. Sie müssen eine Bereitstellung für mehrere Standorte aktivieren, bevor Sie diesen Vorgang ausführen. Verwenden Sie hierzu das Cmdlet `Enable-DAMultiSite`.

## Ursache

Die Funktionen für mehrere Standorte sind auf dem Server, der durch den Parameter *ComputerName* angegeben wird, nicht aktiviert. Sie müssen die Funktionen für mehrere Standorte aktivieren, um einer Remotezugriffsbereitstellung einen neuen Einstiegspunkt hinzuzufügen.

## Lösung

Verwenden Sie das Cmdlet `Enable-DaMultiSite` zum Aktivieren der Funktionen für mehrere Standorte. Weitere Informationen finden Sie unter Bereitstellen des [Remote Zugriffs für mehrere Standorte](#).

# Probleme mit IPv6-Präfixen

## • Problem 1

Der Fehler wurde empfangen. IPv6 wird im internen Netzwerk bereitgestellt, aber Sie haben kein IPv6-Client Präfix angegeben.

## Ursache

IPv6 wird im Unternehmensnetzwerk bereitgestellt, und ein IP-HTTPS-Präfix ist erforderlich. Es wurde jedoch für den neuen Einstiegspunkt kein Präfix im Parameter *ClientIPv6Prefix* angegeben.

## Lösung

1. Weisen Sie dem neuen Einstiegspunkt ein eindeutiges IP-HTTPS-Präfix zu, und stellen Sie sicher, dass Pakete, die an eine IP-Adresse unter diesem Präfix adressiert sind, an den Server weitergeleitet werden, den Sie hinzufügen.
2. Führen Sie das Cmdlet `Add-DAEntryPoint` aus, und geben Sie im Parameter *ClientIPv6Prefix* das IP-HTTPS-Präfix an.

## • Problem 2

Der Fehler wurde empfangen. Das IPv6-Präfix des Clients wird bereits von einem anderen Einstiegspunkt verwendet. Geben Sie einen anderen Wert an.

## Ursache

Das im Parameter *ClientIPv6Prefix* angegebene IP-HTTPS-Präfix wird bereits von einem anderen Einstiegspunkt verwendet.

## Lösung

1. Weisen Sie dem neuen Einstiegspunkt ein eindeutiges IP-HTTPS-Präfix zu, und stellen Sie sicher, dass Pakete, die an eine IP-Adresse unter diesem Präfix adressiert sind, an den Server weitergeleitet werden, den Sie hinzufügen.
2. Führen Sie das Cmdlet `Add-DAEntryPoint` aus, und geben Sie im Parameter *ClientIPv6Prefix* das IP-HTTPS-Präfix an.

# ConnectTo-Adresse

Der Fehler wurde empfangen. Die Adresse (< connect\_to\_address >), mit der DirectAccess-Clients auf dem remoteaccess-Server eine Verbindung herstellen, ist identisch mit der Adresse des Netzwerkadressenservers. Geben Sie einen anderen Wert an.

## Ursache

Die ConnectTo-Adresse ist identisch mit der Adresse des Netzwerkadressenservers.

## Lösung

Die ConnectTo-Adresse muss über das Internet aufgelöst werden können, damit Clientcomputer eine Verbindung über IP-HTTPS herstellen können. Die Adresse des Netzwerkadressenservers muss über das Unternehmensnetzwerk aufgelöst werden können, nicht jedoch über das Internet. Stellen Sie sicher, dass die Adresse des Netzwerkadressenservers nicht identisch mit der ConnectTo-Adresse ist. Wählen Sie andere Adressen aus, und versuchen Sie es erneut.

## DirectAccess oder VPN bereits installiert

Der **Fehler wurde empfangen**. Auf dem Server wurde eine VPN-Installation erkannt, <server\_name>. Geben Sie einen alternativen Server an, auf dem kein Remotezugriff installiert ist, oder entfernen Sie die VPN-Konfiguration vom Server.

Oder

Der Remote Zugriff ist auf dem Server <server\_name> bereits installiert. Geben Sie einen alternativen Server an, auf dem DirectAccess nicht ausgeführt wird, oder entfernen Sie die vorhandene DirectAccess-Konfiguration vom Server.

## Ursache

DirectAccess oder VPN ist bereits auf dem neuen Einstiegspunkt konfiguriert. Sie können einer Bereitstellung für mehrere Standorte keinen konfigurierten Einstiegspunkt hinzufügen.

## Lösung

Um einem Server eine Bereitstellung für mehrere Standorte hinzuzufügen, müssen Sie die Remotezugriffsrolle auf dem Server installieren. DirectAccess und VPN dürfen jedoch nicht konfiguriert sein.

Führen Sie den Befehl aus, und stellen Sie sicher, dass für den von Ihnen im Parameter *RemoteAccessServer* angegebenen Server DirectAccess und VPN nicht konfiguriert sind.

## IPsec-Stammzertifikat

Der **Fehler wurde empfangen**. Das konfigurierte IPSec-Stamm Zertifikat kann nicht auf dem Server <server\_name> gefunden werden.

## Ursache

Auf dem Server, den Sie zur Bereitstellung hinzufügen möchten, konnte das Zertifikat der Stamm- oder Zwischenzertifizierungsstelle, von der Computerzertifikate ausgestellt werden, nicht gefunden werden.

## Lösung

Klicken Sie in der Remotezugriffs-Verwaltungskonsole in Schritt 2 **RAS-Server** auf **Bearbeiten**. Das Zertifikat, das sich auf der Seite **Authentifizierung** unter **Computerzertifikate verwenden** befindet, muss gültig sein. Wenn das Zertifikat gültig ist, stellen Sie sicher, dass es sich auf dem Server, den Sie hinzufügen möchten, unter der vertrauenswürdigen Stammzertifizierungsstelle befindet, und versuchen Sie es erneut.

### NOTE

Das Zertifikat muss das gleiche Zertifikat mit dem gleichen Fingerabdruck sein.

Ist das Zertifikat ungültig, wählen Sie ein gültiges Zertifikat aus, das auf allen RAS-Servern als vertrauenswürdige Stammzertifizierungsstelle konfiguriert ist.

# Vermischen von IPv6- und IPv4-Einstiegspunkten

Bei der ersten Installation von DirectAccess wird der interne Netzwerkadapter überprüft. Dies dient der Feststellung, ob im Netzwerk ausschließlich IPv4-Adressen vorhanden sind (reines IPv4-Netzwerk), IPv6- und IPv4-Adressen, oder ausschließlich IPv6-Adressen (reines IPv6-Netzwerk). Diese Informationen werden zur Bestimmung des Bereitstellungstyps verwendet (nur IPv4, IPv6 und IPv4 oder nur IPv6).

- **Problem 1**

Die **Warnung wurde empfangen**. Der hinzugefügte RAS-Server wird mit IPv4-und IPv6-Adressen konfiguriert. Bei dieser Bereitstellung handelt es sich um eine reine IPv4-Bereitstellung, und die IPv6-Adressen werden von Remotezugriff ignoriert.

## Ursache

Als diese Bereitstellung zum ersten Mal installiert wurde, wurde das interne Netzwerk als reines IPv4-Netzwerk erkannt. In einer Bereitstellung für mehrere Standorte wird davon ausgegangen, dass sich unterschiedliche Einstiegspunkte in unterschiedlichen Subnetzen mit unterschiedlichen Eigenschaften befinden. Daher kann die Bereitstellung, obwohl sie als reine IPv4-Bereitstellung konfiguriert ist, einen Einstiegspunkt enthalten, der sich in einem IPv6/IPv4-Subnetz befindet. Obwohl der Einstiegspunkt der Bereitstellung hinzugefügt wird, ignoriert DirectAccess die IPv6-Adressen, die in der internen Schnittstelle des neuen Einstiegs Punkts konfiguriert sind.

## Lösung

Wenn das gesamte interne Netzwerk mit IPv6- und IPv4-Adressen konfiguriert ist, ist es u. U. ratsam, zu einer IPv6/IPv4-Bereitstellung zu wechseln, um die Vorteile der IPv6-Technologie nutzen zu können. Weitere Informationen finden Sie unter "Übergang von einem reinen IPv4 zu einem IPv6 + IPv4-Unternehmensnetzwerk" in [Schritt 3: Planen der Bereitstellung für mehrere Standorte](#).

- **Problem 2**

Der **Fehler wurde empfangen**. Die internen Netzwerkadapter der Remote Zugriffs Server in dieser Bereitstellung für mehrere Standorte werden mit IPv4-Adressen konfiguriert. Der hinzugefügte Einstiegspunkt muss auch mit einer IPv4-Adresse im internen Netzwerkadapter konfiguriert werden.

## Ursache

Als diese Bereitstellung zum ersten Mal installiert wurde, wurde das interne Netzwerk als reines IPv4-Netzwerk erkannt. Von Remotezugriff wurde erkannt, dass der Einstiegspunkt, den Sie hinzufügen möchten, in seinem internen Netzwerk ausschließlich mit IPv6-Adressen konfiguriert ist. Dies ist in einer reinen IPv4-Bereitstellung nicht zulässig.

## Lösung

Wenn das gesamte Netzwerk bereits mit IPv6-Adressen konfiguriert ist, sollten Sie zu einer IPv6/IPv4-Bereitstellung oder einer reinen IPv6-Bereitstellung wechseln. Weitere Informationen finden Sie unter "Planen des Übergangs zu IPv6 bei Bereitstellung des Remote Zugriffs für mehrere Standorte".

- **Problem 3**

Der **Fehler wurde empfangen**. Dieser Einstiegspunkt befindet sich in einem IPv4-Netzwerk, aber vorherige Einstiegspunkte befinden sich in einem IPv6-Netzwerk. Verbinden Sie diesen Einstiegspunkt mit dem IPv6-Netzwerk, bevor Sie ihn zu derselben Bereitstellung für mehrere Standorte hinzufügen.

## Ursache

Als diese Bereitstellung zum ersten Mal installiert wurde, wurde das interne Netzwerk als IPv6/IPv4-Netzwerk oder als reines IPv6-Netzwerk erkannt. Es wurde erkannt, dass im internen Netzwerk des neuen

Einstiegspunkts, den Sie hinzufügen möchten, ausschließlich IPv4-Adressen konfiguriert sind. Dies ist in IPv6/IPv4-Bereitstellungen bzw. in reinen IPv6-Bereitstellungen nicht erlaubt.

### Lösung

Konfigurieren Sie den neuen Einstiegspunkt mit IPv6-Adressen, und fügen Sie ihn dann der Bereitstellung für mehrere Standorte hinzu.

- **Problem 4**

Die **Warnung wurde empfangen**. Der interne Netzwerkadapter auf dem Remote Zugriffs Server ist nicht mit einer IPv4-Adresse konfiguriert. DNS64 und NAT64 werden auf diesem Server nicht konfiguriert. DirectAccess-Clients können nur auf interne IPv6-Server zugreifen.

### Ursache

Als diese Bereitstellung zum ersten Mal installiert wurde, wurde das interne Netzwerk als IPv6/IPv4-Netzwerk erkannt. In diesem Bereitstellungsmodus werden DNS64 und NAT64 aktiviert, damit Clientcomputer auf Computer im internen Netzwerk zugreifen können, die ausschließlich mit IPv4-Adressen konfiguriert sind.

Beim Hinzufügen des neuen Einstiegspunkts wurde von Remotezugriff erkannt, dass die interne Schnittstelle auf dem neuen Computer ausschließlich über IPv6-Adressen verfügt. Zum Konfigurieren von DNS64 und NAT64 ist eine IPv4-Adresse erforderlich, um die Pakete vom RAS-Server an den reinen IPv4-Computer weiterzuleiten. Da auf dem neuen Computer keine solche IP-Adresse vorhanden ist, werden NAT64 und DNS64 auf dem RAS-Server nicht konfiguriert. Daher können Clientcomputer, die mithilfe von DirectAccess über diesen Einstiegspunkt auf das Unternehmensnetzwerk zugreifen, nicht auf reine IPv4-Server im internen Netzwerk zugreifen. Informationen zum Übergang zu einem IPv6 + IPv4-Netzwerk oder zu einem reinen IPv6-Netzwerk finden Sie unter "Planen des Übergangs zu IPv6 bei Bereitstellung des Remote Zugriffs für mehrere Standorte".

### Lösung

Fügen Sie dem neuen RAS-Server eine IPv4-Adresse hinzu, um sicherzustellen, dass DNS64 und NAT64 funktionieren.

## Domänenbezogene Probleme mit ServerGpoName

- **Problem 1**

Der **Fehler wurde empfangen**. Die im servergponame-Parameter angegebene Domäne < server\_GPO > ist nicht vorhanden. Geben Sie stattdessen die Domänen < domain\_name > an.

### Ursache

Der Teil mit dem Domänenamen des vom Administrator gesendeten Namens des Server-Gruppenrichtlinienobjekts (Group Policy Object, GPO) konnte nicht gefunden werden.

### Lösung

Stellen Sie sicher, dass Sie den Domänenamen richtig eingegeben haben. Ist der Domänenname richtig, versuchen Sie es erneut mit dem vollqualifizierten Domänenamen (Fully Qualified Domain Name, FQDN).

- **Problem 2**

Der **Fehler wurde empfangen**. Das Server-GPO muss sich in der RAS-Server Domäne befinden. Geben Sie die Domänen < domain\_name > im servergponame-Parameter an.

### Ursache

Die Domäne des Server-GPO ist nicht identisch mit der Domäne, zu der der RAS-Server gehört.

## Lösung

Das Server-GPO sollte sich in der gleichen Domäne wie der RAS-Server befinden. Verwenden Sie den Domänennamen des Servers für das Server-GPO, und versuchen Sie es erneut.

## Split-Brain-DNS

Die **Warnung wurde empfangen**. Der NRPT-Eintrag für das DNS-Suffix < DNS\_suffix > enthält den öffentlichen Namen, der von Client Computern zum Herstellen einer Verbindung mit dem RAS-Server verwendet wird. Fügen Sie den Namen < connect\_to\_address > als Ausnahme in der NRPT hinzu.

## Ursache

Sie verwenden Split-Brain-DNS. Damit Clients eine Verbindung über IP-HTTPS herstellen können, sollten Sie sicherstellen, dass die ausgewählte ConnectTo-Adresse in den NRPT-Regeln ausgenommen ist.

## Lösung

Stellen Sie in einer Bereitstellung für mehrere Standorte sicher, dass alle Adressen der verschiedenen Einstiegspunkte, mit denen eine Verbindung hergestellt wird, von den NRPT-Regeln ausgenommen sind.

So erstellen Sie eine Ausnahme für eine Adresse in den NRPT-Regeln:

1. Klicken Sie in der Remotezugriffs-Verwaltungskonsole in Schritt 3 **Infrastrukturserver** auf **Bearbeiten**.
2. Doppelklicken Sie im Assistenten zum Einrichten des Infrastrukturservers auf der Seite **DNS** auf die Tabelle, um ein neues Namenssuffix einzugeben.
3. Geben Sie im Dialogfeld **DNS-Serveradressen** unter %&quot;DNS-Suffix%&quot; die ConnectTo-Adresse des Einstiegspunkts ein, und klicken Sie auf **Übernehmen**.

Wenn Sie Namenssuffixe hinzufügen, ohne eine Serveradresse anzugeben, wird das Suffix als NRPT-Ausnahme behandelt.

## Speichern der Server-GPO-Einstellungen

Der **Fehler wurde empfangen**. Fehler beim Speichern der Remote Zugriffs Einstellungen auf dem GPO-< GPO\_name >.

Informationen zum Beheben dieses Fehlers finden Sie unter Speichern von Server-GPO-Einstellungen unter Problembehandlung beim [Aktivieren von Multisite](#).

## GPO-Aktualisierungen können nicht angewendet werden

Die **Warnung wurde empfangen**. GPO-Aktualisierungen können nicht auf < server\_name > angewendet werden. Die Änderungen werden erst nach der nächsten Richtlinienaktualisierung wirksam.

## Ursache

Beim Aktualisieren der Richtlinien auf dem angegebenen Computer ist ein Fehler aufgetreten. Daher werden vorgenommene Änderungen erst nach der nächsten Richtlinienaktualisierung wirksam.

## Lösung

Führen Sie auf dem angegebenen Computer `gpupdate /force` aus, um eine Richtlinienaktualisierung zu erzwingen.

# Problembehandlung für Einstellungen für Einstiegspunkte und Domänencontroller

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zum Beheben von Problemen mit dem Befehl `Set-DaEntryPointDC`. Überprüfen Sie, ob das Windows-Ereignisprotokoll ein Ereignis mit der ID 10065 enthält, um sicherzustellen, dass der Fehler mit den Einstellungen für Einstiegspunkte und Domänencontroller zusammenhängt.

## Server-GPO-Einstellungen werden gespeichert

Der **Fehler wurde empfangen**. Fehler beim Speichern der Remote Zugriffs Einstellungen auf dem GPO-< GPO\_name >.

Informationen zum Beheben dieses Fehlers finden Sie unter Speichern der Server-GPO-Einstellungen.

## Nicht konfigurierter Remotezugriff

Der **Fehler wurde empfangen**. Der Remote Zugriff ist auf < server\_name > nicht konfiguriert. Geben Sie den Namen eines Servers an, der zu einer Bereitstellung für mehrere Standorte gehört.

Oder

Der Remote Zugriff ist auf dem Server < server\_name > nicht konfiguriert. Geben Sie einen Computer an, auf dem DirectAccess aktiviert ist.

### Ursache

Remotezugriff ist auf dem mit dem *ComputerName*-Parameter angegebenen Computer nicht konfiguriert.

Das Cmdlet `Set-DaEntryPointDC` ist nur auf Servern verfügbar, die zu einer konfigurierten Bereitstellung für mehrere Standorte gehören.

### Lösung

Führen Sie den Befehl aus, und geben Sie im *ComputerName*-Parameter den Namen des Servers an, der bereits als Teil der Bereitstellung für mehrere Standorte konfiguriert ist.

## Bereitstellung für mehrere Standorte ist nicht aktiviert

Der **Fehler wurde empfangen**. Sie müssen eine Bereitstellung für mehrere Standorte aktivieren, bevor Sie diesen Vorgang ausführen. Verwenden Sie hierzu das Cmdlet `Enable-DAMultisite`.

### Ursache

Die Funktionen für mehrere Standorte sind auf dem Server, der durch den Parameter *ComputerName* angegeben wird, nicht aktiviert.

Das Cmdlet `Set-DaEntryPointDC` ist nur auf Servern verfügbar, die zu einer konfigurierten Bereitstellung für mehrere Standorte gehören.

### Lösung

Führen Sie den Befehl aus, und geben Sie im *ComputerName*-Parameter den Namen des Servers an, der bereits als Teil der Bereitstellung für mehrere Standorte konfiguriert ist.

## Einstiegspunkt und Domänencontroller wurden nicht im Cmdlet angegeben

Das Cmdlet `Set-DaEntryPointDC` bietet Ihnen die Möglichkeit, den zugeordneten Domänencontroller für verschiedene Einstiegspunkte zu ändern, z. B. wenn ein bestimmter Domänencontroller nicht mehr verfügbar ist. Sie können einen spezifischen Einstiegspunkt zur Verwendung eines anderen Domänencontrollers aktualisieren oder alle Einstiegspunkte mit einem bestimmten Domänencontroller zur Verwendung eines neuen Domänencontrollers aktualisieren. In ersten Fall sollten Sie den zu aktualisierenden Einstiegspunkt mit dem *EntryPointName*-Parameter angeben. In zweiten Fall sollten Sie den zu ersetzenen Domänencontroller mit dem *ExistingDC*-Parameter angeben. Sie können nur einen dieser Parameter angeben.

Der **Fehler wurde empfangen**. Es wurden keine erforderlichen Parameter angegeben. Geben Sie einen Einstiegspunktnamen oder den Namen eines vorhandenen Domänencontrollers an.

Oder

Für das Cmdlet `Set-DaEntryPointDC` fehlen alle erforderlichen Parameter.

### Ursache

Die Parameter *EntryPointName* oder *ExistingDC* wurden nicht angegeben oder es wurden beide Parameter für das Cmdlet `Set-DaEntryPointDC` angegeben.

### Lösung

Führen Sie den Befehl aus, und geben Sie dabei entweder den *EntryPointName*-Parameter oder den *ExistingDC*-Parameter an.

## Domänencontroller wurde nicht gefunden

Der **Fehler wurde empfangen**. Ein neuer Domänen Controller kann nicht automatisch gefunden werden. Versuchen Sie es später noch einmal, oder überprüfen Sie die Einstellungen des Domänencontrollers.

### Ursache

Der mit dem *ComputerName*-Parameter angegebene Computer ist nicht über RPC erreichbar, oder die Domäne enthält keine verfügbaren beschreibbaren Domänencontroller.

### Lösung

Stellen Sie sicher, dass der Remotecomputer über RPC erreichbar und ein beschreibbarer Domänencontroller für die Domäne verfügbar ist. Falls ein beschreibbarer Domänencontroller für die Domäne verfügbar ist, können Sie seinen Namen auch explizit mit dem *NewDC*-Parameter angeben.

## Es konnte keine Verbindung mit dem Domänencontroller hergestellt werden

- **Problem 1**

Der **Fehler wurde empfangen**. Der Domänen Controller < domain\_controller > kann nicht erreicht werden. Überprüfen Sie die Netzwerkkonnektivität und die Serververfügbarkeit.

### Ursache

Der Domänencontroller ist nicht erreichbar. Dieses Problem tritt nur auf, wenn der Administrator mit den

Parametern *NewDC* oder *ExistingDC* einen Domänencontroller angibt.

### Lösung

Stellen Sie sicher, dass der Name des Domänencontrollers richtig geschrieben ist. Falls Sie einen Kurznamen als Namen angegeben haben, verwenden Sie den vollqualifizierten Domänennamen (FQDN), und versuchen Sie es noch einmal.

- **Problem 2**

Der Fehler wurde empfangen. Der Domänen Controller < domain\_controller > kann nicht kontaktiert werden.

### Ursache

Möglicherweise liegt ein Netzwerkproblem vor, aufgrund dessen der mit dem *NewDC*-Parameter angegebene Domänencontroller oder ein anderer vorhandener Domänencontroller in der Konfiguration nicht erreicht werden kann.

### Lösung

Stellen Sie sicher, dass der Name des Domänencontrollers richtig geschrieben ist, dass er aktiv und beschreibbar ist und eine Vertrauensstellung zwischen dem Domänencontroller und der Domäne besteht.

- **Problem 3**

Der Fehler wurde empfangen. Der Domänen Controller < domain\_controller > für %2! s! nicht erreicht werden.

### Ursache

Um die Einheitlichkeit der Konfiguration in einer Bereitstellung für mehrere Standorte zu wahren, müssen Sie sicherstellen, dass jedes GPO von einem einzigen Domänencontroller verwaltet wird. Wenn der Domänen Controller, der das Server-Gruppenrichtlinien Objekt eines Einstiegs Punkts verwaltet, nicht verfügbar ist, können die RAS-Konfigurationseinstellungen nicht gelesen oder geändert werden.

### Lösung

Befolgen Sie das Verfahren "so ändern Sie den Domänen Controller, der Server-Gruppenrichtlinien Objekte verwaltet" in [2.4. Konfigurieren Sie GPOs](#).

- **Problem 4**

Der Fehler wurde empfangen. Der primäre Domänen Controller in der Domänen < domain\_name > kann nicht erreicht werden.

### Ursache

Um die Einheitlichkeit der Konfiguration in einer Bereitstellung für mehrere Standorte zu wahren, müssen Sie sicherstellen, dass jedes GPO von einem einzigen Domänencontroller verwaltet wird. Client-GPOs werden auf dem primären Domänencontroller verwaltet. Wenn der primäre Domänencontroller nicht verfügbar ist, können die RAS-Konfigurationseinstellungen nicht gelesen oder geändert werden.

### Lösung

Befolgen Sie das Verfahren "So übertragen Sie die PDC-Emulatorrolle" in [2.4. Konfigurieren Sie GPOs](#).

## Schreibgeschützter Domänencontroller

Der Fehler wurde empfangen. Der Domänen Controller < domain\_controller > schreibgeschützt ist. Geben Sie einen Domänencontroller an, der nicht schreibgeschützt ist.

## **Ursache**

Der mit dem *NewDC*-Parameter angegebene Domänencontroller ist schreibgeschützt.

## **Lösung**

Bei der Verwendung von `Set-DAEntryPointDC` wird der *NewDC*-Parameter zum Aktualisieren des zugeordneten Domänencontrollers eines bestimmten Einstiegspunkts oder zum Aktualisieren aller zugeordneten Einstiegspunkte eines Domänencontrollers verwendet. Der neue Domänencontroller muss daher beschreibbar sein. Geben Sie einen beschreibbaren Domänencontroller im *NewDC*-Parameter an, und versuchen Sie es noch einmal.

# **GPO kann nicht abgerufen werden**

- **Problem 1**

**Der Fehler wurde empfangen.** Die GPO-< GPO\_name > auf dem Domänen Controller < previous\_domain\_controller > nicht vom Domänen Controller < replacement\_domain\_controller > abgerufen werden kann, da Sie sich nicht in derselben Domäne befinden.

## **Ursache**

Der RAS-Server und der Domänencontroller befinden sich nicht in derselben Domäne. Daher kann das GPO nicht abgerufen werden.

## **Lösung**

Falls Sie versucht haben, einen bestimmten Einstiegspunkt zu aktualisieren, vergewissern Sie sich, dass sich der neue Domänencontroller in derselben Domäne befindet wie der Einstiegspunktserver. Falls Sie versucht haben, einen bestimmten Domänencontroller zu aktualisieren, vergewissern Sie sich, dass sich der neue Domänencontroller in derselben Domäne befindet wie der, den Sie ersetzen möchten.

- **Problem 2**

**Der Fehler wurde empfangen.** Die GPO-< GPO\_name > auf dem Domänen Controller < previous\_domain\_controller > nicht vom Domänen Controller < replacement\_domain\_controller > abgerufen werden. Warten Sie, bis die Domänenreplikation abgeschlossen ist, und wiederholen Sie den Vorgang.

## **Ursache**

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, das Server-GPO vom neuen Domänencontroller zu lesen. Das GPO wird jedoch nicht auf dem neuen Domänencontroller gefunden, weil es noch nicht repliziert wurde.

## **Lösung**

Das Server-GPO ist nicht auf dem neuen Domänencontroller vorhanden. Stellen Sie sicher, dass die GPOs erfolgreich zum neuen Domänencontroller repliziert wurden, und versuchen Sie es noch einmal.

- **Problem 3**

**Der Fehler wurde empfangen.** Sie verfügen nicht über die erforderlichen Berechtigungen für den Zugriff auf GPO-< GPO\_name >.

## **Ursache**

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, das Server-GPO vom neuen Domänencontroller zu lesen. Das GPO kann jedoch nicht vom neuen Domänencontroller gelesen werden, weil Sie nicht über die entsprechenden Berechtigungen verfügen.

## Lösung

Das GPO ist auf dem Domänencontroller vorhanden, kann aber nicht gelesen werden. Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, und versuchen Sie es noch einmal.

## Einstiegspunkt ist nicht Teil der Bereitstellung für mehrere Standorte

Der **Fehler wurde empfangen**. Der Einstiegspunkt < entry\_point\_name > ist nicht Teil der Bereitstellung für mehrere Standorte. Geben Sie einen anderen Wert an.

### Ursache

Der angegebene Einstiegspunktname wurde nicht gefunden.

### Lösung

Stellen Sie sicher, dass der Name des Einstiegspunkts richtig geschrieben ist und GPOs zu den erforderlichen Domänencontrollern repliziert wurden, und versuchen Sie es noch einmal. Verwenden Sie `Get-DAEntryPointDC`, um den zugewiesenen Domänencontroller für jeden Einstiegspunkt anzuzeigen.

## Einstellungen des RAS-Servers

- **Problem 1**

Der **Fehler wurde empfangen**. Server < server\_name > im Einstiegspunkt, < entry\_point\_name > nicht darauf zugegriffen werden kann.

### Ursache

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, den Domänencontroller für den Einstiegspunkt von allen relevanten RAS-Servern zu lesen und zu schreiben. Das Cmdlet konnte die Daten von mindestens einem RAS-Server nicht lesen.

### Lösung

Stellen Sie sicher, dass alle relevanten RAS-Server aktiv sind und Sie auf allen Servern über lokale Administratorberechtigungen verfügen, und versuchen Sie es noch einmal.

- **Problem 2**

Der **Fehler wurde empfangen**. Die Einstellungen können nicht in der Registrierung auf dem Server < server\_name > im Einstiegspunkt < entry\_point\_name > gespeichert werden.

### Ursache

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, den Domänencontroller für den Einstiegspunkt von allen relevanten RAS-Servern zu lesen und zu schreiben. Das Cmdlet konnte die Daten auf mindestens einen RAS-Server nicht schreiben.

### Lösung

Stellen Sie sicher, dass alle relevanten RAS-Server aktiv sind und Sie auf allen Servern über lokale Administratorberechtigungen verfügen, und versuchen Sie es noch einmal.

- **Problem 3**

Der **Fehler wurde empfangen**. GPO-Aktualisierungen können nicht auf < server\_name > angewendet werden. Die Änderungen werden erst nach der nächsten Richtlinienaktualisierung wirksam.

### Ursache

Bei der Verwendung des Cmdlets `Set-DAEntryPointDC` ist der angegebene *ComputerName*-Parameter ein RAS-Server an einem anderen Einstiegspunkt als dem, der der Bereitstellung für mehrere Standorte zuletzt hinzugefügt wurde.

### Lösung

Alle Server, die nicht aktualisiert wurden, können mithilfe des **Konfigurationsstatus** im DASHBOARD der Remotezugriffs-Verwaltungskonsole angezeigt werden. Dieser Fehler verursacht keine Funktionsprobleme. Sie können jedoch auf allen nicht aktualisierten Servern `gpupdate /force` ausführen, damit der Konfigurationsstatus sofort aktualisiert wird.

## Problem bei der Auflösung des vollqualifizierten Domänennamens (FQDN)

Der **Fehler wurde empfangen**. Server <server\_name> im Einstiegspunkt, <entry\_point\_name> nicht darauf zugegriffen werden kann.

### Ursache

Beim Abrufen der Liste zu ändernder DirectAccess-Server konnte das Cmdlet den vollqualifizierten Domänennamen (FQDN) eines der Server nicht aus der Computer-SID auflösen.

### Lösung

Der in der Fehlermeldung angegebene Einstiegspunkt ist einem Domänencontroller zugeordnet. Stellen Sie sicher, dass der Domänencontroller für den Einstiegspunkt verfügbar ist. Falls der Computer, zu dem die angegebene SID gehört, aus der Domäne entfernt wurde, ignorieren Sie die Meldung, und entfernen Sie den Server aus der Bereitstellung für mehrere Standorte.

## Keine zu aktualisierenden Einstiegspunkte vorhanden

Die **Warnung wurde empfangen**. Die Domänen Controller Einstellungen wurden nicht geändert. Wenn Ihrer Meinung nach Änderungen erforderlich sind, stellen Sie sicher, dass die Cmdlet-Parameter richtig konfiguriert sind und GPOs auf den erforderlichen Domänencontrollern repliziert werden.

### Ursache

Wenn das Cmdlet `Set-DaEntryPointDC` mit dem *ExistingDC*-Parameter aufgerufen wird, überprüft DirectAccess alle Einstiegspunkte und aktualisiert die Einstiegspunkte, die dem angegebenen Domänencontroller zugeordnet sind. Es ist jedoch kein Einstiegspunkt mit dem angegebenen *ExistingDC* vorhanden.

### Lösung

Verwenden Sie das Cmdlet `Get-DAEntryPointDC`, um eine Liste der Einstiegspunkte und der zugeordneten Domänencontroller anzuzeigen. Falls Änderungen vorgenommen wurden, stellen Sie sicher, dass die Cmdlet-Parameter richtig geschrieben sind und die GPOs zu den erforderlichen Domänencontrollern repliziert wurden, und versuchen Sie es noch einmal.

# Problembehandlung für Webtest-URLs

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zum Beheben von Problemen mit dem Befehl `Set-DAEntryPointDC`. Überprüfen Sie, ob das Windows-Ereignisprotokoll ein Ereignis mit der ID 10065 enthält, um sicherzustellen, dass der Fehler mit den Einstellungen für Einstiegspunkte und Domänencontroller zusammenhängt.

## Server-GPO-Einstellungen werden gespeichert

Der **Fehler wurde empfangen**. Fehler beim Speichern der Remote Zugriffs Einstellungen auf dem GPO-< GPO\_name >.

Informationen zum Beheben dieses Fehlers finden Sie unter Speichern der Server-GPO-Einstellungen.

## Nicht konfigurierter Remotezugriff

Der **Fehler wurde empfangen**. Der Remote Zugriff ist auf < server\_name > nicht konfiguriert. Geben Sie den Namen eines Servers an, der zu einer Bereitstellung für mehrere Standorte gehört.

Oder

Der Remote Zugriff ist auf dem Server < server\_name > nicht konfiguriert. Geben Sie einen Computer an, auf dem DirectAccess aktiviert ist.

### Ursache

Remotezugriff ist auf dem mit dem *ComputerName*-Parameter angegebenen Computer nicht konfiguriert.

Das Cmdlet `Set-DaEntryPointDC` ist nur auf Servern verfügbar, die zu einer konfigurierten Bereitstellung für mehrere Standorte gehören.

### Lösung

Führen Sie den Befehl aus, und geben Sie im *ComputerName*-Parameter den Namen des Servers an, der bereits als Teil der Bereitstellung für mehrere Standorte konfiguriert ist.

## Bereitstellung für mehrere Standorte ist nicht aktiviert

Der **Fehler wurde empfangen**. Sie müssen eine Bereitstellung für mehrere Standorte aktivieren, bevor Sie diesen Vorgang ausführen. Verwenden Sie hierzu das Cmdlet `Enable-DAMultiSite`.

### Ursache

Die Funktionen für mehrere Standorte sind auf dem Server, der durch den Parameter *ComputerName* angegeben wird, nicht aktiviert.

Das Cmdlet `Set-DaEntryPointDC` ist nur auf Servern verfügbar, die zu einer konfigurierten Bereitstellung für mehrere Standorte gehören.

### Lösung

Führen Sie den Befehl aus, und geben Sie im *ComputerName*-Parameter den Namen des Servers an, der bereits als

Teil der Bereitstellung für mehrere Standorte konfiguriert ist.

## Einstiegspunkt und Domänencontroller wurden nicht im Cmdlet angegeben

Das Cmdlet `Set-DaEntryPointDC` bietet Ihnen die Möglichkeit, den zugeordneten Domänencontroller für verschiedene Einstiegspunkte zu ändern, z. B. wenn ein bestimmter Domänencontroller nicht mehr verfügbar ist. Sie können einen spezifischen Einstiegspunkt zur Verwendung eines anderen Domänencontrollers aktualisieren oder alle Einstiegspunkte mit einem bestimmten Domänencontroller zur Verwendung eines neuen Domänencontrollers aktualisieren. In ersten Fall sollten Sie den zu aktualisierenden Einstiegspunkt mit dem *EntryPointName*-Parameter angeben. In zweiten Fall sollten Sie den zu ersetzen Domänencontroller mit dem *ExistingDC*-Parameter angeben. Sie können nur einen dieser Parameter angeben.

Der **Fehler wurde empfangen**. Es wurden keine erforderlichen Parameter angegeben. Geben Sie einen Einstiegspunktnamen oder den Namen eines vorhandenen Domänencontrollers an.

Oder

Für das Cmdlet `Set-DaEntryPointDC` fehlen alle erforderlichen Parameter.

### Ursache

Die Parameter *EntryPointName* oder *ExistingDC* wurden nicht angegeben oder es wurden beide Parameter für das Cmdlet `Set-DaEntryPointDC` angegeben.

### Lösung

Führen Sie den Befehl aus, und geben Sie dabei entweder den *EntryPointName*-Parameter oder den *ExistingDC*-Parameter an.

## Domänencontroller wurde nicht gefunden

Der **Fehler wurde empfangen**. Ein neuer Domänen Controller kann nicht automatisch gefunden werden. Versuchen Sie es später noch einmal, oder überprüfen Sie die Einstellungen des Domänencontrollers.

### Ursache

Der mit dem *ComputerName*-Parameter angegebene Computer ist nicht über RPC erreichbar, oder die Domäne enthält keine verfügbaren beschreibbaren Domänencontroller.

### Lösung

Stellen Sie sicher, dass der Remotecomputer über RPC erreichbar und ein beschreibbarer Domänencontroller für die Domäne verfügbar ist. Falls ein beschreibbarer Domänencontroller für die Domäne verfügbar ist, können Sie seinen Namen auch explizit mit dem *NewDC*-Parameter angeben.

## Es konnte keine Verbindung mit dem Domänencontroller hergestellt werden

- **Problem 1**

Der **Fehler wurde empfangen**. Der Domänen Controller < domain\_controller > kann nicht erreicht werden. Überprüfen Sie die Netzwerkkonnektivität und die Serververfügbarkeit.

### Ursache

Der Domänencontroller ist nicht erreichbar. Dieses Problem tritt nur auf, wenn der Administrator mit den Parametern *NewDC* oder *ExistingDC* einen Domänencontroller angibt.

## Lösung

Stellen Sie sicher, dass der Name des Domänencontrollers richtig geschrieben ist. Falls Sie einen Kurznamen als Namen angegeben haben, verwenden Sie den vollqualifizierten Domänennamen (FQDN), und versuchen Sie es noch einmal.

- **Problem 2**

Der Fehler wurde empfangen. Der Domänen Controller < domain\_controller > kann nicht kontaktiert werden.

### Ursache

Möglicherweise liegt ein Netzwerkproblem vor, aufgrund dessen der mit dem *NewDC*-Parameter angegebene Domänencontroller oder ein anderer vorhandener Domänencontroller in der Konfiguration nicht erreicht werden kann.

### Lösung

Stellen Sie sicher, dass der Name des Domänencontrollers richtig geschrieben ist, dass er aktiv und beschreibbar ist und eine Vertrauensstellung zwischen dem Domänencontroller und der Domäne besteht.

- **Problem 3**

Der Fehler wurde empfangen. Der Domänen Controller < domain\_controller > für %2! s! nicht erreicht werden.

### Ursache

Um die Einheitlichkeit der Konfiguration in einer Bereitstellung für mehrere Standorte zu wahren, müssen Sie sicherstellen, dass jedes GPO von einem einzigen Domänencontroller verwaltet wird. Wenn der Domänen Controller, der das Server-Gruppenrichtlinien Objekt eines Einstiegs Punkts verwaltet, nicht verfügbar ist, können die RAS-Konfigurationseinstellungen nicht gelesen oder geändert werden.

### Lösung

Befolgen Sie das Verfahren "so ändern Sie den Domänen Controller, der Server-Gruppenrichtlinien Objekte verwaltet" in [2.4. Konfigurieren Sie GPOs](#).

- **Problem 4**

Der Fehler wurde empfangen. Der primäre Domänen Controller in der Domänen < domain\_name > kann nicht erreicht werden.

### Ursache

Um die Einheitlichkeit der Konfiguration in einer Bereitstellung für mehrere Standorte zu wahren, müssen Sie sicherstellen, dass jedes GPO von einem einzigen Domänencontroller verwaltet wird. Client-GPOs werden auf dem primären Domänencontroller verwaltet. Wenn der primäre Domänencontroller nicht verfügbar ist, können die RAS-Konfigurationseinstellungen nicht gelesen oder geändert werden.

### Lösung

Befolgen Sie das Verfahren "So übertragen Sie die PDC-Emulatorrolle" in [2.4. Konfigurieren Sie GPOs](#).

## Schreibgeschützter Domänencontroller

Der Fehler wurde empfangen. Der Domänen Controller < domain\_controller > schreibgeschützt ist. Geben Sie einen Domänencontroller an, der nicht schreibgeschützt ist.

### Ursache

Der mit dem *NewDC*-Parameter angegebene Domänencontroller ist schreibgeschützt.

## Lösung

Bei der Verwendung von `Set-DAEntryPointDC` wird der *NewDC*-Parameter zum Aktualisieren des zugeordneten Domänencontrollers eines bestimmten Einstiegspunkts oder zum Aktualisieren aller zugeordneten Einstiegspunkte eines Domänencontrollers verwendet. Der neue Domänencontroller muss daher beschreibbar sein. Geben Sie einen beschreibbaren Domänencontroller im *NewDC*-Parameter an, und versuchen Sie es noch einmal.

# GPO kann nicht abgerufen werden

- **Problem 1**

Der **Fehler wurde empfangen**. Die GPO-< GPO\_name > auf dem Domänen Controller < previous\_domain\_controller > nicht vom Domänen Controller < replacement\_domain\_controller > abgerufen werden kann, da Sie sich nicht in derselben Domäne befinden.

## Ursache

Der RAS-Server und der Domänencontroller befinden sich nicht in derselben Domäne. Daher kann das GPO nicht abgerufen werden.

## Lösung

Falls Sie versucht haben, einen bestimmten Einstiegspunkt zu aktualisieren, vergewissern Sie sich, dass sich der neue Domänencontroller in derselben Domäne befindet wie der Einstiegspunktserver. Falls Sie versucht haben, einen bestimmten Domänencontroller zu aktualisieren, vergewissern Sie sich, dass sich der neue Domänencontroller in derselben Domäne befindet wie der, den Sie ersetzen möchten.

- **Problem 2**

Der **Fehler wurde empfangen**. Die GPO-< GPO\_name > auf dem Domänen Controller < previous\_domain\_controller > nicht vom Domänen Controller < replacement\_domain\_controller > abgerufen werden. Warten Sie, bis die Domänenreplikation abgeschlossen ist, und wiederholen Sie den Vorgang.

## Ursache

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, das Server-GPO vom neuen Domänencontroller zu lesen. Das GPO wird jedoch nicht auf dem neuen Domänencontroller gefunden, weil es noch nicht repliziert wurde.

## Lösung

Das Server-GPO ist nicht auf dem neuen Domänencontroller vorhanden. Stellen Sie sicher, dass die GPOs erfolgreich zum neuen Domänencontroller repliziert wurden, und versuchen Sie es noch einmal.

- **Problem 3**

Der **Fehler wurde empfangen**. Sie verfügen nicht über die erforderlichen Berechtigungen für den Zugriff auf GPO-< GPO\_name >.

## Ursache

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, das Server-GPO vom neuen Domänencontroller zu lesen. Das GPO kann jedoch nicht vom neuen Domänencontroller gelesen werden, weil Sie nicht über die entsprechenden Berechtigungen verfügen.

## Lösung

Das GPO ist auf dem Domänencontroller vorhanden, kann aber nicht gelesen werden. Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, und versuchen Sie es noch einmal.

## Einstiegspunkt ist nicht Teil der Bereitstellung für mehrere Standorte

Der **Fehler wurde empfangen**. Der Einstiegspunkt < entry\_point\_name > ist nicht Teil der Bereitstellung für mehrere Standorte. Geben Sie einen anderen Wert an.

### Ursache

Der angegebene Einstiegspunktname wurde nicht gefunden.

### Lösung

Stellen Sie sicher, dass der Name des Einstiegspunkts richtig geschrieben ist und GPOs zu den erforderlichen Domänencontrollern repliziert wurden, und versuchen Sie es noch einmal. Verwenden Sie `Get-DAEntryPointDC`, um den zugewiesenen Domänencontroller für jeden Einstiegspunkt anzuzeigen.

## Einstellungen des RAS-Servers

- **Problem 1**

Der **Fehler wurde empfangen**. Server < server\_name > im Einstiegspunkt, < entry\_point\_name > nicht darauf zugegriffen werden kann.

### Ursache

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, den Domänencontroller für den Einstiegspunkt von allen relevanten RAS-Servern zu lesen und zu schreiben. Das Cmdlet konnte die Daten von mindestens einem RAS-Server nicht lesen.

### Lösung

Stellen Sie sicher, dass alle relevanten RAS-Server aktiv sind und Sie auf allen Servern über lokale Administratorberechtigungen verfügen, und versuchen Sie es noch einmal.

- **Problem 2**

Der **Fehler wurde empfangen**. Die Einstellungen können nicht in der Registrierung auf dem Server < server\_name > im Einstiegspunkt < entry\_point\_name > gespeichert werden.

### Ursache

Wenn Sie den Domänencontroller für einen Einstiegspunkt aktualisieren, versucht das Cmdlet, den Domänencontroller für den Einstiegspunkt von allen relevanten RAS-Servern zu lesen und zu schreiben. Das Cmdlet konnte die Daten auf mindestens einen RAS-Server nicht schreiben.

### Lösung

Stellen Sie sicher, dass alle relevanten RAS-Server aktiv sind und Sie auf allen Servern über lokale Administratorberechtigungen verfügen, und versuchen Sie es noch einmal.

- **Problem 3**

Der **Fehler wurde empfangen**. GPO-Aktualisierungen können nicht auf < server\_name > angewendet werden. Die Änderungen werden erst nach der nächsten Richtlinienaktualisierung wirksam.

### Ursache

Bei der Verwendung des Cmdlets `Set-DAEntryPointDC` ist der angegebene *ComputerName*-Parameter ein RAS-Server an einem anderen Einstiegspunkt als dem, der der Bereitstellung für mehrere Standorte zuletzt

hinzugefügt wurde.

## Lösung

Alle Server, die nicht aktualisiert wurden, können mithilfe des **Konfigurationsstatus** im DASHBOARD der Remotezugriffs-Verwaltungskonsole angezeigt werden. Dieser Fehler verursacht keine Funktionsprobleme. Sie können jedoch auf allen nicht aktualisierten Servern `gpupdate /force` ausführen, damit der Konfigurationsstatus sofort aktualisiert wird.

## Problem bei der Auflösung des vollqualifizierten Domänennamens (FQDN)

Der **Fehler wurde empfangen**. Server < server\_name > im Einstiegspunkt, < entry\_point\_name > nicht darauf zugegriffen werden kann.

## Ursache

Beim Abrufen der Liste zu ändernder DirectAccess-Server konnte das Cmdlet den vollqualifizierten Domänennamen (FQDN) eines der Server nicht aus der Computer-SID auflösen.

## Lösung

Der in der Fehlermeldung angegebene Einstiegspunkt ist einem Domänencontroller zugeordnet. Stellen Sie sicher, dass der Domänencontroller für den Einstiegspunkt verfügbar ist. Falls der Computer, zu dem die angegebene SID gehört, aus der Domäne entfernt wurde, ignorieren Sie die Meldung, und entfernen Sie den Server aus der Bereitstellung für mehrere Standorte.

## Keine zu aktualisierenden Einstiegspunkte vorhanden

Die **Warnung wurde empfangen**. Die Domänen Controller Einstellungen wurden nicht geändert. Wenn Ihrer Meinung nach Änderungen erforderlich sind, stellen Sie sicher, dass die Cmdlet-Parameter richtig konfiguriert sind und GPOs auf den erforderlichen Domänencontrollern repliziert werden.

## Ursache

Wenn das Cmdlet `Set-DaEntryPointDC` mit dem *ExistingDC*-Parameter aufgerufen wird, überprüft DirectAccess alle Einstiegspunkte und aktualisiert die Einstiegspunkte, die dem angegebenen Domänencontroller zugeordnet sind. Es ist jedoch kein Einstiegspunkt mit dem angegebenen *ExistingDC* vorhanden.

## Lösung

Verwenden Sie das Cmdlet `Get-DAEntryPointDC`, um eine Liste der Einstiegspunkte und der zugeordneten Domänencontroller anzuzeigen. Falls Änderungen vorgenommen wurden, stellen Sie sicher, dass die Cmdlet-Parameter richtig geschrieben sind und die GPOs zu den erforderlichen Domänencontrollern repliziert wurden, und versuchen Sie es noch einmal.

# Problembehandlung bei allgemeinen Problemen

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zur Problembehandlung für allgemeine Probleme im Zusammenhang mit dem Remote Zugriff.

## GPO-Abruf Fehler

Der **Fehler wurde empfangen**. Die GPO-Einstellungen des DirectAccess-Servers können nicht abgerufen werden. Stellen Sie sicher, dass Sie über Bearbeitungs Berechtigungen für das GPO verfügen.

Die Remote Zugriffs-Verwaltungskonsole reagiert nach dem Empfang dieses Fehlers nicht mehr.

### Ursache

DirectAccess kann nicht auf das Gruppenrichtlinien Objekt eines der Einstiegspunkte in der Bereitstellung zugreifen. Daher kann die Konfiguration nicht geladen werden.

### Lösung

Stellen Sie sicher, dass jeder Einstiegspunkt in der Bereitstellung über ein entsprechendes GPO auf seinem Domänen Controller verfügt, und überprüfen Sie, ob der angemeldete Benutzer über Lese-und Schreibberechtigungen für alle in der Remote Zugriffs Bereitstellung konfigurierten GPOs verfügt.

Um dieses Problem zu umgehen, verwenden Sie die Configuration-Cmdlets anstelle der Remote Zugriffs-Verwaltungskonsole. beispielsweise mithilfe von `Get-RemoteAccess` und `Get-DAEntryPoint`.

### NOTE

Dieses Szenario tritt nicht ein, wenn das Server-GPO des aktuellen Einstiegs Punkts nicht verfügbar ist.

Sie können das Cmdlet "`Get-DAEntryPointDC`" verwenden, um alle Domänen Controller aufzulisten, die Server-Gruppenrichtlinien Objekte speichern, und `Get-DAMultiSite` in Verbindung mit `Get-RemoteAccess`, um eine vollständige Liste der Server-Gruppenrichtlinien Objekte in der Bereitstellung abzurufen. Beispiel:

```
$ServerGpos = Get-DAEntryPointDC | ForEach-Object {  
    @{  
        GpoName = (Get-RemoteAccess -EntryPoint $_.EntryPointName).ServerGpoName;  
        DC = $_.DomainControllerName  
    }  
}  
$ServerGpos | ForEach-Object { $GpoName = $_.GpoName ; $DC = $_.DC ; Write-Host "Server GPO '$GpoName' on  
DC '$DC'" }
```

## Client Upgrade für Windows 7 zu Windows 8 oder 10

**Symptom.** Nachdem ein Windows 7-Client in einer Bereitstellung mit mehreren Standorten auf Windows 10 oder Windows 8 aktualisiert wurde, ist die DirectAccess-Verbindung in der Liste der Netzwerke nicht sichtbar.

### Ursache

Die Windows 7-Gruppenrichtlinien Objekte in einer Bereitstellung mit mehreren Standorten enthalten nicht die Konfiguration des Windows 8-netzwerkonnektivitätsassistenten

Bei Windows 7-Clients sollte der DirectAccess-Konnektivitätsassistent zum Überwachen Ihres DirectAccess-Verbindungsstatus verwendet werden, der eine separate manuelle Konfiguration in den Windows 7-Client-Gruppenrichtlinien Objekten Wenn Windows 7-Clients auf Windows 10 oder Windows 8 aktualisiert werden, funktioniert der netzwerkonnektivitätsassistent nicht, wenn das Windows 7-Client-Gruppenrichtlinien Objekt weiterhin angewendet wird.

## Lösung

Wenn die Einstellungen für den DirectAccess-konnektivitätsassistant in den Gruppenrichtlinien Objekten von Windows 7 konfiguriert sind, können Sie dieses Problem beheben, bevor Sie die Windows 7-Gruppenrichtlinien Objekte mithilfe der folgenden PowerShell-Cmdlets ändern:

```
Set-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant" -ValueName "TemporaryValue" -Type Dword -Value 1
Remove-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant"
```

Wenn ein Client bereits aktualisiert wurde oder die DCA nicht konfiguriert ist, verschieben Sie den Client Computer in die Sicherheitsgruppe Windows 10 oder Windows 8.

## Allgemeine Cmdlet-Fehler

- **Problem 1**

Der Fehler wurde empfangen. Domänen Controller < domain\_controller > für < server\_name oder entry\_point\_name > nicht erreicht werden.

### Ursache

Um die Einheitlichkeit der Konfiguration in einer Bereitstellung für mehrere Standorte zu wahren, müssen Sie sicherstellen, dass jedes GPO von einem einzigen Domänencontroller verwaltet wird. Wenn der Domänen Controller, der das Server-Gruppenrichtlinien Objekt eines Einstiegs Punkts verwaltet, nicht verfügbar ist, können die RAS-Konfigurationseinstellungen nicht gelesen oder geändert werden.

### Lösung

Befolgen Sie das Verfahren "so ändern Sie den Domänen Controller, der Server-Gruppenrichtlinien Objekte verwaltet" in [2.4. Konfigurieren Sie GPOs](#).

- **Problem 2**

Der Fehler wurde empfangen. Der primäre Domänen Controller in der Domänen < domain\_name > kann nicht erreicht werden.

### Ursache

Um die Einheitlichkeit der Konfiguration in einer Bereitstellung für mehrere Standorte zu wahren, müssen Sie sicherstellen, dass jedes GPO von einem einzigen Domänencontroller verwaltet wird. Client-GPOs werden auf dem primären Domänencontroller verwaltet. Wenn der primäre Domänencontroller nicht verfügbar ist, können die RAS-Konfigurationseinstellungen nicht gelesen oder geändert werden.

### Lösung

Befolgen Sie das Verfahren "So übertragen Sie die PDC-Emulatorrolle" in [2.4. Konfigurieren Sie GPOs](#).

# Bereitstellen des Remotezugriffs mit OTP-Authentifizierung

09.04.2020 • 14 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess und Routing-und RAS-Dienst (RRAS-)VPN zu einer einzigen Remote Zugriffs Rolle.

## Szenariobeschreibung

In diesem Szenario wird ein RAS-Server, auf dem DirectAccess aktiviert ist, so konfiguriert, dass er DirectAccess-Client Benutzer mit zwei-Factor-Kenn Wort () Authentifizierung zusätzlich zu den standardmäßigen Active Directory Anmelde Informationen authentifiziert.

## Erforderliche Komponenten

Bevor Sie mit der Bereitstellung dieses Szenarios beginnen, sollten Sie die Liste der wichtigen Anforderungen lesen:

- [Eine Bereitstellung eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) muss vor der Bereitstellung von OTP bereitgestellt werden.
- Windows 7-Clients müssen DCA 2,0 zur Unterstützung von OTP verwenden.
- OTP unterstützt nicht die PIN-Änderung.
- Eine Public Key-Infrastruktur muss bereitgestellt werden.

Weitere Informationen finden Sie unter: [Testumgebungsanleitung – Minimodul: Basis-PKI für Windows Server 2012](#)

- Das Ändern von Richtlinien außerhalb der DirectAccess-Verwaltungskonsole oder der Windows PowerShell-Cmdlets wird nicht unterstützt.

## Inhalt dieses Szenarios

Das Szenario für die OTP-Authentifizierung besteht aus mehreren Schritten:

1. Stellen Sie [einen einzelnen DirectAccess-Server mit erweiterten Einstellungen](#) bereit. Vor dem Konfigurieren von OTP muss ein einzelner Remote Zugriffs Server bereitgestellt werden. Die Planung und Bereitstellung eines einzelnen Servers umfasst das Entwerfen und Konfigurieren einer Netzwerktopologie, das Planen und Bereitstellen von Zertifikaten, das Einrichten von DNS und Active Directory, das Konfigurieren von Remotezugriffsservereinstellungen, das Bereitstellen von DirectAccess-Clients und das Vorbereiten von Intranetservern.
2. [Planen Sie den Remote Zugriff mit OTP-Authentifizierung](#). Zusätzlich zur Planung, die für einen einzelnen Server erforderlich ist, erfordert OTP die Planung einer Microsoft-Zertifizierungsstelle (ca) und Zertifikat Vorlagen für OTP und einen RADIUS--aktivierten OTP-Server. Die Planung kann auch eine Anforderung für Sicherheitsgruppen beinhalten, bestimmte Benutzer von starkem (OTP oder Smartcard) Authentifizierung auszuschließen. Informationen zur Konfiguration von OTP in einer Umgebung mit mehreren-Gesamtstrukturen finden Sie unter [Konfigurieren einer Bereitstellung mit mehreren-Gesamtstrukturen](#).

3. [Konfigurieren von DirectAccess mit OTP-Authentifizierung](#). Die OTP-Bereitstellung besteht aus einer Reihe von Konfigurationsschritten, einschließlich der Vorbereitung der Infrastruktur für die OTP-Authentifizierung, dem Konfigurieren des OTP-Servers, dem Konfigurieren von OTP-Einstellungen auf dem RAS-Server und dem Aktualisieren der DirectAccess-Client Einstellungen.
4. [Problembehandlung bei der OTP-Bereitstellung] ([//troubleshoot/Troubleshoot-an-OTP-Deployment.md](#)). In diesem Abschnitt zur Problembehandlung werden einige der häufigsten Fehler beschrieben, die beim Bereitstellen des Remote Zugriffs mit OTP-Authentifizierung auftreten können.

## Praktische Anwendungen

Erhöhung der Sicherheit: die Verwendung von OTP erhöht die Sicherheit Ihrer DirectAccess-Bereitstellung. Ein Benutzer benötigt OTP-Anmeldeinformationen, um auf das interne Netzwerk zugreifen zu können. Ein Benutzer gibt OTP-Anmelde Informationen über die in den Netzwerkverbindungen auf dem Windows 10- oder Windows 8-Client Computer verfügbaren Arbeitsplatz Verbindungen oder mithilfe des DirectAccess-konnektivitätsassistenten (DCA-) auf Client Computern unter Windows 7 an. Der OTP-Authentifizierungsprozess läuft wie folgt ab:

1. Der DirectAccess-Client gibt die Domänen Anmelde Informationen ein, um über den Infrastruktur Tunnel) auf DirectAccess-Infrastruktur Server zuzugreifen (. Wenn aufgrund eines bestimmten IKE-Fehlers keine Verbindung zum internen Netzwerk verfügbar ist, erhält der Benutzer über die Arbeitsplatzverbindungen des Clientcomputers eine Benachrichtigung, dass Anmeldeinformationen eingegeben werden müssen. Auf Client Computern, auf denen Windows 7 ausgeführt wird, wird ein Popup-anfordernder Smartcardanmelde Informationen angezeigt.
2. Nachdem die OTP-Anmelde Informationen eingegeben wurden, werden Sie über SSL an den RAS-Server gesendet, und es wird eine Anforderung für einen kurzen-Term Smartcard-Anmeldezertifikat gesendet.
3. Der Remote Zugriffs Server initiiert die Überprüfung der OTP-Anmelde Informationen mit dem RADIUS--basierten OTP-Server.
4. Bei Erfolg signiert der RAS-Server die Zertifikatanforderung mithilfe seines Registrierungsstellenzertifikats und sendet sie an den DirectAccess-Clientcomputer zurück.
5. Der DirectAccess-Client Computer leitet die signierte Zertifikat Anforderung an die Zertifizierungsstelle weiter und speichert das registrierte Zertifikat für die Verwendung durch die Kerberos SSP/AP.
6. Der Clientcomputer verwendet dieses Zertifikat für eine transparente Standard-Kerberos-Authentifizierung mit einer Smartcard.

## In diesem Szenario enthaltene Rollen und Features

Die folgende Tabelle enthält die für dieses Szenario erforderlichen Rollen und Features:

ROLLEN/FUNKTION	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD

ROLLEN/FUNKTION	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
<p><i>Rollen für die Remote Zugriffs Verwaltung</i></p>	<p>Diese Rolle wird mithilfe der Server-Manager-Konsole installiert und deinstalliert. Diese Rolle umfasst DirectAccess (zuvor ein Feature in Windows Server 2008 R2) sowie die Routing-und RAS-Dienste, die zuvor ein Rollen Dienst unter der Netzwerk Richtlinien-und Zugriffs Dienste (NPAS) Server Rolle waren. Die Remotezugriffs-Rolle besteht aus zwei Komponenten:</p> <ol style="list-style-type: none"> <li>1. DirectAccess-und Routing-und RAS-Dienste (RRAS) VPN-DirectAccess und VPN werden in der Remote Zugriffs-Verwaltungskonsole verwaltet.</li> <li>2. RRAS-Routing-RRAS-Routing Features werden in der Legacy-Routing-und Remote Zugriffs Konsole verwaltet.</li> </ol> <p>Die Remotezugriffsrolle ist von den folgenden Serverfeatures abhängig:</p> <ul style="list-style-type: none"> <li>-Internetinformationsdienste (IIS)-Webserver: dieses Feature ist erforderlich, um den Netzwerkadressen Server zu konfigurieren, die OTP-Authentifizierung zu verwenden und den Standardweb Test zu konfigurieren.</li> <li>-Interne Windows-Datenbank: wird für die lokale Kontoführung auf dem Remote Zugriffs Server verwendet.</li> </ul>
<p>Feature %amp;quot;Tools für die Remotezugriffsverwaltung%amp;quot;</p>	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"> <li>-Sie wird standardmäßig auf einem RAS-Server installiert, wenn die Remote Zugriffs Rolle installiert ist, und unterstützt die Benutzeroberfläche der Remote Verwaltungskonsole.</li> <li>-Es kann optional auf einem Server installiert werden, auf dem die Remote Zugriffs-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.</li> </ul> <p>Das Feature "Tools für die Remotezugriffsverwaltung" besteht aus den folgenden Komponenten:</p> <ul style="list-style-type: none"> <li>-Remote Zugriffs-GUI und Befehlszeilen Tools</li> <li>-Remote Zugriffs Modul für Windows PowerShell</li> </ul> <p>Abhängigkeiten umfassen:</p> <ul style="list-style-type: none"> <li>-Gruppenrichtlinien-Verwaltungskonsole</li> <li>-RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li> <li>-Windows PowerShell 3,0</li> <li>-Tools und Infrastruktur für die grafische Verwaltung</li> </ul>

## Hardwareanforderungen

Für dieses Szenario müssen die folgenden Hardwareanforderungen erfüllt werden:

- Ein Computer, der die Hardwareanforderungen für Windows Server 2016 oder Windows Server 2012 erfüllt.
- Um das Szenario zu testen, ist mindestens ein Computer erforderlich, auf dem Windows 10, Windows 8 oder Windows 7 ausgeführt wird und der als DirectAccess-Client konfiguriert ist.
- Ein OTP-Server, der PAP über RADIUS unterstützt
- Ein OTP-Hardware- oder Software-Token

# Software Anforderungen

Für dieses Szenario gelten eine Reihe von Anforderungen:

1. Softwareanforderungen für die Bereitstellung auf einem Einzelserver. Weitere Informationen finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).
2. Zusätzlich zu den Softwareanforderungen für einen einzelnen Server gibt es eine Reihe von OTP-spezifischen Anforderungen:
  - a. Zertifizierungsstelle für die IPSec-Authentifizierung: in einer OTP-Bereitstellung muss DirectAccess mithilfe von IPSec-Computer Zertifikaten bereitgestellt werden, die von einer Zertifizierungsstelle Die IPsec-Authentifizierung mithilfe des RAS-Servers als Kerberos-Proxy wird bei der OTP-Bereitstellung nicht unterstützt. Eine interne Zertifizierungsstelle ist erforderlich.
  - b. Zertifizierungsstelle für die OTP-Authentifizierung: eine Microsoft-Unternehmens Zertifizierungsstelle (, die unter Windows 2003 Server oder höher ausgeführt wird) ist erforderlich, um das OTP-Client Zertifikat auszustellen. Es kann dieselbe Zertifizierungsstelle verwendet werden, die auch die Zertifikate für die IPsec-Authentifizierung ausstellt. Der Zertifizierungsstellenserver muss über den ersten Infrastrukturtunnel erreichbar sein.
  - c. Sicherheitsgruppe: um Benutzer von der starken Authentifizierung auszuschließen, ist eine Active Directory Sicherheitsgruppe erforderlich, die diese Benutzer enthält.
  - d. Client-seitige Anforderungen: für Windows 10-und Windows 8-Client Computer wird der netzwerkkonnektivitätsassistent (NCA)-Dienst verwendet, um zu ermitteln, ob OTP-Anmelde Informationen erforderlich sind. Wenn dies der Fall ist, fordert der DirectAccess-Medien-Manager Anmelde Informationen an. NCA ist im Betriebssystem enthalten, und es ist keine Installation oder Bereitstellung erforderlich. Für Windows 7-Client Computer ist der DirectAccess-Konnektivitätsassistent (DCA) 2,0 erforderlich. Dieser kann aus dem [Microsoft Download Center](#) heruntergeladen werden.
  - e. Beachten Sie Folgendes:
    - a. Die OTP-Authentifizierung kann parallel zum Smartcard-und Trusted Platform Module (TPM)-basierten Authentifizierung verwendet werden. Das Aktivieren der OTP-Authentifizierung in der Remotezugriffsverwaltungskonsole ermöglicht auch die Verwendung der Smartcard-Authentifizierung.
    - b. Während der Remote Zugriffs Konfiguration können Benutzer in einer angegebenen Sicherheitsgruppe von zwei-Faktor Authentifizierung ausgenommen werden und müssen sich daher mit dem Benutzernamen/Kennwort authentifizieren.
    - c. Die OTP-Modi "Neue PIN" und "Nächster Tokencode" werden nicht unterstützt.
    - d. Bei einer Remotezugriffsbereitstellung an mehreren Standorten sind die OTP-Einstellungen global und dienen zur Identifikation an allen Einstiegspunkten. Wenn mehrere RADIUS- oder Zertifizierungsstellenserver für OTP konfiguriert werden, müssen sie von jedem RAS-Server anhand ihrer Verfügbarkeit und Nähe sortiert werden.
    - e. Beim Konfigurieren von OTP in einer Remote Zugriffs Umgebung mit mehreren-Gesamtstruktur sollten die OTP-Zertifizierungsstellen nur aus der Ressourcen Gesamtstruktur und die Zertifikat Registrierung über Gesamtstruktur-Vertrauens Stellungen hinweg konfiguriert werden. Weitere Informationen finden Sie unter [AD CS: Gesamtstrukturübergreifende Zertifikatsregistrierung mit Windows Server 2008 R2](#).
    - f. Benutzer, die ein Schlüsselbobjekt OTP-Token verwenden, sollten die PIN gefolgt von Tokencode (ohne Trennzeichen) im Dialogfeld DirectAccess-OTP einfügen. Benutzer, die einen

PIN PAD OTP-Token verwenden, geben in diesem Dialogfeld nur den Tokencode ein.

- g. Bei aktiviertem WEBDAV darf OTP nicht aktiviert werden.

## Bekannte Probleme

Im Folgenden finden Sie bekannte Probleme beim Konfigurieren eines OTP-Szenarios:

- Der Remote Zugriff verwendet einen Test Mechanismus, um die Konnektivität mit RADIUS--basierten OTP-Servern zu überprüfen. In einigen Fällen kann auf dem OTP-Server ein Fehler ausgelöst werden. Gehen Sie zur Vermeidung dieses Problems auf dem OTP-Server folgendermaßen vor:
  - Erstellen Sie ein Benutzerkonto entsprechend dem auf dem RAS-Server für den Testmechanismus konfigurierten Benutzernamen und Kennwort. Der Benutzername darf keinen Active Directory-Benutzer definieren.

Standardmäßig ist der Benutzername auf dem RAS-Server "DAProbeUser", und das Kennwort lautet "DAProbePass". Diese Standardeinstellungen können mithilfe der folgenden Werte in der Registrierung auf dem RAS-Server geändert werden:

- HKEY\_lokalen\_Machine\Software\Microsoft\DirectAccess\OTP\radiusprobeuser
- HKEY\_lokalen\_Machine\Software\Microsoft\DirectAccess\OTP\radiusprobepass
- Wenn Sie das IPsec-Stammzertifikat in einer konfigurierten und ausgeführten DirectAccess-Bereitstellung ändern, funktioniert OTP nicht mehr. Um dieses Problem zu beheben, führen Sie auf jedem DirectAccess-Server an einer Windows PowerShell-Eingabeaufforderung den folgenden Befehl aus: `iisreset`

# Planen des Remotezugriffs mit OTP-Authentifizierung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess-und RRAS-VPN (Routing and Remote Access Service, Routing-und RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle. Diese Übersicht bietet eine Einführung in die Konfigurationsschritte, die erforderlich sind, um eine einzelne Bereitstellung von Windows Server 2016 oder Windows Server 2012 Remote Access für mehrere Standorte bereitzustellen.

- Schritt 1: bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) Dieser Schritt umfasst die Planung der Infrastruktur, die für die Bereitstellung eines einzelnen Servers erforderlich ist. Dazu gehört die Planung von Netzwerk- und Servereinstellungen, Zertifikat Anforderungen, DNS-Einstellungen, Bereitstellung des Netzwerkadressen Servers, DirectAccess-Verwaltungs Servern, Active Directory Einstellungen und Gruppenrichtlinie Objekte (GPOs).
- [Schritt 2: Planen der RADIUS-Server Bereitstellung](#)
- [Schritt 3: Planen der OTP-Zertifikat Bereitstellung](#)
- [Schritt 4: Planen von OTP auf dem Remote Zugriffs Server](#)

Nachdem Sie diese Planungsschritte abgeschlossen haben, finden Sie weitere Informationen unter [Konfigurieren des Remote Zugriffs mit OTP-Authentifizierung](#). Informationen zum Konfigurieren einer Bereitstellung für mehrere Standorte als Proof of Concept in einer Lab-Umgebung finden Sie unter [Test Umgebungs Anleitung: veranschaulichen von DirectAccess mit OTP-Authentifizierung und RSA SecurID](#).

# Schritt 1 Planen einer erweiterten Einzel Server Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt bei der Planung eines Remote Zugriffs mit der Bereitstellung eines einmaligen Kennworts (OTP)-Client Authentifizierung ist das Planen und Konfigurieren einer erweiterten Einzel Server Bereitstellung.

## Planen einer Bereitstellung auf einem einzelnen Server

Stellen Sie vor dem Bereitstellen des Remote Zugriffs mit OTP sicher, dass Sie alle Schritte zum Bereitstellen eines einzelnen Remote Zugriffs Servers abgeschlossen haben. Weitere Informationen finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).

# Schritt 2 Planen der RADIUS-Server Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Planen Sie nach der Bereitstellung eines einzelnen RAS-Servers den einmal Kennwort (One-time password, OTP)-Authentifizierungsserver ein.

AUFGABE	BESCHREIBUNG
2,1 Planen des RADIUS-Servers	Für den OTP-Authentifizierungsserver unterstützt der Remote Zugriff in Windows Server 2016 und Windows Server 2012 alle RADIUS-fähigen OTP-Server, die das Kennwort Authentication Protocol (PAP) unterstützen.

## 2,1 Planen des RADIUS-Servers

Beachten Sie Folgendes, wenn Sie einen RADIUS-Server für die OTP-Authentifizierung planen:

- Für die meisten Arten von OTP-bereit Stellungen müssen Sie den RAS-Server als RADIUS-Agent konfigurieren. Weitere Informationen finden Sie in der Dokumentation des OTP-Herstellers.
- Für alle OTP-bereit Stellungen müssen Sie Ihre Active Directory Benutzer mit dem RADIUS-Server synchronisieren.
- Der RADIUS-Server muss kein Domänen Mitglied sein.
- Wenn Sie den RADIUS-Server bereitstellen, konfigurieren Sie einen gemeinsamen geheimen Schlüssel und die Portnummer für RADIUS-Datenverkehr. Notieren Sie sich diese Details. Sie sind erforderlich, wenn Sie den Remote Zugriffs Server konfigurieren.

Ein Beispiel für eine Test Umgebungs Anleitung zum Einrichten der OTP-Authentifizierung mit einem RSA SecurID-Server finden Sie in der [Test Umgebungs Anleitung: demonstrieren von DirectAccess mit OTP-Authentifizierung und RSA SecurID](#).

# Schritt 3 Planen der OTP-Zertifikat Bereitstellung

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nach der Planung des RADIUS-Servers müssen Sie die Anforderungen der Zertifizierungsstelle (Certification Authority, ca) planen, einschließlich der Zertifizierungsstelle, von der die Zertifikate für einmal Kennwort (OTP), die OTP-Zertifikat Vorlage und das vom Remote Server verwendete Registrierungsstellen Zertifikat ausgestellt werden. Zugriffs Server zum Signieren aller OTP-Zertifikat Anforderungen für den DirectAccess-Client. Diese Zertifikate werden wie folgt verwendet:

1. Der DirectAccess-Client fordert ein OTP-Zertifikat an, und der Remote Zugriffs Server empfängt die Anforderung.
2. Der RAS-Server überprüft die OTP-Anmelde Informationen, wenn diese gültig sind, fungiert der Server als Registrierungsstelle und signiert die OTP-Zertifikat Registrierungs Anforderung mithilfe eines kurzlebigen Signatur Zertifikats.
3. Der Remote Zugriffs Server sendet die signierte Zertifikat Registrierungs Anforderung an den DirectAccess-Client zurück.
4. Der Client registriert dann das OTP-Zertifikat von der Zertifizierungsstelle mithilfe der Zertifikat Registrierungsanforderungen, die vom Server signiert wurden.
5. Die Zertifizierungsstelle überprüft die Anmelde Informationen und die Anforderung.

AUFGABE	BESCHREIBUNG
<a href="#">3,1 Planen der OTP-Zertifizierungsstelle</a>	Planen Sie die Zertifizierungsstelle, die zum Ausstellen von Zertifikaten für DirectAccess-Clients für die OTP-Authentifizierung verwendet werden soll.
<a href="#">3,2 Planen der OTP-Zertifikat Vorlage</a>	Planen Sie die OTP-Zertifikat Vorlage.
<a href="#">3,3 Planen des Registrierungsstellen Zertifikats</a>	Planen Sie das Registrierungsstellen Zertifikat, um alle OTP-Authentifizierungszertifikat Anforderungen zu signieren.

## 3,1 Planen der OTP-Zertifizierungsstelle

Zum Bereitstellen von DirectAccess mithilfe von einmal Kennwort-Authentifizierung (einmal Kennwort-Authentifizierung) benötigen Sie eine interne Zertifizierungsstelle, um die OTP-Authentifizierungs Zertifikate für DirectAccess-Client Computer auszustellen. Zu diesem Zweck können Sie dieselbe interne Zertifizierungsstelle verwenden, mit der Sie die Zertifikate ausstellen, die für die reguläre IPSec-Computer Authentifizierung verwendet werden.

## 3,2 Planen der OTP-Zertifikat Vorlage

Jeder DirectAccess-Client benötigt ein OTP-Authentifizierungszertifikat, um Zugriff auf das interne Netzwerk zu erhalten. Sie müssen eine Vorlage für die interne Zertifizierungsstelle für das OTP-Zertifikat konfigurieren. Beachten Sie beim Konfigurieren der OTP-Zertifikat Vorlage Folgendes:

- Alle Benutzer, die die OTP-Authentifizierung durchführen müssen, müssen über die Berechtigungen Lesen und anmelden für diese Vorlage verfügen.
- Der Name des Antragstellers sollte aus Active Directory Informationen erstellt werden, um sicherzustellen, dass der Antragsteller Name mit dem OTP-Benutzernamen übereinstimmt, und nicht mit dem Namen des RAS-Servers, von dem die Zertifikat Anforderung durchführt. Der Antragsteller Name muss das vollständig gekennzeichnete Namensformat aufweisen, und der alternative Antragsteller Name muss das UPN-Format aufweisen. Dadurch wird sichergestellt, dass das registrierte OTP-Zertifikat für die Smartcard-Kerberos-Authentifizierung gültig ist.
- Der beabsichtigte Zweck des Zertifikats muss die Smartcard-Anmeldung sein.
- Die Ausstellung muss eine autorisierte Signatur erfordern. Die Signatur muss mit der vordefinierten DirectAccess OTP-Anwendungs Richtlinie konfiguriert werden, die in der Registrierungsstelle-Signaturzertifikat Vorlage festgelegt ist.
- Der Gültigkeits Zeitraum muss auf eine Stunde festgelegt werden.

**NOTE**

In Fällen, in denen der Zertifizierungsstellen Server ein Windows Server 2003-Computer ist, muss die Vorlage auf einem anderen Computer konfiguriert werden. Dies liegt daran, dass das Festlegen der **Gültigkeitsdauer** in Stunden nicht möglich ist, wenn Windows-Versionen vor 2008/Vista ausgeführt werden. Wenn auf dem Computer, den Sie zum Konfigurieren der Vorlage verwenden, die Zertifizierungsdienst Rolle nicht installiert ist, oder es sich um einen Client Computer handelt, müssen Sie möglicherweise das Zertifikat Vorlagen-Snap-in installieren. Weitere Informationen zu diesem Betreff finden Sie [hier](#).

- Der Erneuerungs Zeitraum muss auf 0 festgelegt werden.
- Optionale Zertifikate und Anforderungen dürfen nicht in der Zertifizierungsstellen-Datenbank gespeichert werden.
- Der erweiterte Schlüssel Verwendungs Parameter des Zertifikats muss wie folgt ordnungsgemäß festgelegt werden:
  - Verwenden Sie für die DirectAccess-Registrierungs Signaturzertifikat-Vorlage den Schlüssel 1.3.6.1.4.1.311.81.1.1.
  - Verwenden Sie für die OTP-Authentifizierungszertifikat Vorlage den Schlüssel 1.3.6.1.4.1.311.20.2.2 Key.

### 3,3 Planen des Registrierungsstellen Zertifikats

Wenn DirectAccess-Clients ein OTP-Zertifikat anfordern, empfängt der RAS-Server die Anforderung vom Client. Der RAS-Server signiert alle OTP-Zertifikat Anforderungen von Clients mithilfe des Registrierungsstellen Zertifikats. Die Zertifizierungsstelle gibt Zertifikate nur dann aus, wenn die Anforderung vom Registrierungsstellen Zertifikat auf dem RAS-Server signiert wurde. Das Zertifikat muss von einer internen Zertifizierungsstelle ausgestellt werden, das Zertifikat kann nicht selbst signiert werden. Er muss nicht von der Zertifizierungsstelle ausgestellt werden, die die OTP-Zertifikate ausgestellt hat, aber die Zertifizierungsstelle, die die OTP-Zertifikate ausgibt, muss der Zertifizierungsstelle vertrauen, die das Signaturzertifikat der Registrierungsstelle ausgibt.

### Siehe auch

- [Schritt 4: Planen von OTP für den Remote Zugriffs Server](#)

# Schritt 4 Planen von OTP auf dem Remote Zugriffs Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nach der Planung der Server-und Zertifikat Einstellungen für das einmalige Kennwort (One-time password, OTP) müssen Sie den letzten Schritt bei der Planung einer Bereitstellung für den Remote Zugriff auf den RAS-Server planen.

AUFGABE	BESCHREIBUNG
<a href="#">4,1 Planen von OTP-Client Ausnahmen</a>	Planen Sie Ausnahmen für Benutzer ein, die für die Authentifizierung mit OTP nicht erforderlich sind.
<a href="#">4,2 Planen für Windows 7-Clients</a>	Planen Sie die Bereitstellung des DirectAccess-konnektivitätsassistenten (DCA) 2,0 für Windows 7-Client Computer.
<a href="#">4,3 Planen von Smartcards</a>	Planen Sie die Verwendung von Smartcards für zusätzliche Autorisierung.

## 4,1 Planen von OTP-Client Ausnahmen

Wenn die OTP-Authentifizierung aktiviert ist, müssen sich alle Benutzer standardmäßig mit einer Kombination aus Benutzername und Kennwort und OTP-Anmelde Informationen authentifizieren. Allerdings können Sie es Benutzern ermöglichen, sich nur mit einem Benutzernamen und einem Kennwort zu authentifizieren, ohne OTP zu verwenden. Erstellen Sie dazu eine Sicherheitsgruppe, und fügen Sie alle Benutzer hinzu, die von der OTP-Authentifizierung ausgenommen werden sollen.

### NOTE

Nur Client Computer aus einer einzelnen Gesamtstruktur können aufgrund der Tatsache, dass nur eine Sicherheitsgruppe für Client Ausnahmen ausgewählt werden kann, ausgenommen werden.

## 4,2 Planen für Windows 7-Clients

Windows 7-Client Computer können sich standardmäßig nicht mithilfe von OTP authentifizieren. Windows 7-Client Computer erfordern eine DCA 2,0 für die Authentifizierung mithilfe von OTP in einer Windows Server 2012-Remote Zugriffs Bereitstellung. Weitere Informationen zu DCA 2,0 finden Sie unter [DirectAccess Connectivity Assistant 2,0](#) im Microsoft Download Center.

## 4,3 Planen von Smartcards

Wenn die OTP-Authentifizierung aktiviert ist, ist die Option zum Aktivieren der Verwendung von Smartcards für zusätzliche Autorisierung verfügbar. Erstellen Sie eine Sicherheitsgruppe, um vorübergehenden Zugriff zuzulassen, falls die Smartcard eines Benutzers nicht funktionsfähig ist.

## Siehe auch

- [Konfigurieren von DirectAccess mit OTP-Authentifizierung](#)

# Planen des Remotezugriffs mit OTP-Authentifizierung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess-und RRAS-VPN (Routing and Remote Access Service, Routing-und RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle. Diese Übersicht bietet eine Einführung in die Konfigurationsschritte, die erforderlich sind, um eine einzelne Bereitstellung von Windows Server 2016 oder Windows Server 2012 Remote Access für mehrere Standorte bereitzustellen.

- [Schritt 1: Implementieren einer Einzel Server-Remote Zugriffs Bereitstellung.](#) Installieren und konfigurieren Sie einen einzelnen Remote Zugriffs Server. Anweisungen finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).
- [Schritt 2: Konfigurieren Sie den RADIUS-Server.](#)
- [Schritt 3: Konfigurieren Sie den Remote Zugriffs Server für OTP.](#)
- [Schritt 4: Überprüfen von DirectAccess mit OTP](#)

# Schritt 1 Implementieren einer einzelnen Server Bereitstellung für den Remote Zugriff

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Konfigurationsschritt zum Bereitstellen des Remote Zugriffs in einer Topologie mit mehreren Standorten ist die Implementierung einer erweiterten Bereitstellung mit einem einzelnen Server und das Hinzufügen von Servern zu jedem Multisite-Einstiegspunkt.

## Implementieren einer Bereitstellung auf einem einzelnen Server

Bevor Sie eine Bereitstellung für mehrere Standorte konfigurieren können, müssen Sie wie unter Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen beschrieben eine erweiterte Bereitstellung für den Remote Zugriff mit einem Server konfigurieren.

## Siehe auch

- [Schritt 2: Konfigurieren der Infrastruktur für mehrere Standorte](#)

# Schritt 2 Konfigurieren des RADIUS-Servers

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Bevor Sie den Remote Zugriffs Server für die Unterstützung von DirectAccess mit OTP-Unterstützung konfigurieren, konfigurieren Sie den RADIUS-Server.

AUFGABE	BESCHREIBUNG
<a href="#">2,1. Konfigurieren der RADIUS-Software Verteilungs Token</a>	Konfigurieren Sie auf dem RADIUS-Server Software Verteilungs Token.
<a href="#">2,2. Konfigurieren der RADIUS-Sicherheitsinformationen</a>	Konfigurieren Sie auf dem RADIUS-Server die zu verwendenden Ports und den gemeinsamen geheimen Schlüssel.
<a href="#">2,3 Hinzufügen eines Benutzerkontos für die OTP-Überprüfung</a>	Erstellen Sie auf dem RADIUS-Server ein neues Benutzerkonto für die OTP-Überprüfung.
<a href="#">2,4 synchronisieren mit Active Directory</a>	Erstellen Sie auf dem RADIUS-Server Benutzerkonten, die mit Active Directory Konten synchronisiert sind.
<a href="#">2,5 Konfigurieren des RADIUS-Authentifizierungs-Agents</a>	Konfigurieren Sie den RAS-Server als RADIUS-Authentifizierungs-Agent.

## 2,1 Konfigurieren der RADIUS-Software Verteilungs Token

Der RADIUS-Server muss mit den erforderlichen Lizenz-und Software-und/oder Hardware Verteilungs Token konfiguriert werden, die von DirectAccess mit OTP verwendet werden. Dieser Prozess wird für jede Implementierung des RADIUS-Anbieters spezifisch sein.

## 2,2 Konfigurieren der RADIUS-Sicherheitsinformationen

Der RADIUS-Server verwendet UDP-Ports zu Kommunikationszwecken, und jeder RADIUS-Anbieter verfügt über eigene UDP-Standardports für die eingehende und ausgehende Kommunikation. Damit der RADIUS-Server mit dem RAS-Server funktioniert, müssen Sie sicherstellen, dass alle Firewalls in der Umgebung so konfiguriert sind, dass der UDP-Datenverkehr zwischen den DirectAccess-und OTP-Servern bei Bedarf über die erforderlichen Ports zugelassen wird.

Der RADIUS-Server verwendet für die Authentifizierung einen gemeinsamen geheimen Schlüssel. Konfigurieren Sie den RADIUS-Server mit einem sicheren Kennwort für den gemeinsamen geheimen Schlüssel. Beachten Sie, dass dieser verwendet wird, wenn die Client Computerkonfiguration des DirectAccess-Servers für die Verwendung mit dem OTP-Server konfiguriert wird.

## 2,3 Hinzufügen eines Benutzerkontos für die OTP-Überprüfung

Erstellen Sie auf dem RADIUS-Server ein neues Benutzerkonto mit dem Namen **daprobeuser**, und geben Sie ihm das Kennwort **daprobeppass**.

## 2,4 synchronisieren mit Active Directory

Der RADIUS-Server muss über Benutzerkonten verfügen, die den Benutzern in Active Directory entsprechen, die DirectAccess mit OTP verwenden werden.

### **So synchronisieren Sie den RADIUS-und den Active Directory Benutzer**

1. Notieren Sie die Benutzerinformationen aus Active Directory für alle DirectAccess-Benutzer mit OTP-Benutzern.
2. Verwenden Sie das herstellerspezifische Verfahren, um identische Benutzer **Domänen \ Benutzernamen** Konten auf dem Server zu erstellen, die aufgezeichnet wurden.

## 2,5 Konfigurieren des RADIUS-Authentifizierungs-Agents

Der RAS-Server muss als RADIUS-Authentifizierungs-Agent für die Implementierung von DirectAccess mit OTP konfiguriert werden. Befolgen Sie die Anweisungen des RADIUS-Anbieters, um den RAS-Server als RADIUS-Authentifizierungs-Agent zu konfigurieren.

# Schritt 3 Konfigurieren des Remote Zugriffs Servers für OTP

09.04.2020 • 14 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nachdem der RADIUS-Server mit Software Verteilungs Token konfiguriert wurde, sind die Kommunikationsports geöffnet, ein gemeinsamer geheimer Schlüssel wurde erstellt, Benutzerkonten, die Active Directory entsprechen, wurden auf dem RADIUS-Server erstellt, und der RAS-Server hat der RAS-Server muss für die Unterstützung von OTP konfiguriert werden, wenn er als RADIUS-Authentifizierungs-Agent konfiguriert wurde.

AUFGABE	BESCHREIBUNG
<a href="#">3,1 Benutzer von OTP-Authentifizierung ausgenommen (optional)</a>	Wenn bestimmte Benutzer von DirectAccess mit OTP-Authentifizierung ausgenommen werden, führen Sie die folgenden Schritte aus.
<a href="#">3,2 Konfigurieren des Remote Zugriffs Servers für die Unterstützung von OTP</a>	Aktualisieren Sie auf dem Remote Zugriffs Server die Konfiguration des Remote Zugriffs, um die zweistufige Authentifizierung von OTP zu unterstützen.
<a href="#">3,3 Smartcards für zusätzliche Autorisierung</a>	Weitere Informationen zur Verwendung von Smartcards.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## 3,1 Benutzer von OTP-Authentifizierung ausgenommen (optional)

Wenn bestimmte Benutzer von der OTP-Authentifizierung ausgenommen werden sollen, müssen diese Schritte vor der Konfiguration des Remote Zugriffs ausgeführt werden:

### NOTE

Beim Konfigurieren der OTP-Ausnahme Gruppe müssen Sie auf den Abschluss der Replikation zwischen Domänen warten.

### Benutzer Ausnahme-Sicherheitsgruppe erstellen

1. Erstellen Sie eine Sicherheitsgruppe in Active Directory für die OTP-Ausnahme.
2. Fügen Sie alle Benutzer, die von der OTP-Authentifizierung ausgenommen werden sollen, der Sicherheitsgruppe hinzu.

### NOTE

Stellen Sie sicher, dass nur Benutzerkonten und keine Computer Konten in der Sicherheitsgruppe "OTP" ausgenommen sind.

## 3.2 Konfigurieren des Remote Zugriffs Servers für die Unterstützung von OTP

Führen Sie die folgenden Schritte aus, um den Remote Zugriff für die Verwendung von zweistufiger Authentifizierung und OTP mit dem RADIUS-Server und der Zertifikat Bereitstellung aus den vorherigen Abschnitten zu konfigurieren:

### Konfigurieren des Remote Zugriffs für OTP

1. Öffnen Sie **Remote Zugriffs Verwaltung**, und klicken Sie auf **Konfiguration**.
2. Klicken Sie im Fenster **DirectAccess-Setup** unter **Schritt 2-RAS-Server** auf **Bearbeiten**.
3. Klicken Sie dreimal auf **weiter**, und wählen Sie im Abschnitt **Authentifizierung** beide **zwei** stufige Authentifizierung aus, und vergewissern Sie sich, dass die Option **Computer Zertifikate verwenden** aktiviert ist.

#### NOTE

Wenn Sie OTP auf dem RAS-Server aktiviert haben, werden die ISAPI- und CGI-Erweiterungen auf dem Server deinstalliert, wenn Sie OTP durch Deaktivieren der **Verwendung von OTP** deaktivieren.

4. Wenn Windows 7-Unterstützung erforderlich ist, aktivieren Sie das Kontrollkästchen **Windows 7-Client Computer zum Herstellen einer Verbindung über DirectAccess aktivieren**. Hinweis: wie im Abschnitt zur Planung erläutert, muss für Windows 7-Clients DCA 2,0 installiert sein, damit DirectAccess mit OTP unterstützt werden kann.
5. Klicken Sie auf **Weiter**.
6. Doppelklicken Sie im Abschnitt "OTP RADIUS-Server" auf das Feld "**leerer Server Name**".
7. Geben Sie im Dialogfeld **RADIUS-Server hinzufügen** den Namen des RADIUS-Servers in das Feld **Server Name** ein. Klicken Sie neben dem Feld **gemeinsamer geheimer Schlüssel** auf **ändern**, und geben Sie das Kennwort ein, das Sie beim Konfigurieren des RADIUS-Servers in den **neuen geheimen Schlüsseln** und **bestätigen neuer geheimer** Schlüssel verwendet haben. Klicken Sie zweimal auf **OK**, und klicken Sie auf **weiter**.

#### NOTE

Wenn sich der RADIUS-Server in einer anderen Domäne als der RAS-Server befindet, muss im Feld **Server Name** der voll qualifizierte Domänen Name des RADIUS-Servers angegeben werden.

8. Wählen Sie im Abschnitt **OTP -Zertifizierungsstellen** Server die Zertifizierungsstellen Server aus, die für die Registrierung von OTP-Client Authentifizierungs Zertifikaten verwendet werden sollen, und klicken Sie auf **Hinzufügen**. Klicken Sie auf **Weiter**.
9. Klicken Sie im Abschnitt **OTP-Zertifikat Vorlagen** auf **Durchsuchen**, um die Zertifikat Vorlage auszuwählen, die für die Registrierung von Zertifikaten verwendet wird, die für die OTP-Authentifizierung ausgestellt werden.

#### NOTE

Die Zertifikat Vorlage für OTP-Zertifikate, die von der Unternehmens Zertifizierungsstelle ausgestellt wurde, muss ohne die Option "keine Sperrinformationen in ausgestellten Zertifikaten einschließen" konfiguriert werden. Wenn diese Option während der Erstellung der Zertifikat Vorlage ausgewählt wird, können sich die OTP-Client Computer nicht ordnungsgemäß anmelden.

Klicken Sie auf **Durchsuchen**, um eine Zertifikat Vorlage auszuwählen, die zum Registrieren des Zertifikats verwendet wird, das vom RAS-Server zum Signieren von OTP-Zertifikat Registrierungsanforderungen verwendet wird. Klicken Sie auf **OK**. Klicken Sie auf **Weiter**.

10. Wenn die Angabe bestimmter Benutzer von DirectAccess mit OTP erforderlich ist, wählen Sie im Abschnitt "**OTP-Ausnahmen**" die Option **Benutzer in der angegebenen Sicherheitsgruppe darf nicht mithilfe der zweistufigen Authentifizierung authentifizieren** aus. Klicken Sie auf **Sicherheitsgruppe**, und wählen Sie die Sicherheitsgruppe aus, die für OTP-Ausnahmen erstellt wurde.
11. Klicken Sie auf der Seite **Setup des Remote Zugriffs Servers** auf **Fertigstellen**.
12. Klicken Sie im Fenster **DirectAccess-Setup** unter **Schritt 3-Infrastruktur Server** auf **Bearbeiten**.
13. Klicken Sie zweimal auf **weiter**, und doppelklicken Sie im Abschnitt **Verwaltung** auf das Feld **Verwaltungs Server**.
14. Geben Sie den **Computer Namen** oder die **Adresse** des Zertifizierungsstellen Servers ein, der für das Ausstellen von OTP-Zertifikaten konfiguriert ist, und klicken Sie auf **OK**.
15. Klicken Sie im Fenster **Remote Zugriffs Einrichtung** auf **Fertigstellen**.
16. Klicken Sie im **DirectAccess-Experten-Assistenten** auf **Fertig** stellen.
17. Klicken Sie im Dialogfeld **Remote Zugriffs Überprüfung** auf **über nehmen, warten Sie**, bis die DirectAccess-Richtlinie aktualisiert wurde, und klicken Sie dann auf **Schließen**.
18. Geben Sie im **Start BildschirmPowerShell. exeein**, klicken Sie mit der rechten Maustaste auf **PowerShell**, klicken Sie auf **erweitert**, und klicken Sie dann auf **als Administrator ausführen**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
19. Geben Sie im Windows PowerShell-Fenster **gpupdate/force** ein, und drücken Sie die EINGABETASTE.

So konfigurieren Sie den Remote Zugriff für OTP mithilfe von PowerShell-Befehlen:

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

So konfigurieren Sie den Remote Zugriff für die Verwendung der zweistufigen Authentifizierung für eine Bereitstellung, die derzeit die Computer Zertifikat Authentifizierung verwendet:

```
Set-DAServer -UserAuthentication TwoFactor
```

So konfigurieren Sie den Remote Zugriff, um die OTP-Authentifizierung mit den folgenden Einstellungen zu verwenden:

- Ein OTP-Server mit dem Namen OTPCorp.contoso.com.

- Ein Zertifizierungsstellen Server mit dem Namen App1.Corp.ca.com\corp-App1-CA1.
- Eine Zertifikat Vorlage mit dem Namen daotplogon, die für die Registrierung von Zertifikaten verwendet wird, die für die OTP-Authentifizierung ausgestellt werden.
- Eine Zertifikat Vorlage namens daotpra, mit der das Registrierungsstellen Zertifikat registriert wird, das vom RAS-Server zum Signieren von OTP-Zertifikat Registrierungsanforderungen verwendet wird.

```
Enable-DAOtpAuthentication -CertificateTemplateName 'DAOTPLogon' -SigningCertificateTemplateName 'DAOTPRA' -  
CAServer @('APP1.corp.contoso.com\corp-APP1-CA1') -RadiusServer OTP.corp.contoso.com -SharedSecret Abcd123$
```

Nachdem Sie die PowerShell-Befehle ausgeführt haben, führen Sie die Schritte 12-19 aus dem vorherigen Verfahren zum Konfigurieren des RAS-Servers für die Unterstützung von OTP aus

#### **NOTE**

Stellen Sie sicher, dass Sie die OTP-Einstellungen auf dem RAS-Server angewendet haben, bevor Sie einen Einstiegspunkt hinzufügen.

## 3,3 Smartcards für zusätzliche Autorisierung

Auf der Seite Authentifizierung von Schritt 2 im Setup-Assistenten für Remote Zugriff können Sie die Verwendung von Smartcards für den Zugriff auf das interne Netzwerk vorschreiben. Wenn diese Option ausgewählt ist, konfiguriert der Remote Zugriffs-Setup-Assistent die IPsec-Verbindungs Sicherheitsregel für den intranettunnel auf dem DirectAccess-Server so, dass eine Tunnel Modus-Autorisierung mit Smartcards erforderlich ist. Mithilfe der Tunnelmodusautorisierung können Sie angeben, dass nur autorisierte Computer oder Benutzer einen eingehenden Tunnel einrichten können.

Um bei der IPsec-Tunnelmodusberechtigung für den Intranettunnel Smartcards zu verwenden, müssen Sie eine Public Key-Infrastruktur (PKI) für die Verwendung mit Smartcards bereitstellen.

Da Ihre DirectAccess-Clients Smartcards für den Zugriff auf das Intranet verwenden, können Sie auch die Authentifizierungsmechanismus-Sicherung, ein Feature von Windows Server 2008 R2, verwenden, um den Zugriff auf Ressourcen wie Dateien, Ordner und Drucker zu steuern, je nachdem, ob Benutzer, der mit einem smartcardbasierten Zertifikat angemeldet ist. Die Authentifizierung des Authentifizierungsmechanismus erfordert eine Domänen Funktionsebene von Windows Server 2008 R2.

### **Zugriffssteuerung für Benutzer mit unbrauchbaren Smartcards**

Gehen Sie wie folgt vor, um Benutzern mit unbrauchbaren Smartcards temporären Zugriff zu gestatten:

1. Erstellen Sie eine Active Directory-Sicherheitsgruppe mit den Benutzerkonten von Benutzern, die ihre Smartcards vorübergehend nicht verwenden können.
2. Konfigurieren Sie für das Gruppenrichtlinie Objekt des DirectAccess-Servers globale IPsec-Einstellungen für die IPsec-Tunnel Autorisierung, und fügen Sie der Liste der autorisierten Benutzer die Active Directory Sicherheitsgruppe hinzu.

Um einem Benutzer, der seine Smartcard nicht verwenden kann, Zugriff zu gewähren, fügen Sie der Active Directory-Sicherheitsgruppe vorübergehend sein Benutzerkonto hinzu. Entfernen Sie das Benutzerkonto aus der Gruppe, sobald die Smartcard wieder verwendbar ist.

### **Im folgenden Abschnitt: Smartcard-Autorisierung**

Die Smartcard-Autorisierung funktioniert, indem die Tunnelmodusautorisierung der Verbindungssicherheitsregel für den Intranettunnel zum DirectAccess-Server für eine bestimmte Kerberos-basierte Sicherheits-ID (SID) aktiviert wird. Bei der Smartcardautorisierung ist dies die bekannte SID (S-1-5-65-1), die smartcardbasierten Anmeldungen

zuordnet ist. Diese SID ist im Kerberos-Token eines DirectAccess-Clients vorhanden und wird als "dieses Organisations Zertifikat" bezeichnet, wenn Sie in den globalen IPsec-tunnelmodusautorisierungs-Einstellungen konfiguriert ist.

Wenn Sie die Smartcard-Autorisierung in Schritt 2 des DirectAccess-Setup-Assistenten aktivieren, konfiguriert der DirectAccess-Setup-Assistent die globale IPsec-tunnelmodusautorisierungseinstellung mit dieser sid für das Gruppenrichtlinie Objekt des DirectAccess-Servers. Führen Sie die folgenden Schritte aus, um diese Konfiguration im Snap-in "Windows-Firewall mit erweiterter Sicherheit" für das Objekt "DirectAccess-Server Gruppenrichtlinie" anzuzeigen:

1. Klicken Sie mit der rechten Maustaste auf Windows-Firewall mit erweiterter Sicherheit, und klicken Sie dann auf Eigenschaften.
2. Klicken Sie auf der Registerkarte IPsec-Einstellungen unter IPsec-Tunnel Autorisierung auf anpassen.
3. Klicken Sie auf die Registerkarte Benutzer. Als autorisierter Benutzer sollte "NT-Autorität \ dieses Organisations Zertifikat" angezeigt werden.

# Schritt 4 Überprüfen von DirectAccess mit OTP

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie überprüfen können, ob Sie DirectAccess mit OTP-Bereitstellung ordnungsgemäß konfiguriert haben.

## So überprüfen Sie die OTP-Integrität auf dem Remote Zugriffs Server

1. Öffnen Sie auf dem Remote Zugriffs Server die **Remote Zugriffs-Verwaltungs Konsole**.
2. Klicken Sie unter **Remote Zugriffs Server** auf den Remote Zugriffs Server, der für die OTP-Unterstützung konfiguriert wurde.
3. Klicken Sie auf **Vorgangs Status**.
4. Vergewissern Sie sich, dass der Status von OTP das grüne Symbol anzeigt und funktioniert.

### NOTE

Das Aktualisierungs Intervall für den Integritäts Status ist ein Maximum der Summe der Werte aus dem Registrierungsschlüssel `hklm\SYSTEM\CCS\services\ramgmsvc\parameters\healthrefreshtimeout` und dem **Zeitintervall für die Serveraktivität**, das in der Konfiguration des Remote Zugriffs festgelegt wurde.

## So überprüfen Sie den Zugriff auf interne Ressourcen mithilfe der OTP-Authentifizierung

1. Verbinden Sie einen DirectAccess-Client Computer mit dem Unternehmensnetzwerk, und führen Sie `gpupdate/force` an der Eingabeaufforderung aus, um die Gruppenrichtlinie zu erhalten.
2. Trennen Sie den Client Computer vom Unternehmensnetzwerk, stellen Sie eine Verbindung mit dem externen Netzwerk her, und versuchen Sie, auf interne Ressourcen zuzugreifen. Sie sollten keinen Zugriff auf die internen Ressourcen haben.
3. Im Fall eines Software Tokens greifen Sie mithilfe der Anweisungen des Anbieters auf das OTP-Client Token zu, und notieren Sie sich den aktuellen Tokencode. Wenn ein Hardware Token verwendet wird, befolgen Sie die Anweisungen des Herstellers für die Authentifizierung.
4. Klicken Sie im Infobereich auf das Symbol **Netzwerkverbindungen**, um auf die DirectAccess-Medienverwaltung zuzugreifen.
5. Klicken Sie auf die **DirectAccess-Verbindung**, und klicken Sie auf **weiter**.
6. Geben Sie den zuvor notierten Tokencode ein, und klicken Sie auf **OK**. Warten Sie, bis die Authentifizierung fertiggestellt ist. Der Status der DirectAccess-Arbeitsplatz Verbindung wird nun **verbunden**.
7. Es wurde versucht, auf interne Ressourcen zuzugreifen. Sie sollten auf alle Unternehmensressourcen zugreifen können.

# Problembehandlung bei einer OTP-Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie die häufigsten Fehler beheben können, die beim Konfigurieren einer Remote Zugriffs Bereitstellung mit OTP-Authentifizierung auftreten können.

- [Problembehandlung bei Authentifizierungs Problemen](#)
- [Problembehandlung beim Aktivieren von OTP](#)

# Problembehandlung bei Authentifizierungsfehlern

09.04.2020 • 21 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zur Problembehandlung bei Problemen im Zusammenhang mit Problemen, die Benutzer möglicherweise bei der Verbindungs Herstellung mit DirectAccess mithilfe der OTP-Authentifizierung haben. Directaccesss OTP-bezogene Ereignisse werden auf dem Client Computer in Ereignisanzeige unter **Anwendungs- und Dienst Protokolle/Microsoft/Windows/otpkredentialprovider** protokolliert. Stellen Sie sicher, dass dieses Protokoll bei der Behandlung von Problemen mit DirectAccess OTP aktiviert ist.

## Fehler beim Zugriff auf die Zertifizierungsstelle, die OTP-Zertifikate ausgibt.

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Fehler bei der OTP-Zertifikat Registrierung für die Benutzer auf dem Zertifizierungsstellen Server < CA\_name >, Anforderung fehlgeschlagen, mögliche Ursachen für Fehler: der ZS-Servername kann nicht aufgelöst werden. der Zugriff auf den Zertifizierungsstellen Server ist über den ersten DirectAccess-Tunnel nicht möglich, oder die Verbindung mit dem Zertifizierungsstellen Server kann nicht

### Ursache

Der Benutzer hat ein gültiges einmal Kennwort angegeben, und der DirectAccess-Server hat die Zertifikat Anforderung signiert. der Client Computer kann jedoch keine Verbindung mit der Zertifizierungsstelle hergestellt werden, die OTP-Zertifikate ausgibt, um den Registrierungsvorgang abzuschließen.

### Lösung

Führen Sie auf dem DirectAccess-Server die folgenden Windows PowerShell-Befehle aus:

1. Hier finden Sie die Liste der konfigurierten OTP-ausstellenden Zertifizierungsstellen und den Wert von "caserver": `Get-DAOtpAuthentication`
2. Stellen Sie sicher, dass die Zertifizierungsstellen als Verwaltungs Server konfiguriert sind:  
`Get-DAMgmtServer -Type All`
3. Stellen Sie sicher, dass der Client Computer den Infrastruktur Tunnel eingerichtet hat: Erweitern Sie in der Konsole Windows-Firewall mit erweiterter Sicherheit den Knoten **Überwachung/Sicherheits Zuordnungen**, klicken Sie auf **Hauptmodus**, und stellen Sie sicher, dass die IPSec-Sicherheits Zuordnungen mit den korrekten Remote Adressen für die DirectAccess-Konfiguration angezeigt werden

## Konnektivitätsprobleme beim DirectAccess-Server

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

### Fehler empfangen (Client Ereignisprotokoll)

Einer der folgenden Fehler:

- Es kann keine Verbindung mit dem RAS-Server hergestellt werden, < DirectAccess\_server\_hostname >

mithilfe von Basispfad < OTP\_authentication\_path > und Port < OTP\_authentication\_port >. Fehlercode: < internal\_error\_code >.

- Benutzer Anmelde Informationen können nicht an den RAS-Server gesendet werden < DirectAccess\_server\_hostname > mithilfe von Basispfad < OTP\_authentication\_path > und Port < OTP\_authentication\_port >. Fehlercode: < internal\_error\_code >.
- Es wurde keine Antwort vom RAS-Server < DirectAccess\_server\_hostname > mithilfe von Basispfad < OTP\_authentication\_path > und Port < OTP\_authentication\_port > empfangen. Fehlercode: < internal\_error\_code >.

#### Ursache

Der Client Computer kann aufgrund von Netzwerkproblemen oder eines falsch konfigurierten IIS-Servers auf dem DirectAccess-Server nicht über das Internet auf den DirectAccess-Server zugreifen.

#### Lösung

Stellen Sie sicher, dass die Internet Verbindung auf dem Client Computer funktioniert, und stellen Sie sicher, dass der DirectAccess-Dienst ausgeführt wird und über das Internet erreichbar ist.

## Fehler beim Registrieren für das Anmeldezertifikat für das DirectAccess-OTP.

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Fehler bei der Zertifikat Registrierung von der Zertifizierungsstelle < CA\_name >. Die Anforderung wurde vom OTP-Signaturzertifikat nicht erwartungsgemäß signiert, oder der Benutzer verfügt nicht über die Berechtigung, sich zu registrieren.

#### Ursache

Das vom Benutzer bereitgestellte einmalige Kennwort war richtig, aber die ausstellende Zertifizierungsstelle hat das Ausstellen des OTP-Anmelde Zertifikats verweigert. Die Zertifikat Anforderung ist möglicherweise nicht ordnungsgemäß mit der richtigen EKU-Anwendungs Richtlinie (OTP-Registrierungsstelle) signiert, oder der Benutzer verfügt nicht über die Berechtigung "registrieren" für die Vorlage "da OTP".

#### Lösung

Stellen Sie sicher, dass DirectAccess-OTP-Benutzer über die Berechtigung zum Registrieren für das Registrierungszertifikat für das DirectAccess-OTP verfügen, und dass die richtige "Anwendungs Richtlinie" in der Signatur Vorlage der Registrierungsstelle für die Registrierungsstelle enthalten ist. Stellen Sie außerdem sicher, dass das DirectAccess-Registrierungsstellen Zertifikat auf dem RAS-Server gültig ist. Weitere Informationen finden Sie unter 3,2 Planen der OTP-Zertifikat Vorlage und 3,3 Planen des Registrierungsstellen Zertifikats.

## Fehlendes oder ungültiges Computer Konto Zertifikat

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Die OTP-Authentifizierung kann nicht abgeschlossen werden, da das für OTP erforderliche Computer Zertifikat im Zertifikat Speicher des lokalen Computers nicht gefunden werden kann.

#### Ursache

Für die DirectAccess-OTP-Authentifizierung ist ein Client Computer Zertifikat erforderlich, um eine SSL-Verbindung mit dem DirectAccess-Server herzustellen. das Zertifikat des Client Computers wurde jedoch nicht gefunden oder

ist ungültig, z. B. wenn das Zertifikat abgelaufen ist.

## Lösung

Stellen Sie sicher, dass das Computer Zertifikat vorhanden und gültig ist:

1. Öffnen Sie auf dem Client Computer in der MMC-Zertifikat Konsole für das lokale Computer Konto "persönlich/Zertifikate".
2. Stellen Sie sicher, dass ein Zertifikat ausgestellt wurde, das mit dem Computernamen übereinstimmt, und doppelklicken Sie auf das Zertifikat.
3. Vergewissern Sie sich, dass im Dialogfeld **Zertifikat** auf der Registerkarte **Zertifikat Pfad** unter **Zertifikat Status** die Meldung "dieses Zertifikat ist OK" angezeigt wird.

Wenn kein gültiges Zertifikat gefunden wird, löschen Sie das ungültige Zertifikat (sofern vorhanden), und melden Sie sich erneut für das Computer Zertifikat an, indem Sie `gpupdate /Force` an einer Eingabeaufforderung mit erhöhten Rechten ausführen oder den Client Computer neu starten.

## Fehlende Zertifizierungsstelle, die OTP-Zertifikate ausgibt

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Die OTP-Authentifizierung kann nicht abgeschlossen werden, da der da-Server keine Adresse einer ausstellenden Zertifizierungsstelle zurückgegeben hat.

## Ursache

Entweder gibt es keine Zertifizierungsstellen, die OTP-Zertifikate ausstellen, oder alle konfigurierten Zertifizierungsstellen, die OTP-Zertifikate ausstellen, werden nicht reagiert.

## Lösung

1. Verwenden Sie den folgenden Befehl, um die Liste der Zertifizierungsstellen zu erhalten, die OTP-Zertifikate ausstellen (der Name der Zertifizierungsstelle wird unter caserver angezeigt): `Get-DAOtpAuthentication`.
2. Wenn keine Zertifizierungsstellen konfiguriert sind:
  - a. Verwenden Sie entweder den Befehl `Set-DAOtpAuthentication` oder die Remote Zugriffs-Verwaltungskonsole, um die Zertifizierungsstellen zu konfigurieren, die das Registrierungszertifikat für das DirectAccess-OTP ausstellen.
  - b. Wenden Sie die neue Konfiguration an, und erzwingen Sie, dass die Clients die DirectAccess-GPO-Einstellungen aktualisieren, indem Sie `gpupdate /Force` über eine Eingabeaufforderung mit erhöhten Rechten ausführen oder den Client Computer neu starten.
3. Wenn CAS konfiguriert sind, stellen Sie sicher, dass Sie online sind und auf Registrierungsanforderungen reagieren.

## Falsch konfigurierte DirectAccess-Server Adresse

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Die OTP-Authentifizierung kann nicht wie erwartet ausgeführt werden. Der Name oder die Adresse des Remote Zugriffs Servers kann nicht bestimmt werden. Fehlercode: < error\_code >. Die DirectAccess-Einstellungen sollten vom Server Administrator überprüft werden.

## Ursache

Die Adresse des DirectAccess-Servers ist nicht ordnungsgemäß konfiguriert.

## Lösung

Überprüfen Sie die konfigurierte DirectAccess-Server Adresse mithilfe `Get-DirectAccess`, und korrigieren Sie die Adresse, wenn Sie falsch konfiguriert ist.

Stellen Sie sicher, dass die neuesten Einstellungen auf dem Client Computer bereitgestellt werden, indem Sie `gpupdate /force` über eine Eingabeaufforderung mit erhöhten Rechten ausführen oder den Client Computer neu starten.

# Die OTP-Anmeldezertifikat Anforderung konnte nicht generiert werden.

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Die Zertifikat Anforderung für die OTP-Authentifizierung kann nicht initialisiert werden. Ein privater Schlüssel kann nicht generiert werden, oder Benutzer nicht auf die Zertifikat Vorlage zugreifen können <OTP\_template\_name> auf dem Domänen Controller.

## Ursache

Für diesen Fehler gibt es zwei mögliche Ursachen:

- Der Benutzer verfügt nicht über die Berechtigung zum Lesen der OTP-Anmeldevorlage.
- Der Computer des Benutzers kann aufgrund von Netzwerkproblemen nicht auf den Domänen Controller zugreifen.

## Lösung

- Überprüfen Sie die Berechtigungseinstellung für die OTP-Anmeldevorlage, und stellen Sie sicher, dass alle Benutzer, die für DirectAccess OTP bereitgestellt wurden, über die Berechtigung Lesen verfügen.
- Stellen Sie sicher, dass der Domänen Controller als Management Server konfiguriert ist und dass der Client Computer den Domänen Controller über den Infrastruktur Tunnel erreichen kann. Weitere Informationen finden Sie unter 3,2 Planen der OTP-Zertifikat Vorlage.

# Keine Verbindung mit dem Domänen Controller

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Eine Verbindung mit dem Domänen Controller zum Zweck der OTP-Authentifizierung kann nicht hergestellt werden. Fehlercode: <error\_code>.

## Ursache

Für diesen Fehler gibt es zwei mögliche Ursachen:

- Der Computer des Benutzers verfügt über keine Netzwerk Konnektivität.
- Der Domänen Controller ist über den Infrastruktur Tunnel nicht erreichbar.

## Lösung

- Stellen Sie sicher, dass der Domänen Controller als Management Server konfiguriert ist, indem Sie den folgenden Befehl an einer PowerShell-Eingabeaufforderung ausführen: `Get-DAMgmtServer -Type All`.
- Stellen Sie sicher, dass der Client Computer den Domänen Controller über den Infrastruktur Tunnel erreichen

kann.

## Der OTP-Anbieter erfordert Challenge/Response.

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Die OTP-Authentifizierung mit dem Remote Zugriffs Server (<DirectAccess\_server\_name >) für den Benutzer () erforderte eine Herausforderung des Benutzers.

### Ursache

Der verwendete OTP-Anbieter erfordert, dass der Benutzer zusätzliche Anmelde Informationen in Form eines RADIUS-Challenge/Antwort-Austauschs bereitstellt, der von Windows Server 2012 DirectAccess OTP nicht unterstützt wird.

### Lösung

Konfigurieren Sie den OTP-Anbieter so, dass in keinem Szenario Challenge/Response erforderlich ist.

## Falsche OTP-Anmeldevorlage verwendet

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Die Zertifizierungsstellen Vorlage, von der die Benutzer ein Zertifikat angefordert hat, ist nicht für das Ausstellen von OTP-Zertifikaten konfiguriert.

### Ursache

Die "DirectAccess OTP"-Anmeldevorlage wurde ersetzt, und der Client Computer versucht, sich mit einer älteren Vorlage zu authentifizieren.

### Lösung

Stellen Sie sicher, dass der Client Computer die neueste OTP-Konfiguration verwendet, indem Sie eine der folgenden Aktionen ausführen:

- Erzwingen Sie eine Gruppenrichtlinie Aktualisierung, indem Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten ausführen: `gpupdate /Force`.
- Starten Sie den Clientcomputer neu.

## Fehlendes OTP-Signaturzertifikat

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Ereignisprotokoll). Ein OTP-Signaturzertifikat wurde nicht gefunden. Die OTP-Zertifikat Registrierungs Anforderung kann nicht signiert werden.

### Ursache

Das Registrierungszertifikat für den DirectAccess-OTP wurde auf dem Remote Zugriffs Server nicht gefunden. Daher kann die Benutzerzertifikat Anforderung nicht vom RAS-Server signiert werden. Entweder ist kein Signaturzertifikat vorhanden, oder das Signaturzertifikat ist abgelaufen und wurde nicht erneuert.

### Lösung

Führen Sie diese Schritte auf dem Remote Zugriffs Server aus.

1. Überprüfen Sie den Namen der konfigurierten OTP-Signaturzertifikat Vorlage, indem Sie das PowerShell-Cmdlet `Get-DAOtpAuthentication` ausführen und den Wert `SigningCertificateTemplateName` überprüfen.
2. Verwenden Sie das MMC-Snap-in Zertifikate, um sicherzustellen, dass auf dem Computer ein gültiges Zertifikat vorhanden ist, das bei dieser Vorlage registriert ist.
3. Wenn ein solches Zertifikat nicht vorhanden ist, löschen Sie das abgelaufene Zertifikat (sofern vorhanden), und registrieren Sie sich für ein neues Zertifikat auf der Grundlage dieser Vorlage.

Informationen zum Erstellen der OTP-Signaturzertifikat Vorlage finden Sie unter 3,3 Planen des Registrierungsstellen Zertifikats.

## Fehlender oder falscher UPN/DN für den Benutzer.

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

### Fehler empfangen (Client Ereignisprotokoll)

Einer der folgenden Fehler:

- Benutzer können nicht mit OTP authentifiziert werden. Stellen Sie sicher, dass ein UPN für den Benutzernamen in Active Directory definiert ist. Fehlercode: < error\_code >.
- Benutzer können nicht mit OTP authentifiziert werden. Stellen Sie sicher, dass für den Benutzernamen in Active Directory ein DN definiert ist. Fehlercode: < error\_code >.

### Fehler empfangen (Server Ereignisprotokoll)

Der für die OTP-Authentifizierung angegebene Benutzername nicht vorhanden.

### Ursache

Der Benutzer verfügt nicht über die ordnungsgemäße Festlegung der Benutzer Principal Namen (UPN) oder DN-Attribute (DN) im Benutzerkonto. Diese Eigenschaften sind für eine ordnungsgemäße Funktionsweise von DirectAccess OTP erforderlich.

### Lösung

Überprüfen Sie mithilfe der Konsole Active Directory Benutzer und Computer auf dem Domänen Controller, ob beide Attribute ordnungsgemäß für den authentifizierenden Benutzer festgelegt sind.

## OTP-Zertifikat ist für die Anmeldung nicht vertrauenswürdig.

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

### Ursache

Die Zertifizierungsstelle, die OTP-Zertifikate ausgibt, befindet sich nicht im Enterprise NTAuth-Speicher. Daher können registrierte Zertifikate nicht für die Anmeldung verwendet werden. Dies kann in Umgebungen mit mehreren Domänen und mehreren Gesamtstrukturen vorkommen, in denen keine Domänen übergreifende Zertifizierungsstellen-Vertrauensstellung eingerichtet ist.

### Lösung

Stellen Sie sicher, dass das Zertifikat des Stamms der Zertifizierungsstellen Hierarchie, von der OTP-Zertifikate ausgestellt werden, im NTAuth-Zertifikat Speicher des Unternehmens der Domäne installiert ist, zu der der Benutzer eine Authentifizierung durchführen soll.

# Die Benutzer Anmelde Informationen konnten nicht überprüft werden.

**Szenario.** Der Benutzer kann sich nicht mit OTP authentifizieren, weil der folgende Fehler aufgetreten ist:  
"Authentifizierung aufgrund eines internen Fehlers fehlgeschlagen"

**Fehler** (Client Computer). Es ist ein Fehler aufgetreten, während Windows Ihre Anmelde Informationen überprüfte.  
Versuchen Sie es erneut, oder bitten Sie Ihren Administrator um Hilfe.

## Ursache

Das Kerberos-Authentifizierungsprotokoll funktioniert nicht, wenn das Registrierungszertifikat für den DirectAccess-OTP keine CRL enthält. Das Registrierungszertifikat für das DirectAccess-OTP enthält keine CRL:

- Die "DirectAccess OTP"-Anmeldevorlage wurde mit der Option "**keine Sperrinformationen in ausgestellten Zertifikaten einschließen**" konfiguriert.
- Die Zertifizierungsstelle ist so konfiguriert, dass keine CRLs veröffentlicht werden.

## Lösung

1. Um die Ursache für diesen Fehler zu überprüfen, klicken Sie in der Remote Zugriffs-Verwaltungskonsole in **Schritt 2RAS-Server auf Bearbeiten**, und klicken Sie dann im Setup-Assistenten für den **Remote Zugriffs Server auf OTP-Zertifikat Vorlagen**. Notieren Sie sich die Zertifikat Vorlage, die für die Registrierung von Zertifikaten verwendet wird, die für die OTP-Authentifizierung ausgestellt werden. Öffnen Sie die Zertifizierungsstellen Konsole, klicken Sie im linken Bereich auf **Zertifikat Vorlagen**, doppelklicken Sie auf das OTP-Anmeldezertifikat, um die Eigenschaften der Zertifikat Vorlage anzuzeigen.

Um dieses Problem zu beheben, konfigurieren Sie ein Zertifikat für das OTP-Anmeldezertifikat, und aktivieren Sie im Dialogfeld Vorlagen Eigenschaften auf der Registerkarte **Server** das Kontrollkästchen **Sperr Informationen in ausgestellten Zertifikaten einschließen**.

2. Öffnen Sie auf dem Zertifizierungsstellen Server die MMC der Zertifizierungsstelle, klicken Sie mit der rechten Maustaste auf die ausstellende Zertifizierungsstelle **und klicken** Vergewissern Sie sich auf der Registerkarte **Erweiterungen**, dass die CRL-Veröffentlichung ordnungsgemäß konfiguriert ist.

# Problembehandlung bei der Aktivierung von OTP

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält Informationen zur Problembehandlung bei Problemen im Zusammenhang mit dem Aktivieren der DirectAccess-OTP-Authentifizierung über das PowerShell-Cmdlet " `enable-daotpauthentication` " oder über die Remote Zugriffs-Verwaltungskonsole.

## Fehler beim Registrieren des OTP-Signatur Zertifikats.

**Fehler** (Server Ereignisprotokoll). Ein OTP-Signaturzertifikat kann nicht mithilfe der Zertifikat Vorlage < `OTP_signing_template_name` registriert werden >

### Ursache

Für diesen Fehler gibt es drei mögliche Ursachen:

- Die Vorlage ist nicht vorhanden.
- Die in der Vorlage festgelegten Berechtigungen lassen nicht zu, dass sich der DirectAccess-Server registrieren kann.
- Es ist keine Netzwerkverbindung mit der ausstellenden Zertifizierungsstelle (Certification Authority, ca) vorhanden.

### Lösung

1. Stellen Sie sicher, dass die OTP-Signaturzertifikat Vorlage mit dem angegebenen Namen lautet:
  - a. Ist vorhanden und verfügt über die entsprechenden Berechtigungen.
  - b. Ist so festgelegt, dass Sie von mindestens einer Zertifizierungsstelle ausgestellt wird, die Zertifikate an den DirectAccess-Server ausstellen kann.
2. Wenn die Vorlage nicht vorhanden ist, erstellen Sie sie wie in 3,3 Planen des Registrierungsstellen Zertifikats beschrieben. Wenn eine andere entsprechende Vorlage vorhanden ist, konfigurieren Sie DirectAccess OTP mit dem neuen Vorlagen Namen neu.

## Fehler beim Aktivieren von DirectAccess OTP, wenn WebDAV installiert ist.

**Szenario.** Beim Versuch, die Konfiguration von DirectAccess OTP in der Remote Zugriffs-Verwaltungskonsole oder mithilfe des `Enable-DAOtpAuthentication` PowerShell-Cmdlets anzuwenden, schlägt der Vorgang fehl.

**Fehler** (Server Ereignisprotokoll). DirectAccess-OTP-Einstellungen können nicht angewendet werden, weil die WebDAV-IIS-Erweiterung auf dem Server ausgeführt wird. Entfernen Sie WebDAV, und wenden Sie die Einstellungen erneut an.

### Ursache

Der DirectAccess-OTP-Dienst ist nicht mit der WebDAV-Veröffentlichungs Funktion kompatibel und kann nicht aktiviert werden, während WebDAV installiert ist.

## Lösung

Deinstallieren Sie die WebDAV-Rolle:

1. Klicken Sie in der Server-Manager Konsole im linken Bereich auf **IIS**.
2. Scrollen Sie im Hauptbereich zu **Rollen und Features**.
3. Klicken Sie mit der rechten Maustaste auf **WebDAV-Veröffentlichung**, und klicken Sie dann auf **Rolle oder Feature entfernen**.
4. Vervollständigen Sie den Assistenten zum Entfernen von Rollen und Features.
5. Wenden Sie die Konfiguration von DirectAccess OTP erneut an.

## In der Remote Zugriffs-Verwaltungskonsole sind keine Vorlagen verfügbar.

**Szenario.** Beim Konfigurieren von OTP-oder Registrierungsstellen-Zertifikat Vorlagen mithilfe der Remote Zugriffs-Verwaltungskonsole fehlen einige oder alle Vorlagen in den Auswahl Fenstern.

## Ursache

Für diesen Fehler gibt es zwei mögliche Ursachen:

- Die Vorlage ist nicht gemäß den Anforderungen des DirectAccess-OTP konfiguriert und kann daher nicht ausgewählt werden.
- Die ausgewählten Zertifizierungsstellen unter den **OTP -Zertifizierungsstellen** Servern sind nicht so konfiguriert, dass die erforderlichen Vorlagen ausgestellt werden.

## Lösung

1. Stellen Sie sicher, dass die OTP-Anmeldevorlage und die OTP-Signaturzertifikat Vorlage ordnungsgemäß konfiguriert sind, wie in 3,2 Planen der OTP-Zertifikat Vorlage und 3,3 Planen des Registrierungsstellen Zertifikats beschrieben.
2. Stellen Sie sicher, dass die konfigurierten Zertifizierungsstellen in der Liste der **OTP -Zertifizierungsstellen** Server so konfiguriert sind, dass Sie die relevanten Vorlagen
  - a. Öffnen Sie auf dem Zertifizierungsstellen Server die Konsole Zertifizierungsstelle.
  - b. Erweitern Sie im linken Bereich den ausgewählten Zertifizierungsstellen Server.
  - c. Klicken Sie auf **Zertifikat Vorlagen**, und stellen Sie sicher, dass die erforderlichen Vorlagen aktiviert sind. Falls nicht, klicken Sie mit der rechten Maustaste auf **Zertifikat Vorlagen**, klicken Sie auf **neu**, dann auf Auszustellende **Zertifikat Vorlage**, und wählen Sie dann die Vorlagen aus, die Sie aktivieren möchten.

## Erneuerungs Zeitraum der OTP-Vorlage kann nicht auf 1 Stunde festgelegt werden.

**Szenario.** Bei der Konfiguration der DirectAccess OTP-Anmeldevorlage mithilfe von Windows 2003 ca ist es nicht möglich, den Erneuerungs Zeitraum der Vorlage auf 1 Stunde festzulegen.

## Ursache

Mit dem MMC-Snap-in "Zertifikat Vorlagen" in Windows Server 2003 können Sie den Erneuerungs Zeitraum einer Vorlage nicht auf eine Stunde festlegen.

## Lösung

Installieren Sie das Zertifikat Vorlagen-Snap-in auf einem Post-Windows Server 2003-Server, und verwenden Sie es zum Konfigurieren der OTP-Anmeldevorlage. Weitere Informationen finden Sie unter [Installieren des Zertifikat Vorlagen-Snap-Ins](#)

# Bereitstellen von Remotezugriff in einer Umgebung mit mehreren Gesamtstrukturen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die Remote Zugriffs-Konfigurationstools (die Remote Zugriffs-Verwaltungskonsole und die Windows PowerShell-Cmdlets) sind so konzipiert, dass Sie in einer Umgebung mit einer einzelnen Gesamtstruktur mit einer oder mehreren Domänen ordnungsgemäß funktionieren. Wird der Remotezugriff jedoch in einer Umgebung mit mehreren Gesamtstrukturen bereitgestellt, muss der Remotezugriffsadministrator für eine erfolgreiche Bereitstellung eine manuelle Konfiguration ausführen. In diesem Handbuch werden die Planungs- und Konfigurationsschritte für eine Bereitstellung mit mehreren Gesamtstrukturen aufgeführt. Unter anderem wird auch erläutert, wann die Authentifizierung mit Einmalkennwörtern (One-Time Password, OTP) verwendet wird.

- [Planen einer Bereitstellung mit mehreren Gesamtstrukturen](#)
- [Konfigurieren einer Bereitstellung mit mehreren Gesamtstrukturen](#)

# Planen einer Bereitstellung mit mehreren Gesamtstrukturen

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema werden die zum Konfigurieren des Remotezugriffs für eine Bereitstellung mit mehreren Gesamtstrukturen erforderlichen Planungsschritte beschrieben.

## Erforderliche Komponenten

Bevor Sie mit der Bereitstellung dieses Szenarios beginnen, sollten Sie die Liste der wichtigen Anforderungen lesen:

- Eine bidirektionale Vertrauensstellung ist erforderlich.

## Planen von Vertrauensstellungen zwischen Gesamtstrukturen

Wenn Sie den Zugriff auf Ressourcen von einer neuen Gesamtstruktur ermöglichen, für Clients aus der neuen Gesamtstruktur die Verwendung von DirectAccess zulassen oder RAS-Server in der neuen Gesamtstruktur als Einstiegspunkte für die Remotezugriffsbereitstellung hinzufügen möchten, muss eine volle Vertrauenswürdigkeit, d. h. eine bidirektionale transitive Vertrauensstellung, zwischen den beiden Gesamtstrukturen konfiguriert werden. Informationen hierzu finden Sie unter [Vertrauenstypen](#). Die volle Vertrauenswürdigkeit zwischen Gesamtstrukturen ist die Voraussetzung dafür, dass in einer Bereitstellung mit mehreren Gesamtstrukturen Administratoren bestimmte Vorgänge ausführen können. Zu diesen Vorgängen gehören das Bearbeiten von Gruppenrichtlinienobjekten in der neuen Gesamtstruktur, das Verwenden von Sicherheitsgruppen aus der neuen Gesamtstruktur als Clientsicherheitsgruppe, Ausführen von Remoteaufrufen (WinRM, RPC) von Computern in der neuen Gesamtstruktur und Authentifizieren von Remoteclients in der neuen Gesamtstruktur.

## Planen der Administratorberechtigungen für den Remotezugriff

Beim Konfigurieren des Remotezugriffs werden Gruppenrichtlinienobjekte aktualisiert und manchmal in den einzelnen Domänen erstellt, die RAS-Server oder Remotezugriffsclients enthalten. In einer Umgebung mit mehreren Gesamtstrukturen muss der Remotezugriffsadministrator genau wie in einer Umgebung mit einer Gesamtstruktur über Berechtigungen zum Schreiben und Ändern von DirectAccess-Gruppenrichtlinienobjekten und ihren Sicherheitsfiltern verfügen. Optional muss er Berechtigungen zum Erstellen von Links für die DirectAccess-Gruppenrichtlinienobjekte in allen betroffenen Gesamtstrukturen besitzen. Diese Berechtigungen sind unabhängig von der Gesamtstruktur erforderlich, zu der der Remotezugriffsadministrator gehört.

Darüber hinaus muss es sich beim Remotezugriffsadministrator um einen lokalen Administrator für alle RAS-Server handeln, einschließlich der RAS-Server in der neuen Gesamtstruktur, die als Einstiegspunkte zur ursprünglichen Remotezugriffsbereitstellung hinzugefügt werden.

## Planen von Client Sicherheitsgruppen

Sie müssen mindestens eine Sicherheitsgruppe in der neuen Gesamtstruktur für DirectAccess-Clientcomputer in der neuen Gesamtstruktur konfigurieren. Eine einzelne Sicherheitsgruppe kann keine Konten aus verschiedenen Gesamtstrukturen enthalten.

#### **NOTE**

- Für DirectAccess ist mindestens eine Windows 10-®-oder Windows® 8-Client Sicherheitsgruppe für jede Gesamtstruktur erforderlich. Es wird jedoch empfohlen, eine Windows 10- oder Windows 8-Client Sicherheitsgruppe für jede Domäne zu haben, die Windows 10- oder Windows 8-Clients enthält.
- Wenn mehrere Standorte aktiviert sind, ist für DirectAccess mindestens eine Windows 7-® Client Sicherheitsgruppe pro Gesamtstruktur für jeden DirectAccess-Einstiegspunkt erforderlich, auf dem Windows 7-Client Computer unterstützt werden. Es wird jedoch empfohlen, eine separate Windows 7-Client Sicherheitsgruppe für jeden Einstiegspunkt für jede Domäne zu haben, die Windows 7-Clients enthält.

Damit DirectAccess auf Clientcomputer in zusätzlichen Domänen angewendet wird, müssen Client-Gruppenrichtlinienobjekte in diesen Domänen erstellt werden. Durch das Hinzufügen von Sicherheitsgruppen wird das Schreiben neuer Client-Gruppenrichtlinienobjekte für die neuen Domänen ausgelöst. Wenn Sie der Liste der Sicherheitsgruppen für DirectAccess-Clients eine neue Sicherheitsgruppe aus einer neuen Domäne hinzufügen, wird daher automatisch ein Client-Gruppenrichtlinienobjekt in der neuen Domäne erstellt. Clientcomputer in der neuen Domäne erhalten die DirectAccess-Einstellungen über das Client-Gruppenrichtlinienobjekt.

Wenn Sie einer vorhandenen Sicherheitsgruppe, die bereits als Sicherheitsgruppe für DirectAccess-Clients konfiguriert ist, einen Client aus einer neuen Domäne hinzufügen, wird das Client-Gruppenrichtlinienobjekt nicht automatisch von DirectAccess in der neuen Domäne erstellt. Der Client in der neuen Domäne erhält nicht die DirectAccess-Einstellungen und kann daher keine Verbindung mithilfe von DirectAccess herstellen.

## Planen von Zertifizierungsstellen

Ist die DirectAccess-Bereitstellung für die Verwendung der Authentifizierung mit Einmalkennwörtern (One-Time Password, OTP) konfiguriert, enthält jede Gesamtstruktur die gleichen Signaturzertifikatvorlagen. Diese Vorlagen enthalten jedoch unterschiedliche OID-Werte. Dies führt dazu, dass die Gesamtstrukturen nicht als eine Konfigurationseinheit konfiguriert werden können. Informationen zum Beheben dieses Problems und zum Konfigurieren von OTP in einer Umgebung mit mehreren Gesamtstrukturen finden Sie im Abschnitt "Konfigurieren von OTP in einer Bereitstellung mit mehreren Gesamtstrukturen" im Thema [Konfigurieren einer Bereitstellung mit mehreren Gesamtstrukturen](#).

Bei der Verwendung der IPsec-Computerzertifikatauthentifizierung muss auf allen Client- und Servercomputern (unabhängig von der Gesamtstruktur, zu der sie gehören) ein von derselben Stamm- oder Zwischenzertifizierungsstelle ausgestelltes Computerzertifikat vorhanden sein.

## Planen von OTP-Ausnahmen

Bei der Verwendung der DirectAccess-OTP-Authentifizierung ist die Sicherheitsgruppe für OTP-Ausnahmen auf Benutzer einer einzelnen Gesamtstruktur beschränkt. Dies liegt daran, dass jede Sicherheitsgruppe nur Benutzer aus einer einzelnen Gesamtstruktur enthalten und nur eine Sicherheitsgruppe konfiguriert werden kann.

# Configure a Multi-Forest Deployment

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie eine Remotezugriffsbereitstellung mit mehreren Gesamtstrukturen in verschiedenen möglichen Szenarien konfigurieren. In allen Szenarien wird davon ausgegangen, dass DirectAccess gegenwärtig in einer einzigen Gesamtstruktur mit dem Namen %&quot;Forest1%&quot; bereitgestellt ist und Sie DirectAccess für eine neue Gesamtstruktur mit dem Namen %&quot;Forest2%&quot; konfigurieren.

## Zugreifen auf Ressourcen von Forest2

In diesem Szenario ist DirectAccess bereits in %&quot;Forest1%&quot; bereitgestellt und so konfiguriert, dass Clients aus %&quot;Forest1%&quot; auf das Unternehmensnetzwerk zugreifen können. Clients, die eine Verbindung über DirectAccess herstellen, können standardmäßig nur auf Ressourcen in %&quot;Forest1%&quot; zugreifen und haben keinen Zugriff auf Server in %&quot;Forest2%&quot;.

**So ermöglichen Sie DirectAccess-Clients den Zugriff auf Ressourcen in %&quot;Forest2%&quot;**

1. Wenn das DNS-Suffix von %&quot;Forest2%&quot; nicht Teil des DNS-Suffix von %&quot;Forest1%&quot; ist, fügen Sie NRPT-Regeln mit den Suffixen der Domänen in %&quot;Forest2%&quot; hinzu, und fügen Sie optional die Suffixe der Domänen in %&quot;Forest2%&quot; der DNS-Suffixsuchliste hinzu.
2. Fügen Sie die entsprechenden internen IPv6-Präfixe in %&quot;Forest2%&quot; hinzu, wenn IPv6 im internen Netzwerk bereitgestellt ist.

## Aktivieren von Clients über Forest2 zum Herstellen einer Verbindung über DirectAccess

In diesem Szenario konfigurieren Sie die Remotezugriffsbereitstellung so, dass Clients in %&quot;Forest2%&quot; auf das Unternehmensnetzwerk zugreifen können. Es wird vorausgesetzt, dass Sie die erforderlichen Sicherheitsgruppen für Clientcomputer in %&quot;Forest2%&quot; erstellt haben.

**So ermöglichen Sie Clients in %&quot;Forest2%&quot; den Zugriff auf das Unternehmensnetzwerk**

1. Fügen Sie die Sicherheitsgruppe der Clients in %&quot;Forest2%&quot; hinzu.
2. Wenn das DNS-Suffix von Forest2 nicht Teil des DNS-Suffix von Forest1 ist, fügen Sie NRPT-Regeln mit den Suffixen der Domäne der Clients in Forest2 hinzu, um den Zugriff auf die Domänen Controller für die Authentifizierung zu aktivieren, und fügen Sie optional die Suffixe der Domänen in Forest2 dem DNS hinzu. Suffixsuchliste.
3. Fügen Sie die internen IPv6-Präfixe in %&quot;Forest2%&quot; hinzu, damit DirectAccess den IPsec-Tunnel zu den Domänencontrollern für die Authentifizierung erstellen kann.
4. Aktualisieren Sie die Liste der Verwaltungsserver.

## Hinzufügen von Einstiegspunkten aus Forest2

In diesem Szenario ist DirectAccess in einer Konfiguration für mehrere Standorte in

%%amp;quot;Forest1%%amp;quot; bereitgestellt und Sie möchten einen RAS-Server mit dem Namen %%amp;quot;DA2%%amp;quot; in %%amp;quot;Forest2%%amp;quot; als Einstiegspunkt zur vorhandenen DirectAccess-Bereitstellung für mehrere Standorte hinzufügen.

**So fügen Sie einen RAS-Server in %%amp;quot;Forest2%%amp;quot; als Einstiegspunkt hinzu**

1. Stellen Sie sicher, dass der Remotezugriffsadministrator über ausreichende Berechtigungen zum Schreiben von GPOs in der Domäne von %%amp;quot;DA2%%amp;quot; verfügt und ein lokaler Administrator auf %%amp;quot;DA2%%amp;quot; ist.
2. Fügen Sie DA2 als Einstiegspunkt hinzu.
3. Fügen Sie NRPT-Regeln mit den Suffixen der Domänen in %%amp;quot;Forest2%%amp;quot; hinzu, um den Zugriff auf die Domänencontroller für die Authentifizierung zu ermöglichen, und fügen Sie optional die Suffixe der Domänen in %%amp;quot;Forest2%%amp;quot; der DNS-Suffixsuchliste hinzu.
4. Fügen Sie ggf. die entsprechenden internen IPv6-Präfixe in %%amp;quot;Forest2%%amp;quot; hinzu, um dem Remotezugriff das Erstellen des IPsec-Tunnels zu den Unternehmensressourcen zu ermöglichen und sicherzustellen, dass NCSI-Tests korrekt funktionieren.
5. Aktualisieren Sie die Liste der Verwaltungsserver.

## Konfigurieren von OTP in einer Bereitstellung mit mehreren Gesamtstrukturen

Folgende Begriffe sind beim Konfigurieren von OTP (One-Time Password = Einmalkennwort) in einer Bereitstellung mit mehreren Gesamtstrukturen wichtig:

- Stamm Zertifizierungsstelle: die Gesamtstruktur der PKI-Struktur der Gesamtstruktur (en).
- Unternehmens Zertifizierungsstelle-alle anderen Zertifizierungsstellen.
- Ressourcen Gesamtstruktur: die Gesamtstruktur, die die Stamm Zertifizierungsstelle enthält und als "Verwaltung von forest\domain" angesehen wird.
- Konto Gesamtstruktur-alle anderen Gesamtstrukturen in der Topologie.

Für dieses Verfahren ist das PowerShell-Skript %%amp;quot;PKISync.ps1%%amp;quot; erforderlich. Weitere Informationen finden Sie unter [AD CS: Skript "PKISync.ps1" für die gesamtstrukturübergreifende Zertifikatregistrierung](#).

**NOTE**

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

### Konfigurieren von Zertifizierungsstellen als Zertifikat Verleger

1. Aktivieren Sie die LDAP-Weiterleitungsunterstützung für alle Unternehmenszertifizierungsstellen in allen Gesamtstrukturen, indem Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten ausführen:

```
certutil -setreg Policy>EditFlags +EDITF_ENABLELDAPREFERRALS
```

2. Fügen Sie alle Unternehmenszertifizierungsstellen-Computerkonten der Active Directory-Sicherheitsgruppe %%amp;quot;Zertifikatherausgeber%%amp;quot; in jeder der Kontengesamtstrukturen hinzu.

- Starten Sie alle Zertifikatdienste (certsvc) auf allen Zertifizierungsstellenscomputern in allen Gesamtstrukturen neu, indem Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten ausführen:

```
net stop certsvc && net start certsvc
```

- Extrahieren Sie das Stammzertifizierungsstellenzertifikat, indem Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten ausführen.

```
certutil -config <Computer-Name>\<Root-CA-Name> -ca.cert <root-ca-cert-filename.cer>
```

(Wenn Sie den Befehl auf der Stamm Zertifizierungsstelle ausführen, können Sie die Verbindungsinformationen auslassen,-config < Computer Name >\< root-ca-Name >).

- Importieren Sie das Stammzertifizierungsstellenzertifikat aus dem vorherigen Schritt auf der Zertifizierungsstelle der Kontengesamtstruktur, indem Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten ausführen:

```
certutil -dspublish -f <root-ca-cert-filename.cer> RootCA
```

- Erteilen Sie den Zertifikat Vorlagen der Ressourcen Gesamtstruktur Lese-/Schreibberechtigungen für die <Konto Gesamtstruktur>\< Administrator Konto>.
- Extrahieren Sie alle Unternehmenszertifizierungsstellenzertifikate der Ressourcengesamtstruktur, indem Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten ausführen.

```
certutil -config <Computer-Name>\<Enterprise-CA-Name> -ca.cert <enterprise-ca-cert-filename.cer>
```

(Wenn Sie den Befehl auf der Stamm Zertifizierungsstelle ausführen, können Sie die Verbindungsinformationen auslassen,-config < Computer Name >\< root-ca-Name >).

- Importieren Sie die Unternehmenszertifizierungsstellenzertifikate aus dem vorherigen Schritt auf der Zertifizierungsstelle der Kontengesamtstruktur, indem Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten ausführen:

```
certutil -dspublish -f <enterprise-ca-cert-filename.cer> NTAuthCA  
certutil -dspublish -f <enterprise-ca-cert-filename.cer> SubCA
```

- Entfernen Sie OTP-Zertifikatvorlagen der Kontengesamtstruktur aus der Liste ausgestellter Zertifikatvorlagen.

#### **Löschen und Importieren von OTP-Zertifikat Vorlagen**

- Löschen Sie OTP-Zertifikatvorlagen aus der Kontengesamtstruktur, d. h. aus %quot;Forest2%quot;.
- Kopieren Sie mithilfe der folgenden PowerShell-Befehle Zertifikatvorlagen und OID-Objekte aus der Ressourcengesamtstruktur in jede der Kontengesamtstrukturen:

```
.\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type Template -cn <DA OTP registration authority template common name>.  
.\\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type Template -cn <Secure DA OTP logon certificate template common name>.  
.\\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type Oid -f
```

## Veröffentlichen von OTP-Zertifikat Vorlagen

- Stellen Sie die neu importierten Zertifikatvorlagen auf allen Zertifizierungsstellen der Kontengesamtstrukturen aus.

## Extrahieren und Synchronisieren der Zertifizierungsstelle

1. Extrahieren Sie alle Unternehmenszertifizierungsstellenzertifikate aus den Kontengesamtstrukturen, indem Sie die folgenden Befehle an einer Eingabeaufforderung mit erhöhten Rechten ausführen:

```
certutil -config <Computer-Name>\<Enterprise-CA-Name> -ca.cert <enterprise-ca-cert-filename.cer>
```

2. Synchronisieren Sie Zertifizierungsstellen aus den Kontengesamtstrukturen mithilfe des folgenden PowerShell-Befehls gesamtstrukturübergreifend mit der Ressourcengesamtstruktur:

```
.\\PKISync.ps1 -sourceforest <account forest DNS> -targetforest <resource forest DNS> -type CA -cn <enterprise CA sanitized name> -f
```

3. Synchronisieren Sie Zertifizierungsstellen aus der Ressourcengesamtstruktur mithilfe des folgenden PowerShell-Befehls gesamtstrukturübergreifend mit den Kontengesamtstrukturen:

```
.\\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type CA -cn <enterprise CA sanitized name> -f
```

## Konfigurationsverfahren

In den folgenden Abschnitten werden die Konfigurationsverfahren für die Bereitstellungen in den obigen Szenarien beschrieben. Kehren Sie nach dem Ausführen eines Verfahrens zum Szenario zurück, um damit fortzufahren.

### Hinzufügen von NRPT-Regeln und DNS-Suffixen

Clients, die über DirectAccess eine Verbindung mit dem Unternehmensnetzwerk herstellen, verwenden die Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT), um zu ermitteln, welcher DNS-Server zum Auflösen der Adresse verschiedener Ressourcen verwendet werden sollte. Dies ermöglicht es dem Client, Adressen von Unternehmensressourcen aufzulösen und die für die einwandfreie Funktion von DirectAccess erforderliche Klassifizierung für Ressourcen innerhalb/außerhalb des Unternehmens aufrecht zu erhalten. Die DirectAccess-Konfigurationstools erkennen das DNS-Stammsuffix von %&quot;Forest1%&quot; automatisch und fügen es der NRPT-Tabelle hinzu. Die Suffixe des vollqualifizierten Domäennamens (Fully Qualified Domain Name, FQDN) von %&quot;Forest2%&quot; werden der NRPT-Tabelle jedoch nicht automatisch hinzugefügt und müssen manuell vom Remotezugriffsadministrator hinzugefügt werden.

Die DNS-Suffixsuchliste ermöglicht es den Clients, anstelle von FQDNs Kurznamen zu verwenden. Die Remotezugriffs-Konfigurationstools fügen der DNS-Suffixsuchliste automatisch alle Domänen in %&quot;Forest1%&quot; hinzu. Wenn Clients in der Lage sein sollen, Kurznamen für Ressourcen in %&quot;Forest2%&quot; zu verwenden, müssen Sie sie manuell hinzufügen.

So fügen Sie der NRPT-Tabelle ein DNS-Suffix und der DNS-Suffixsuchliste Domänensuffixe hinzu

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter Schritt 3

## Infrastrukturserver auf Bearbeiten.

2. Klicken Sie auf der Seite **Netzwerkadressenserver** auf **Weiter**.
3. Geben Sie auf der Seite **DNS** in der Tabelle alle zusätzlichen Namensuffixe ein, die Teil des Unternehmensnetzwerks in %&quot;Forest2%&quot; sind. Geben Sie in **DNS-Serveradresse** die Adresse des DNS-Servers manuell ein, oder klicken Sie auf **Erkennen**. Wenn Sie die Adresse nicht eingeben, werden die neuen Einträge als NRPT-Ausnahmen angewendet. Klicken Sie dann auf **Weiter**.
4. Optional: Fügen Sie auf der Seite **DNS-Suffixsuchliste** DNS-Suffixe hinzu, indem Sie das Suffix in das Feld **Neues Suffix** eingeben und dann auf **Hinzufügen** klicken. Klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite **Verwaltung** auf **Fertig stellen**.
6. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole auf **Fertig stellen**.
7. Klicken Sie im Dialogfeld **Überprüfung des Remotezugriffs** auf **Anwenden**.
8. Klicken Sie im Dialogfeld **Anwenden der Einstellungen zum Einrichten des Remotezugriffs** auf **Schließen**.

## Internes IPv6-Präfix hinzufügen

### NOTE

Das Hinzufügen eines internen IPv6-Präfix ist nur erforderlich, wenn IPv6 im internen Netzwerk bereitgestellt ist.

Der Remotezugriff verwaltet eine Liste von IPv6-Präfixen für Unternehmensressourcen. Clients, die über DirectAccess eine Verbindung herstellen, können nur auf Ressourcen mit diesen IPv6-Präfixen zugreifen. Da die Remote Zugriffs-Verwaltungskonsole und Windows PowerShell-Befehle die IPv6-Präfixe von Forest1 automatisch hinzufügen und die Präfixe anderer Gesamtstrukturen möglicherweise nicht hinzufügen, müssen Sie alle fehlenden Präfixe von Forest2 manuell hinzufügen.

### So fügen Sie ein IPv6-Präfix hinzu

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 2 RAS-Server** auf **Bearbeiten**.
2. Klicken Sie im Setup-Assistenten für den RAS-Server auf **Präfixkonfiguration**.
3. Fügen Sie auf der Seite **Präfixkonfiguration** unter **IPv6-Präfixe des internen Netzwerks** alle zusätzlichen IPv6-Präfixe durch Semikolons getrennt hinzu (z. B. 2001:db8:1::/64;2001:db8:2::/64). Klicken Sie dann auf **Weiter**.
4. Klicken Sie auf der Seite **Authentifizierung** auf **Fertig stellen**.
5. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole auf **Fertig stellen**.
6. Klicken Sie im Dialogfeld **Überprüfung des Remotezugriffs** auf **Anwenden**.
7. Klicken Sie im Dialogfeld **Anwenden der Einstellungen zum Einrichten des Remotezugriffs** auf **Schließen**.

## Hinzufügen von Client Sicherheitsgruppen

Damit Windows 8-Client Computer von Forest2 über DirectAccess auf Ressourcen zugreifen können, müssen Sie die Sicherheitsgruppe von Forest2 der Remote Zugriffs Bereitstellung hinzufügen.

### So fügen Sie Windows 8-Clientsicherheitsgruppen hinzu

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 1 Remoteclients** auf **Bearbeiten**.
2. Klicken Sie im Assistenten zum Einrichten des DirectAccess-Clients auf **Gruppen auswählen**, und klicken

Sie dann auf der Seite **Gruppen auswählen auf Hinzufügen**.

3. Wählen Sie im Dialogfeld **Gruppen auswählen** die Sicherheitsgruppen aus, die DirectAccess-Clientcomputer enthalten. Klicken Sie dann auf **Weiter**.
4. Klicken Sie auf der Seite **Netzwerkkonnektivitäts-Assistent** auf **Fertig stellen**.
5. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole auf **Fertig stellen**.
6. Klicken Sie im Dialogfeld **Überprüfung des Remotezugriffs** auf **Anwenden**.
7. Klicken Sie im Dialogfeld **Anwenden der Einstellungen zum Einrichten des Remotezugriffs** auf **Schließen**.

Damit Windows 7-Client Computer von Forest2 über DirectAccess auf Ressourcen zugreifen können, wenn die Option für mehrere Standorte aktiviert ist, müssen Sie die Sicherheitsgruppe von Forest2 der RAS-Bereitstellung für jeden Einstiegspunkt hinzufügen. Weitere Informationen zum Hinzufügen von Windows 7-Sicherheitsgruppen finden Sie in der Beschreibung der Seite **Client Unterstützung** in 3.6. Aktivieren Sie die Bereitstellung für mehrere Standorte.

#### **Aktualisieren der Liste der Verwaltungs Server**

Der Remotezugriff erkennt automatisch die Infrastrukturserver in allen Gesamtstrukturen, die GPOs für die DirectAccess-Konfiguration enthalten. Wenn DirectAccess auf einem Server in %&quot;Forest1%&quot; bereitgestellt wurde, wird das Server-GPO in seine Domäne in %&quot;Forest1%&quot; geschrieben. Nachdem Sie den Zugriff auf DirectAccess für Clients in %&quot;Forest2%&quot; aktiviert haben, wird das Client-GPO in eine Domäne in %&quot;Forest2%&quot; geschrieben.

Der automatische Ermittlungsprozess von Infrastruktur Servern ist erforderlich, um den Zugriff über DirectAccess auf die Domänen Controller und den Microsoft-Endpunkt Configuration Manager zuzulassen. Sie müssen den Erkennungsprozess manuell starten.

**So aktualisieren Sie die Liste der Verwaltungsserver**

1. Klicken Sie in der Remotezugriffs-Verwaltungskonsole auf **Konfiguration** und dann im Bereich **Aufgaben** auf **Verwaltungsserver aktualisieren**.
2. Klicken Sie im Dialogfeld **Aktualisieren von Verwaltungsservern** auf **Schließen**.

# Verwalten des Remotezugriffs

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Im Bereitstellungsszenario "DirectAccess-Clientremoteverwaltung" wird DirectAccess verwendet, um Clients über das Internet zu verwalten. In diesem Abschnitt wird das Szenario samt Phasen, Rollen, Features und Links zu weiteren Ressourcen beschrieben.

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess-und RRAS-VPN (Routing and Remote Access Service, Routing-und RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle.

## NOTE

Über dieses Thema hinaus sind die folgenden Themen zur Verwaltung des Remotezugriffs verfügbar.

- [Verwenden der Remotezugriffsüberwachung und Ressourcenerfassung](#)
- [Remoteverwaltung von DirectAccess-Clients](#)

## Szenariobeschreibung

DirectAccess-Clientcomputer sind unabhängig davon, ob der Benutzer sich am Computer angemeldet hat, mit dem Intranet verbunden. Sie können als Intranetressourcen verwaltet werden und mithilfe von Gruppenrichtlinienänderungen, Betriebssystemupdates, Updates von Antischadsoftware und anderen organisatorischen Änderungen aktualisiert werden.

In einigen Fällen müssen Intranetserver oder -computer Verbindungen mit DirectAccess-Clients initiieren. So können beispielsweise Mitarbeiter der Helpdeskabteilung über den Remotedesktop eine Verbindung mit DirectAccess-Remoteclients herstellen und Probleme beheben. Bei diesem Szenario wird die bestehende Remotezugriffslösung zwecks Benutzerkonnektivität beibehalten, während DirectAccess für die Remoteverwaltung verwendet wird.

DirectAccess bietet eine Konfiguration, die die Remote Verwaltung von DirectAccess-Clients unterstützt. Dies erfolgt mithilfe einer Option im Bereitstellungs-Assistenten, die die Erstellung von Richtlinien auf solche Richtlinien beschränkt, die für die Remoteverwaltung von Clientcomputern benötigt werden.

## NOTE

Bei dieser Bereitstellung sind Konfigurationsoptionen auf Benutzerebene, beispielsweise Tunnelerzwingung, Integration in den Netzwerkzugriffsschutz (Network Access Protection, NAP) und zweistufige Authentifizierung, nicht verfügbar.

## Inhalt dieses Szenarios

Das Szenario der DirectAccess-Bereitstellung für die Remoteverwaltung von Clients umfasst für die Planung und Konfiguration die folgenden Schritte:

### Planen der Bereitstellung

Für die Planung dieses Szenarios müssen nur wenige Computer- und Netzwerkanforderungen erfüllt werden. Dazu gehören:

- **Netzwerk- und Servertopologie:** Mit DirectAccess können Sie den Remotezugriffsserver am Rand des Intranets oder hinter einem NAT-Gerät (Network Address Translation, Netzwerkadressenübersetzung) oder einer Firewall platzieren.
- **DirectAccess-Netzwerkadressenserver:** Der Netzwerkadressenserver wird von DirectAccess-Clients verwendet, um festzustellen, ob sie sich im internen Netzwerk befinden. Der Netzwerkadressenserver kann auf dem DirectAccess-Server oder auf einem anderen Server installiert werden.
- **DirectAccess-Clients:** Legen Sie fest, welche verwalteten Computer als DirectAccess-Clients konfiguriert werden sollen.

## Konfigurieren des Bereitstellung

Das Konfigurieren der Bereitstellung besteht aus einer Reihe von Schritten. Dazu gehören:

- Konfigurieren der Infrastruktur:** Konfigurieren Sie DNS-Einstellungen, fügen Sie den Server und die Clientcomputer bei Bedarf einer Domäne hinzu, und konfigurieren Sie Active Directory-Sicherheitsgruppen.  
Bei diesem Bereitstellungsszenario werden Gruppenrichtlinienobjekte automatisch vom Remotezugriff erstellt. Erweiterte Optionen für das Gruppenrichtlinien Objekt finden Sie unter Bereitstellen des [erweiterten Remote Zugriffs](#).
- Konfigurieren der RAS-Server- und Netzwerkeinstellungen:** Konfigurieren Sie Netzwerkadapter, IP-Adressen und Routing.
- Konfigurieren von Zertifikat Einstellungen:** in diesem Bereitstellungs Szenario erstellt der Assistent für die ersten Schritte selbst signierte Zertifikate, sodass die erweiterte Zertifikat Infrastruktur nicht konfiguriert werden muss.
- Konfigurieren des Netzwerkadressenservers:** Bei diesem Szenario ist der Netzwerkadressenserver auf dem Remotezugriffsserver installiert.
- Planen der DirectAccess-Verwaltungsserver:** Administratoren können DirectAccess-Clientcomputer, die sich außerhalb des Unternehmensnetzwerks befinden, remote über das Internet verwalten.  
Verwaltungsserver sind Computer, die für die Verwaltung von Remoteclients verwendet werden (beispielsweise Updateserver).
- Konfigurieren des Remotezugriffsservers:** Installieren Sie die Rolle "Remotezugriff", und führen Sie den DirectAccess-Assistenten für erste Schritte aus, um DirectAccess zu konfigurieren.
- Überprüfen der Bereitstellung:** Testen Sie einen Client, um sicherzustellen, dass er mithilfe von DirectAccess eine Verbindung mit dem internen Netzwerk und dem Internet herstellen kann.

## Praktische Anwendungen

Die Bereitstellung eines einzelnen Remotezugriffsservers für die Verwaltung von DirectAccess-Clients bietet Folgendes:

- **Einfache ZugriffsMöglichkeiten:** verwaltete Client Computer, auf denen Windows 8 oder Windows 7 ausgeführt wird, können als DirectAccess-Client Computer konfiguriert werden. Diese Clients können bei aktiver Verbindung mit dem Internet über DirectAccess auf interne Netzwerkressourcen zugreifen, ohne sich über eine VPN-Verbindung anmelden zu müssen. Clientcomputer, die keines dieser Betriebssysteme verwenden, können per VPN eine Verbindung mit dem internen Netzwerk herstellen. Sowohl DirectAccess als auch VPN werden über dieselbe Konsole und mit denselben Assistanten verwaltet.
- **Erleichterte Verwaltung:** Die Remoteverwaltung von DirectAccess-Clientcomputern im Internet ist mithilfe von Remotezugriffsadministratoren über DirectAccess möglich, selbst wenn sich die Clientcomputer nicht im internen Unternehmensnetzwerk befinden. Clientcomputer, die nicht den Unternehmensanforderungen entsprechen, können automatisch über Verwaltungsserver gewartet werden. Einer oder mehrere RAS-Server

können über eine einzelne Remotezugriff-Verwaltungskonsole verwaltet werden.

## In diesem Szenario enthaltene Rollen und Features

Die folgende Tabelle enthält die für dieses Szenario erforderlichen Rollen und Features:

ROLLE ODER FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
<i>Remote Zugriffs Rolle</i>	<p>Die Rolle wird über die Server-Manager-Konsole oder Windows PowerShell installiert bzw. deinstalliert. Diese Rolle umfasst DirectAccess (zuvor ein Feature unter Windows Server 2008 R2) sowie die Routing- und RAS-Dienste (zuvor ein Rollendienst unter der Serverrolle für Netzwerkrichtlinien- und Zugriffsdiensste). Die Remotezugriffs-Rolle besteht aus zwei Komponenten:</p> <ol style="list-style-type: none"><li>1. DirectAccess-und RRAS-VPN (Routing and Remote Access Services): DirectAccess und VPN werden in der Remote Zugriffs-Verwaltungskonsole verwaltet.</li><li>2. RRAS: Features werden in der Routing-und RAS-Konsole verwaltet.</li></ol> <p>Die Serverrolle "Remotezugriff" ist von den folgenden Features abhängig:</p> <ul style="list-style-type: none"><li>-Webserver (IIS): ist erforderlich, um den Netzwerkadressen Server und den Standardweb Test zu konfigurieren.</li><li>-Interne Windows-Datenbank: wird für die lokale Kontoführung auf dem Remote Zugriffs Server verwendet.</li></ul>
Feature %quot;Tools für die Remotezugriffsverwaltung%quot;	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"><li>-Standardmäßig auf einem RAS-Server, wenn die Remote Zugriffs Rolle installiert ist und die Benutzeroberfläche der Remote Verwaltungskonsole unterstützt.</li><li>-Als Option auf einem Server, auf dem die Remote Zugriffs-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Servers verwendet.</li></ul> <p>Dieses Feature umfasst Folgendes:</p> <ul style="list-style-type: none"><li>-Remote Zugriffs-GUI und Befehlszeilen Tools</li><li>-Remote Zugriffs Modul für Windows PowerShell</li></ul> <p>Abhängigkeiten umfassen:</p> <ul style="list-style-type: none"><li>-Gruppenrichtlinien-Verwaltungskonsole</li><li>-RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li><li>-Windows PowerShell 3,0</li><li>-Tools und Infrastruktur für die grafische Verwaltung</li></ul>

## Hardwareanforderungen

Für dieses Szenario müssen die folgenden Hardwareanforderungen erfüllt werden:

### Serveranforderungen

- Ein Computer, der die Hardwareanforderungen für Windows Server 2016 erfüllt. Weitere Informationen finden Sie unter [System Anforderungen](#) für Windows Server 2016.
- Auf dem Server muss mindestens ein Netzwerkadapter installiert und aktiviert sein. Es darf nur ein Adapter an das interne Unternehmensnetzwerk und einer an das externe Netzwerk (Internet) angeschlossen sein.

- Falls Teredo als IPv6- bis IPv4-Übergangsprotokoll benötigt wird, benötigt der externe Adapter des Servers zwei aufeinanderfolgenden öffentlichen IPv4-Adressen. Wenn nur eine Netzwerkkarte verfügbar ist, kann nur IP-HTTPS als Übergangsprotokoll verwendet werden.
- Mindestens ein Domänencontroller. Der RAS-Server und die DirectAccess-Clients müssen Domänenmitglieder sein.
- Eine Zertifizierungsstelle ist auf dem Server erforderlich, wenn Sie keine selbstsignierten Zertifikate für IP-HTTPS oder den Netzwerkadressenserver verwenden möchten, oder wenn Sie Clientzertifikate zur IPsec-Clientauthentifizierung verwenden möchten.

## **Clientanforderungen**

- Auf einem Client Computer muss Windows 10, Windows 8 oder Windows 7 ausgeführt werden.

## **Anforderungen an Infrastruktur und Verwaltungsserver**

- Während der Remoteverwaltung von DirectAccess-Clientcomputern initiieren die Clients die Kommunikation mit Verwaltungsservern, z. B. Domänencontrollern, System Center-Konfigurationsservern und Servern für Inhaltsregistrierungsstellen (Health Registration Authority, HRA). Diese Server bieten Dienste für Windows- und Antivirenupdates und NAP-Clientkompatibilität (Network Access Protection, Netzwerkzugriffsschutz). Die erforderlichen Server müssen bereitgestellt sein, bevor mit der Bereitstellung des Remotezugriffs begonnen wird.
- Es ist ein DNS-Server erforderlich, auf dem Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008 mit SP2 ausgeführt wird.

# **Software Anforderungen**

Für dieses Szenario müssen die folgenden Softwareanforderungen erfüllt werden:

## **Serveranforderungen**

- Der Remotezugriffsserver muss Domänenmitglied sein. Der Server kann an der Schwelle zum internen Netzwerks oder geschützt durch eine Edgefirewall oder ein anderes Gerät bereitgestellt werden.
- Wird der RAS-Server durch eine Edgefirewall oder ein NAT-Gerät geschützt, muss das Gerät so konfiguriert sein, dass ein- und ausgehender Datenverkehr für den RAS-Server zugelassen wird.
- Administratoren, die einen Remotezugriffsserver bereitstellen, müssen lokale Administratorberechtigungen für den Server und Domänenbenutzerberechtigungen für die Domäne haben. Zusätzlich benötigt der Administrator Berechtigungen für die Gruppenrichtlinien, die bei der DirectAccess-Bereitstellung verwendet werden. Um die Features nutzen zu können, die die DirectAccess-Bereitstellung auf mobile Computer beschränken, ist die Berechtigung, WMI-Filter zu erstellen (Domänenadministratoren) für den Domänencontroller erforderlich.
- Befindet sich der Netzwerkadressenserver nicht auf dem RAS-Server, ist ein separater Server für die Ausführung erforderlich.

## **Remotezugriffs-Client-Anforderungen**

- DirectAccess-Clients müssen Domänenmitglieder sein. Domänen, die Clients beinhalten, können zur selben Gesamtstruktur gehören wie der RAS-Server, oder sie können eine bidirektionale Vertrauensstellung mit dem RAS-Server und der Domäne innehaben.
- Eine Active Directory-Sicherheitsgruppe wird benötigt, um die Computer aufzunehmen, die als DirectAccess-Clients konfiguriert werden. Computer dürfen immer nur einer Sicherheitsgruppe zugeordnet werden, die DirectAccess-Clients enthält. Wenn Clients in mehreren Gruppen enthalten sind, funktioniert die Namensauflösung für Clientanforderungen nicht wie erwartet.

# Verwenden der Remotezugriffsüberwachung und Ressourcenerfassung

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die Überwachung des Remotezugriffs meldet Remotebenutzeraktivitäten und den Status der DirectAccess- und VPN-Verbindungen. Sie zeichnet die Anzahl und die Dauer der Clientverbindungen (und weitere Statistiken) auf und überwacht den Betriebsstatus des Servers. Eine benutzerfreundliche Überwachungskonsole stellt Ihnen eine Ansicht der gesamten Remotezugriffinfrastruktur bereit. Die Überwachungsansichten sind für einzelne Server-, Cluster- und Konfigurationen für mehrere Standorte.

**Hinweis:** Durch Windows Server 2012 werden DirectAccess und RRAS (Routing and Remote Access Service, Routing- und RAS-Dienst) zu einer einzigen Remotezugriffsrolle zusammengefasst.

## NOTE

Über dieses Thema hinaus sind die folgenden Themen zur Überwachung des Remotezugriffs verfügbar.

- [Überwachen der vorhandenen Last auf dem Remotezugriffsserver](#)
- [Überwachen des Konfigurationsverteilungsstatus des Remotezugriffsservers](#)
- [Überwachen des Betriebs Status des Remote Zugriffs Servers und seiner Komponenten](#)
- [Identifizieren und Beheben von Betriebsproblemen auf dem Remotezugriffsserver](#)
- [Überwachen der Aktivitäten und des Status von verbundenen Remoteclients](#)
- [Erstellen eines Nutzungsberichts für Remoteclients mithilfe von Verlaufsdaten](#)

## In diesem Handbuch

Dieses Dokument enthält Anweisungen zur Nutzung der Überwachungsfunktionen des Remotezugriffs mit der DirectAccess-Verwaltungskonsole und den entsprechenden Windows PowerShell-Cmdlets, die als Teil der Remotezugriffs-Serverrolle bereitgestellt werden.

Es werden folgende Überwachungs- und Ressourcenerfassungsszenarios erläutert:

1. Überwachen der vorhandenen Last auf dem Remotezugriffsserver
2. Überwachen des Konfigurationsverteilungsstatus des Remotezugriffsservers
3. Überwachen des Betriebsstatus des Remotezugriffsservers und dessen Komponenten
4. Identifizieren und Beheben von Betriebsproblemen auf dem Remotezugriffsserver
5. Überwachen der Aktivitäten und des Status von verbundenen Remoteclients
6. Erstellen eines Nutzungsberichts für die Remoteclients mithilfe von Verlaufsdaten

## Grundlagen von Überwachung und Ressourcenerfassung

Bevor Sie mit den Überwachungs- und Ressourcenüberwachungsaufgaben für Remoteclients beginnen, müssen Sie den Unterschied zwischen den beiden Komponenten verstehen.

- Die **Überwachung** zeigt die aktiv zu einem bestimmten Zeitpunkt verbundenen Benutzer an.

- Die **Ressourcenerfassung** erfasst einen Verlauf der Benutzer, die eine Verbindung zum Unternehmensnetzwerk hergestellt haben und ihre Nutzungsdetails (zu Kompatibilitäts- und Prüfzwecken).

Die Remoteclientüberwachung basiert auf Verbindungen. Es gibt zwei Arten von Tunnelverbindungen, die von DirectAccess-Clients aufgebaut werden können:

- **Computer-Tunneldatenverkehrverbindungen:** Dieser Tunnel wird vom Computer im Systemkontext aufgebaut, um auf Server zuzugreifen, die für die Namenauflösung, Authentifizierung, Aktualisierung der Wartung usw. erforderlich sind.
- **Benutzer-Tunneldatenverkehrverbindungen:** Dieser Tunnel wird auf dem Computer vom Benutzerkonto in einem Benutzerkontext aufgebaut, wenn der Benutzer versucht, auf eine Ressource im Unternehmensnetzwerk zuzugreifen. Je nach Bereitstellungsanforderungen muss ein Benutzer möglicherweise sichere Anmeldungsinformationen angeben (z. B. mit einer Smartcard oder einem Einmalkennwort), um auf Ressourcen im Unternehmensnetzwerk zuzugreifen.

Für DirectAccess wird eine Verbindung durch die IP-Adresse des Remoteclients eindeutig identifiziert. Wenn ein Computertunnel beispielsweise für einen Clientcomputer geöffnet wurde und ein Benutzer über diesen Computer verbunden ist, verwenden sie die gleiche Verbindung. Wenn der Benutzer die Verbindung trennt und erneut herstellt, während der Computertunnel noch aktiv ist, handelt es sich um eine einzelne Verbindung.

# Überwachen der vorhandenen Last auf dem Remotezugriffsserver

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Durch Windows Server 2012 werden DirectAccess und RRAS (Routing and Remote Access Service, Routing- und RAS-Dienst) zu einer einzigen Remotezugriffsrolle zusammengefasst.

Der Begriff "Laden" bezieht sich auf die Statistiken, die sich auf die Anzahl der Verbindungen auf dem RAS-Server beziehen. Es folgen die Schritte, die zum Nachverfolgen der Last auf dem RAS-Server erforderlich sind.

Mithilfe des Überwachungs Dashboards, das in der Verwaltungskonsole auf dem RAS-Server zur Verfügung steht, können Sie die Auslastungs Statistiken für den Server anzeigen, oder Sie können Leistungsindikatoren verwenden, um die Statistiken zu überwachen.

## NOTE

Sie müssen auf jedem Computer als Mitglied der Gruppe "Domänen-Admins" oder "Administratoren" angemeldet sein, um die in diesem Thema beschriebenen Aufgaben ausführen zu können. Wenn Sie eine Aufgabe nicht ausführen können, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Administratoren" ist, versuchen Sie, die Aufgabe auszuführen, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Domänen-Admins" ist.

## So verwenden Sie das Überwachungs Dashboard zum Überwachen der Remote Zugriffs Serverauslastung

1. Klicken Sie im Server Manager auf Tools und dann auf Remotezugriffsverwaltung.
2. Klicken Sie auf DASHBOARD, um in der Remotezugriffs-Verwaltungskonsole zum Remotezugriffdashboard zu navigieren.
3. Beachten Sie auf dem Dashboard Überwachung die Kachel Remote Client Status innerhalb der Kachel Server Status . Auf dieser Kachel werden Statistiken wie die Gesamtzahl der verbundenen Remote Clients, die Gesamtzahl der verbundenen DirectAccess-Clients sowie die maximale Anzahl von Benutzern aufgelistet, die in den letzten 24 Stunden eine Verbindung hergestellt haben.
4. Sie können im rechten Bereich unter Aufgaben auf Aktualisieren klicken, um den Integritäts Status erneut zu laden. Um das Standard Aktualisierungs Intervall zu ändern, klicken Sie unter Aufgaben auf Aktualisierungs Intervall konfigurieren .

## So verwenden Sie das System Monitor Tool zum Überwachen von Leistungsindikatoren auf dem Remote Zugriffs Server

1. Klicken Sie auf Start, klicken Sie auf Verwaltung, und doppelklicken Sie dann auf System Monitor.
2. Klicken Sie unter Leistung auf System Monitor.
3. Klicken Sie in der Symbolleiste des System Monitors auf die Schaltfläche Hinzufügen (durch ein grünes Kreuz Symbol gekennzeichnet).
4. Wählen Sie in der Liste der verfügbaren Leistungsindikatoren alle Indikatoren in den Kategorien RAS und ramgmzvc aus, und klicken Sie dann auf > > hinzufügen.
5. Wählen Sie erneut in der Liste der verfügbaren Leistungsindikatoren alle Indikatoren in der Kategorie IPSec-Verbindungen aus, und klicken Sie dann auf > > hinzufügen.

6. Klicken Sie auf **OK**, um die ausgewählten **Leistungsindikatoren** in der System Monitor Konsole für die Überwachung hinzuzufügen.

Der System **Monitor** zeigt nun die ausgewählten Server Lade Statistiken grafisch an.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
PS> Get-RemoteAccessConnectionStatisticsSummary
```

# Überwachen des Konfigurationsverteilungsstatus des Remotezugriffsservers

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Windows Server 2012 kombiniert DirectAccess und RAS-Dienst (RAS) zu einer einzigen Remote Zugriffs Rolle.

Die Remotezugriffs-Verwaltungskonsole vergleicht die Konfigurationsversionen aller überwachten Server, um zu überprüfen, dass sie übereinstimmen und die aktuellste Konfigurationsversion verwenden. Sie zeigt an, ob die aktuellste Konfigurationsversion (die in den Gruppenrichtlinienobjekten angegeben sind) an alle Server verteilt wurde und ob sie erfolgreich sie erfolgreich auf den Servern angewendet wurde.

## So verwenden Sie das Überwachungsdashboard zum Überwachen der Konfigurationsverteilung

1. Klicken Sie im **Server Manager** auf Tools und dann auf **Remotezugriffsverwaltung**.
2. Klicken Sie auf **DASHBOARD**, um in der **Remotezugriffs-Verwaltungskonsole** zum **Remotezugriffdashboard** zu navigieren.
3. Beachten Sie im Überwachungsdashboard die Kachel **Konfigurationsstatus** oben in der Mitte. Die Kachel zeigt den aktuellen Status der Konfigurationsverteilung an.

In der folgenden Tabelle sind die Meldungen, die von der Kachel **Konfigurationsstatus** generiert werden, ihre Bedeutungen und die erforderliche administrative Aktion (falls vorhanden) aufgeführt.

Schweregrad	Meldung	Bedeutung	Maßnahme
Erfolgreich	Die Konfiguration wurde erfolgreich verteilt.	Die Konfiguration in dem Gruppenrichtlinienobjekt wurde erfolgreich auf dem Server angewendet.	Keine Aktion erforderlich.

Warnung	<p>Die Konfiguration für den Server [Servername] wurde nicht vom Domänencontroller abgerufen. Das GPO ist nicht verknüpft.</p>	<p>Die Konfiguration in dem Gruppenrichtlinienobjekt konnte den Server noch nicht erreichen. Die Ursache für dieses Problem könnte sein, dass das GPO nicht mit dem Server verknüpft ist.</p>	<p>Verknüpfen Sie das GPO mit einem Verwaltungsbereich, der auf den Server angewendet wird, oder exportieren Sie die Einstellungen in einem GPO-Bereitstellungsszenario aus der GPO-Bereitstellung und importieren Sie sie in die Produktions-GPO. Weitere Informationen zu staginggruppen Richtlinien Objekten finden Sie unter Verwalten von Remote Zugriffs-Gruppenrichtlinien Objekten <b>mit eingeschränkten Berechtigungen</b> in <a href="#">Schritt-1-Plan-The-DirectAccess-Infrastructure</a>. Informationen zu GPO-stagingschritten finden Sie unter Konfigurieren von Remote Zugriffs-Gruppenrichtlinien Objekten <b>mit eingeschränkten Berechtigungen</b> in <a href="#">Schritt-1: Konfigurieren der DirectAccess-Infrastruktur</a>.</p>
Warnung	<p>Die Konfiguration für den Server [Servername] wurde nicht vom Domänencontroller abgerufen.</p>	<p>Die Konfiguration in dem Gruppenrichtlinienobjekt konnte den Server noch nicht erreichen. Es kann bis zu 10 Minuten dauern, bis eine neue Konfiguration verteilt wird.</p>	<p>Räumen Sie einen weiteren Zeitraum ein, damit die Richtlinien auf dem Server aktualisiert werden können.</p>

Error	Die Konfiguration für den Server [Servername] wurde nicht vom Domänencontroller abgerufen.	Die Konfiguration in dem GPO konnte den Server nicht erreichen. Und seit der Konfigurationsänderung sind mehr als 10 Minuten vergangen.	Diese Problem kann in einem der folgenden Szenarios auftreten: <ul style="list-style-type: none"> <li>-Der Server hat keine Verbindung mit der Domäne, um die Richtlinien zu aktualisieren. Sie können "gpupdate/force" auf dem Server ausführen, um eine Richtlinien Aktualisierung zu erzwingen.</li> <li>-GPO-Replikation ist möglicherweise erforderlich, um die aktualisierte Konfiguration abzurufen.</li> <li>-Der Active Directory Standort des RAS-Servers enthält keinen beschreibbaren Domänen Controller.</li> </ul> <p>Warten Sie, bis die GPOs mit allen Domänencontrollern repliziert wurden, und verwenden Sie dann das Windows PowerShell-Cmdlet <b>Set-DADelegatePoint</b>, um den Einstiegspunkt dem beschreibbaren Domänencontroller auf dem Remotezugriffsserver zuzuordnen.</p>
Warnung	Die Konfiguration für den Server [Servername] wurde vom Domänencontroller abgerufen, jedoch noch nicht angewendet.	Die Konfiguration in dem GPO hat den Server erreicht, sie wurde jedoch noch nicht angewendet.  Es kann bis zu 15 Minuten dauern, bevor die Konfiguration angewendet wird.	Räumen Sie einen weiteren Zeitraum ein, damit die Konfiguration vollständig auf dem Server angewendet werden kann.

Error	<p>Die Konfiguration für den Server [Servername] wurde vom Domänencontroller abgerufen, kann jedoch nicht angewendet werden.</p>	<p>Die Konfiguration in dem GPO konnte den Server erreichen, sie wurde jedoch nicht erfolgreich angewendet. Außerdem sind seit der Konfigurationsänderungen mehr als 15 Minuten vergangen.</p>	<p>Diese Problem kann in einem der folgenden Szenarios auftreten:</p> <ol style="list-style-type: none"> <li>1. die Konfiguration wird zurzeit angewendet. Diese Meldung wird als Fehler angezeigt, da zum Abrufen der Konfiguration aus dem GPO möglicherweise ein längerer Zeitraum erforderlich war. Um diese mögliche Ursache zu bestätigen, verwenden Sie die <b>Aufgabenplanung</b> und navigieren Sie zu Microsoft\Windows\RemoteAccess, um zu prüfen, ob <b>RAConfigTask</b> aktuell ausgeführt wird.</li> <li>2. Wenn <b>raconfigtask</b> zurzeit nicht ausgeführt wird, konnte die Konfiguration möglicherweise nicht auf den Server angewendet werden. Überprüfen Sie die <b>Ereignisanzeige</b> unter dem Remotezugriffsserver-Vorgangskanal, der sich unter \Anwendungs- und Dienstprotokolle\Microsoft\Windows\RemoteAccess-RemoteAccessServer befindet. Überprüfen Sie den <b>VORGANGSSTATUS</b> in der Remotezugriffs-Verwaltungskonsole auf Fehler. Weitere Informationen finden Sie unter <a href="#">Überwachen des Betriebsstatus des Remotezugriffsservers und dessen Komponenten</a>.</li> </ol>
-------	--	--	--

Error	<p>Die Konfiguration für Mehrfachstandortserver wurde vom Domänencontroller abgerufen. Einige Server besitzen abweichende Konfigurationen.</p>	<p>Zwischen den Konfigurationsversionen der Server-GPOs in der Bereitstellung mit mehreren Standorten besteht eine Inkonsistenz.</p> <p>Idealerweise weisen alle Server-GPOs für alle Einstiegpunkte die gleiche globale Konfiguration auf, aus etwaigen Gründen sind sie jedoch nicht synchron.</p>	<p>Das kann vorkommen, wenn durch eine Konfigurationsänderung ein Fehler auftritt und die Änderung nicht erfolgreich zurückgesetzt wird.</p> <p>Sie sollten die GPOs aus einem Sicherungsstatus wiederherstellen, in dem alle Server-GPOs synchronisiert wurden. Informationen zu einem Skript, das Sie verwenden können, finden Sie unter <a href="#">Sichern und Wiederherstellen der Remote Zugriffs Konfiguration</a>.</p>
-------	--	--	--

# Überwachen des Betriebsstatus des Remotezugriffsservers und dessen Komponenten

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Durch Windows Server 2012 werden DirectAccess und RRAS (Routing and Remote Access Service, Routing- und RAS-Dienst) zu einer einzigen Remotezugriffsrolle zusammengefasst.

Die Verwaltungskonsole auf dem RAS-Server kann zum Überwachen des Vorgangs Status verwendet werden.

## NOTE

Sie müssen auf jedem Computer als Mitglied der Gruppe "Domänen-Admins" oder "Administratoren" angemeldet sein, um die in diesem Thema beschriebene Aufgabe abzuschließen. Wenn Sie eine Aufgabe nicht ausführen können, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Administratoren" ist, versuchen Sie, die Aufgabe auszuführen, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Domänen-Admins" ist.

## So überwachen Sie den Betriebsstatus des RAS-Servers

1. Klicken Sie im **Server Manager** auf Tools und dann auf **Remotezugriffsverwaltung**.
2. Klicken Sie auf **Dashboard**, um in der **Remote Zugriffs-Verwaltungskonsole** zur **Remote Zugriffs Berichterstattung** zu navigieren.
3. Beachten Sie auf dem Dashboard Überwachung die Kachel **Betriebsstatus** innerhalb der Kachel **Server Status**. Diese Kachel listet den Serverbetriebs Status und den Status aller Serverkomponenten auf.
4. Klicken Sie im rechten Bereich unter **Tasks** auf **Aktualisieren**, um den Vorgangs Status neu zu laden. Der Vorgangs Status wird automatisch alle fünf Minuten aktualisiert. Dies ist das Standard Aktualisierungs Intervall. Um das Standard Aktualisierungs Intervall zu ändern, klicken Sie auf **Aktualisierungs Intervall konfigurieren**.

## Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

## NOTE

Der Befehl für den Vorgangs Status eines Clusters ist als Verweis enthalten.

```
PS> Get-RemoteAccessHealth  
PS> Get-RemoteAccessHealth -Cluster
```

# Identifizieren und Beheben von Betriebsproblemen auf dem Remotezugriffsserver

09.04.2020 • 6 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Durch Windows Server 2012 werden DirectAccess und RRAS (Routing and Remote Access Service, Routing- und RAS-Dienst) zu einer einzigen Remotezugriffsrolle zusammengefasst.

Mithilfe der folgenden Verfahren können Sie Probleme bei RAS-Server Vorgängen, ihre Hauptursachen und die Lösung ermitteln, die zum Beheben der Probleme erforderlich ist.

## NOTE

Sie müssen auf jedem Computer als Mitglied der Gruppe "Domänen-Admins" oder "Administratoren" angemeldet sein, um die in diesem Thema beschriebenen Aufgaben ausführen zu können. Wenn Sie eine Aufgabe nicht ausführen können, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Administratoren" ist, versuchen Sie, die Aufgabe auszuführen, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Domänen-Admins" ist.

Dieses Thema enthält Informationen zum Ausführen der folgenden Aufgaben:

- Simulieren eines Vorgangs Problems
- Identifizieren des Vorgangs Problems und ergreifen von Korrekturmaßnahmen
- Wiederherstellen des IP Helper-Dienstes

## Simulieren eines Vorgangs Problems

### Caution

Da der RAS-Server wahrscheinlich ordnungsgemäß konfiguriert ist und keine Probleme aufgetreten sind, können Sie das folgende Verfahren verwenden, um ein Vorgangs Problem zu simulieren. Wenn Ihr Server momentan Clients in einer Produktionsumgebung verarbeitet, möchten Sie diese Aktionen möglicherweise zu diesem Zeitpunkt nicht durchführen. Stattdessen können Sie die Schritte lesen, um zu verstehen, wie Sie Probleme beheben können, die in Zukunft auf dem RAS-Server auftreten können.

Der IP-Hilfsdienst (iphlpvc) hostet IPv6-Übergangs Technologien (z. b. IP-HTTPS, IPv6-zu-IPv4 oder Teredo) und ist erforderlich, damit der DirectAccess-Server ordnungsgemäß funktioniert. Zum veranschaulichen eines simulierten Vorgangs Problems auf dem RAS-Server müssen Sie den Netzwerkdienst (iphlpvc) unterbinden.

### So verhindern Sie den IP-Hilfsdienst

1. Klicken Sie auf dem Start Bildschirm des Remote Zugriffs Servers auf **Verwaltung**, und doppelklicken Sie dann auf **Dienste**.
2. Scrollen Sie in der Liste der Diensten nach unten, **und klicken Sie** mit der rechten Maustaste auf **IP-Hilfsobjekt**.

## Identifizieren des Vorgangs Problems und ergreifen von Korrekturmaßnahmen

Das Ausschalten des IP-Hilfsobjekts führt zu einem schwerwiegenden Fehler auf dem RAS-Server. Das Dashboard für die Überwachung zeigt den Betriebsstatus des Servers und die Details des Problems an.

### So identifizieren Sie die Details und ergreifen Korrekturmaßnahmen

1. Klicken Sie im **Server Manager** auf **Tools** und dann auf **Remotezugriffsverwaltung**.

2. Klicken Sie auf **DASHBOARD**, um in der **Remotezugriffs-Verwaltungskonsole** zum **Remotezugriffdashboard** zu navigieren.
3. Stellen Sie sicher, dass der Remote Zugriffs Server im linken Bereich ausgewählt ist, und klicken Sie dann im mittleren Bereich auf **Vorgangs Status**.
4. Die Liste der Komponenten mit grünen oder roten Symbolen wird angezeigt, die den Betriebsstatus angeben. Klicken Sie in der Liste auf die Zeile **IP-HTTPS**. Wenn Sie eine Zeile ausgewählt haben, werden die Details für den Vorgang wie folgt im **Detail** Bereich angezeigt:

### Fehler

Der IP-Hilfsdienst (iphlpsvc) wurde beendet. DirectAccess funktioniert möglicherweise nicht wie erwartet. Der IP-Hilfsdienst bietet Tunnel Konnektivität mithilfe der Konnektivitätsplattform, IPv6-Übergangs Technologien und IP-HTTPS.

### Gründe

- a. Der IP-Hilfsdienst wurde beendet.
- b. Der IP-Hilfsdienst antwortet nicht.

### Lösung

- a. Um sicherzustellen, dass der Dienst ausgeführt wird, geben Sie an einer Windows PowerShell-Eingabeaufforderung **Get-Service iphlpsvc** ein.
- b. Um den Dienst zu aktivieren, geben Sie an einer Windows PowerShell-Eingabeaufforderung mit erhöhten rechten **Start-Service iphlpsvc** ein.
- c. Um den Dienst neu zu starten, geben Sie an einer Windows PowerShell-Eingabeaufforderung mit erhöhten rechten **Restart-Service iphlpsvc** ein.

### Wiederherstellen des IP Helper-Dienstes

Um den IP-Hilfsdienst auf Ihrem RAS-Server wiederherzustellen, können Sie die oben beschriebenen Lösungsschritte ausführen, um den Dienst zu starten oder neu zu starten, oder Sie können das folgende Verfahren verwenden, um das Verfahren umzukehren, das Sie zum Simulieren des Fehlers bei IP-Hilfsobjekten verwendet haben.

**So starten Sie den IP Helper-Dienst auf dem Remote Zugriffs Server neu**

1. Klicken Sie auf dem Bildschirm **Start** auf **Verwaltung**, und doppelklicken Sie dann auf **Dienste**.
2. Scrollen Sie in der Liste der **Diensten** nach unten, **und klicken Sie** mit der rechten Maustaste auf **IP-Hilfsobjekt**.

### Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
PS> Get-RemoteAccessHealth | Where-Object {$_.Component -eq "IP-HTTPS"} | Format-List -Property *
```

# Überwachen der Aktivitäten und des Status von verbundenen Remoteclients

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Windows Server 2012 kombiniert DirectAccess und RAS-Dienst (RAS) zu einer einzigen Remote Zugriffs Rolle.

Sie können die-Verwaltungskonsole auf dem Remote Zugriffs Server verwenden, um die Remote Client Aktivität und den Status zu überwachen.

## NOTE

Sie müssen auf jedem Computer als Mitglied der Gruppe "Domänen-Admins" oder "Administratoren" angemeldet sein, um die in diesem Thema beschriebenen Aufgaben ausführen zu können. Wenn Sie eine Aufgabe nicht ausführen können, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Administratoren" ist, versuchen Sie, die Aufgabe auszuführen, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Domänen-Admins" ist.

## So überwachen Sie die Remote Client Aktivität und den Status

1. Klicken Sie im **Server Manager** auf **Tools** und dann auf **Remotezugriffsverwaltung**.
2. Klicken Sie auf **Berichterstattung**, um in der **Remote Zugriffs-Verwaltungskonsole** zur **Remote Zugriffs Berichterstattung** zu navigieren.
3. Klicken Sie auf **Remote Client Status**, um in der **Remote Zugriffs-Verwaltungskonsole** in der **Remote Zugriffs-Verwaltungskonsole** zur Remote Client Aktivität und zur Benutzeroberfläche
4. Es wird eine Liste der Benutzer angezeigt, die mit dem RAS-Server verbunden sind, sowie ausführliche Statistiken zu diesen. Klicken Sie auf die erste Zeile in der Liste, die einem Client entspricht. Wenn Sie eine Zeile auswählen, wird die Remote Benutzeraktivität im Vorschaubereich angezeigt.

## Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
PS> Get-RemoteAccessConnectionStatistics
```

Die Benutzerstatistiken können mithilfe der Felder in der folgenden Tabelle gefiltert werden, basierend auf der Kriterienauswahl.

FELDNAME	WERT
Benutzername	Der Benutzername oder das Alias des Remotebenutzers. Platzhalter Zeichen können verwendet werden, um eine Gruppe von Benutzern auszuwählen, wie z. B. "*" von "\administrator".

FELDNAME	WERT
Hostname	Der Name des Computerkontos des Remotebenutzers. Außerdem kann eine IPv4- oder IPv6-Adresse angegeben werden.
Typ	DirectAccess oder VPN. Wenn DirectAccess ausgewählt ist, werden alle Remote Benutzer, die über DirectAccess verbunden sind, aufgeführt. Wenn VPN ausgewählt wird, werden alle Remote Benutzer aufgelistet, die über VPN verbunden sind.
ISP-Adresse	Die IPv4- oder IPv6-Adresse des Remotebenutzers.
IPv4-Adresse	Die innere IPv4-Adresse des Tunnels, der den Remote Benutzer mit dem Unternehmensnetzwerk verbindet.
IPv6-Adresse	Die interne IPv6-Adresse des Tunnels, über den der Remotebenutzer mit dem Unternehmensnetzwerk verbunden ist.
Protokoll//Tunnel	Die Übergangstechnologie, die vom Remote Client verwendet wird. Dies ist Teredo, 6de4 oder IP-HTTPS für DirectAccess-Benutzer, und es ist PPTP, L2TP, SSTP oder IKEv2 für VPN-Benutzer.
Aufgerufene Ressource	Alle Benutzer, die auf eine bestimmte Unternehmensressource oder einen bestimmten Unternehmensexpunkt zugreifen. Der Wert, der diesem Feld entspricht, ist der Hostname/die IP-Adresse des Servers.
Server	Der RAS-Server, mit dem Clients verbunden sind. Dies ist nur für Clusterbereitstellungen und Bereitstellungen für mehrere Standorte relevant.

# Erstellen eines Nutzungsberichts für Remoteclients mithilfe von Verlaufsdaten

09.04.2020 • 5 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Durch Windows Server 2012 werden DirectAccess und RRAS (Routing and Remote Access Service, Routing- und RAS-Dienst) zu einer einzigen Remotezugriffsrolle zusammengefasst.

Mithilfe der-Verwaltungskonsole auf dem Remote Zugriffs Server kann ein Verwendungs Bericht für die Remote Clients generiert werden, die auf den Server zugreifen. Um einen Verwendungs Bericht für Remote Clients zu generieren, aktivieren Sie zunächst die Kontoführung auf dem RAS-Server. Nachdem Sie den Bericht generiert haben, können Sie das Überwachungs Dashboard verwenden, das in der-Verwaltungskonsole auf dem RAS-Server verfügbar ist, um die Auslastungs Statistiken auf dem Server anzuzeigen.

## NOTE

Sie müssen auf jedem Computer als Mitglied der Gruppe "Domänen-Admins" oder "Administratoren" angemeldet sein, um die in diesem Thema beschriebenen Aufgaben ausführen zu können. Wenn Sie eine Aufgabe nicht ausführen können, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Administratoren" ist, versuchen Sie, die Aufgabe auszuführen, während Sie mit einem Konto angemeldet sind, das Mitglied der Gruppe "Domänen-Admins" ist.

## So aktivieren Sie die Kontoführung auf dem Remote Zugriffs Server

1. Klicken Sie im Server Manager auf Tools und dann auf Remotezugriffsverwaltung.
2. Klicken Sie auf Berichterstattung , um in der Remote Zugriffs-Verwaltungskonsole zur Remote Zugriffs Berichterstattung zu navigieren.
3. Klicken Sie im Aufgabenbereich Remote Zugriffs Berichterstattung auf Konto Führung konfigurieren .
4. Aktivieren Sie das Kontrollkästchen Posteingangs Erfassung verwenden , um die Kontoführung auf dem Remote Zugriffs Server zu aktivieren.
5. Klicken Sie auf übernehmen, um die Buchhaltungs Konfiguration auf dem Server zu aktivieren, und klicken Sie dann auf Schließen , nachdem der Server die Konfiguration erfolgreich angewendet hat.

## So generieren Sie den Verwendungs Bericht

1. Klicken Sie im Server Manager auf Tools und dann auf Remotezugriffsverwaltung.
2. Klicken Sie auf Berichterstattung , um in der Remote Zugriffs-Verwaltungskonsole zur Remote Zugriffs Berichterstattung zu navigieren.
3. Klicken Sie im mittleren Bereich auf Datumsangaben im Kalender, um das Start Datum für die Berichts Dauer (und das Enddatum: ) auszuwählen, und klicken Sie dann auf Bericht generieren.
4. Es wird eine Liste der Benutzer angezeigt, die innerhalb des ausgewählten Zeitraums eine Verbindung mit dem RAS-Server hergestellt haben, und detaillierte Statistiken dazu. Klicken Sie auf die erste Zeile in der Liste. Wenn Sie eine Zeile auswählen, wird die Remote Benutzeraktivität im Vorschaubereich angezeigt. Wählen Sie nun im Vorschaubereich die Registerkarte Server Lade Statistik aus, um die Verlaufs Auslastung auf dem Server anzuzeigen.

Klicken Sie im Vorschaufenster auf die Registerkarte Statistiken für den Server Lade Vorgang, um die

Verlaufs Auslastung auf dem Server anzuzeigen.

#### NOTE

##### Grundlegendes zu Sitzungen

Die Kontoführung für den Remote Zugriff basiert auf dem Konzept der **Sitzungen**. Im Gegensatz zu einer **Verbindung** wird eine **Sitzung** durch eine Kombination aus Remote Client-IP-Adresse und Benutzername eindeutig identifiziert. Wenn z. b. ein Computer Tunnel vom Remote Client mit dem Namen CLIENT1 gebildet wird, wird eine Sitzung erstellt und in der Buchhaltungs Datenbank gespeichert. Wenn ein Benutzer mit dem Namen user1 nach einiger Zeit eine Verbindung mit diesem Client herstellt (der Computer Tunnel ist jedoch noch aktiv), wird die Sitzung als separate Sitzung aufgezeichnet. Der Unterschied zwischen den verschiedenen Sitzungen besteht darin, den Unterschied zwischen Computer Tunnel und Benutzer Tunnel beizubehalten.

#### Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

Ändern Sie im folgenden Skript den Datumsbereich, für den Sie einen Bericht erstellen möchten, in den Parametern **-StartTime** und **-EndTime**.

```
PS> Get-RemoteAccessConnectionStatisticsSummary -StartTime "1 October 2010 00:00:00" -EndTime "14
October 2010 00:00:00"
Shows server load statistics.
PS> Get-RemoteAccessUserActivity -HostIPAddress 10.0.0.1 -StartTime "1 October 2010 00:00:00" -EndTime
"14 October 2010 00:00:00"
```

# Remote-Verwaltung von DirectAccess-Clients

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die Überwachung des Remotezugriffs meldet Remotebenutzeraktivitäten und den Status der DirectAccess- und VPN-Verbindungen. Sie zeichnet die Anzahl und die Dauer der Clientverbindungen (und weitere Statistiken) auf und überwacht den Betriebsstatus des Servers. Eine benutzerfreundliche Überwachungskonsole stellt Ihnen eine Ansicht der gesamten Remotezugriffinfrastruktur bereit. Die Überwachungsansichten sind für einzelne Server-, Cluster- und Konfigurationen für mehrere Standorte.

**Hinweis:** Windows Server 2016 kombiniert DirectAccess und RAS-Dienst (RAS) zu einer einzigen Remote Zugriffs Rolle.

## In diesem Handbuch

Dieses Dokument enthält Anweisungen zur Nutzung der Überwachungsfunktionen des Remotezugriffs mit der DirectAccess-Verwaltungskonsole und den entsprechenden Windows PowerShell-Cmdlets, die als Teil der Remotezugriffs-Serverrolle bereitgestellt werden.

Es werden folgende Überwachungs- und Ressourcenerfassungsszenarios erläutert:

1. Überwachen der vorhandenen Last auf dem Remotezugriffsserver
2. Überwachen des Konfigurationsverteilungsstatus des Remotezugriffsservers
3. Überwachen des Betriebsstatus des Remotezugriffsservers und dessen Komponenten
4. Identifizieren und Beheben von Betriebsproblemen auf dem Remotezugriffsserver
5. Überwachen der Aktivitäten und des Status von verbundenen Remoteclients
6. Erstellen eines Nutzungsberichts für die Remoteclients mithilfe von Verlaufsdaten

## Grundlagen von Überwachung und Ressourcenerfassung

Bevor Sie mit den Überwachungs- und Ressourcenüberwachungsaufgaben für Remoteclients beginnen, müssen Sie den Unterschied zwischen den beiden Komponenten verstehen.

- Die **Überwachung** zeigt die aktiv zu einem bestimmten Zeitpunkt verbundenen Benutzer an.
- Die **Ressourcenerfassung** erfasst einen Verlauf der Benutzer, die eine Verbindung zum Unternehmensnetzwerk hergestellt haben und ihre Nutzungsdetails (zu Kompatibilitäts- und Prüfzwecken).

Die Remoteclientüberwachung basiert auf Verbindungen. Es gibt zwei Arten von Tunnelverbindungen, die von DirectAccess-Clients aufgebaut werden können:

- **Computer-Tunneldatenverkehrverbindungen:** Dieser Tunnel wird vom Computer im Systemkontext aufgebaut, um auf Server zuzugreifen, die für die Namenauflösung, Authentifizierung, Aktualisierung der Wartung usw. erforderlich sind.
- **Benutzer-Tunneldatenverkehrverbindungen:** Dieser Tunnel wird auf dem Computer vom Benutzerkonto in einem Benutzerkontext aufgebaut, wenn der Benutzer versucht, auf eine Ressource im Unternehmensnetzwerk zuzugreifen. Je nach Bereitstellungsanforderungen muss ein Benutzer möglicherweise sichere Anmeldungsinformationen angeben (z. B. mit einer Smartcard oder einem

Einmalkennwort), um auf Ressourcen im Unternehmensnetzwerk zuzugreifen.

Für DirectAccess wird eine Verbindung durch die IP-Adresse des Remoteclients eindeutig identifiziert. Wenn ein Computertunnel beispielsweise für einen Clientcomputer geöffnet wurde und ein Benutzer über diesen Computer verbunden ist, verwenden sie die gleiche Verbindung. Wenn der Benutzer die Verbindung trennt und erneut herstellt, während der Computertunnel noch aktiv ist, handelt es sich um eine einzelne Verbindung.

# Planen der Bereitstellung für die Remoteverwaltung von DirectAccess-Clients

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die folgenden Themen enthalten Planungsschritte für die Bereitstellung eines einzelnen RAS-Servers, auf dem ausgeführt wird und der für die Remote Verwaltung von DirectAccess-Clients verwendet werden kann.

**Schritt 1: Planen der Infrastruktur für den Remote Zugriff:** in diesem Thema finden Sie Informationen zum Planen der Netzwerktopologie und Servereinstellungen, der Firewallanforderungen, der Zertifikat Anforderungen, der Domain Name System Anforderungen, der DirectAccess-Netzwerkadressen Server-und Verwaltungs Serverkonfiguration, der Active Directory Anforderungen und der Gruppenrichtlinie Objekt Erstellung.

**Schritt 2: Planen der Bereitstellung des Remote Zugriffs:** Planen von Client-und Server Bereitstellungs Strategien und Infrastruktur Serverkonfigurationen.

# Schritt 1 Planen der Infrastruktur für den Remote Zugriff

09.04.2020 • 70 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

## NOTE

Windows Server 2016 kombiniert DirectAccess und den Routing-und RAS-Dienst (RRAS) zu einer einzigen Remote Zugriffs Rolle.

In diesem Thema werden die Schritte zum Planen einer-Infrastruktur beschrieben, die Sie zum Einrichten eines einzelnen Remote Zugriffs Servers für die Remote Verwaltung von DirectAccess-Clients verwenden können. In der folgenden Tabelle sind die Schritte aufgeführt. diese Planungsaufgaben müssen jedoch nicht in einer bestimmten Reihenfolge ausgeführt werden.

AUFGABE	BESCHREIBUNG
<a href="#">Planen der Netzwerktopologie und der Servereinstellungen</a>	Entscheiden Sie, wo der RAS-Server (Edge oder hinter einem NAT-Gerät oder einer Firewall) platziert werden soll, und planen Sie IP-Adressierung und Routing.
<a href="#">Planen der Firewallanforderungen</a>	Planen Sie, den Remotezugriff über Edge-Firewalls zuzulassen.
<a href="#">Planen der Zertifikat Anforderungen</a>	Entscheiden Sie, ob Sie das Kerberos-Protokoll oder Zertifikate für die Client Authentifizierung verwenden möchten, und planen Sie Ihre Website Zertifikate.  IP-HTTPS ist ein Übergangsprotokoll, das von DirectAccess-Clients zum Tunneln von IPv6-Datenverkehr über IPv4-Netzwerke verwendet wird. Entscheiden Sie sich für die Authentifizierung von IP-HTTPS für den Server, indem Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle (Certification Authority, ca) ausgestellt wurde, oder ein selbst signiertes Zertifikat, das automatisch vom Remote Zugriffs Server ausgestellt wird.
<a href="#">Planen der DNS-Anforderungen</a>	Planen Sie die Domain Name System (DNS)-Einstellungen für den Remote Zugriffs Server, die Infrastruktur Server, die Optionen für die lokale Namensauflösung und die Client Konnektivität.
<a href="#">Planen der Netzwerkadressen Server-Konfiguration</a>	Entscheiden Sie, wo die Netzwerkadressen Server-Website in Ihrer Organisation platziert werden soll (auf dem Remote Zugriffs Server oder einem alternativen Server), und planen Sie die Zertifikat Anforderungen, wenn sich der Netzwerkadressen Server auf dem RAS-Server befindet. <b>Hinweis:</b> Der Netzwerkadressen Server wird von DirectAccess-Clients verwendet, um zu bestimmen, ob Sie sich im internen Netzwerk befinden.

AUFGABE	BESCHREIBUNG
Planen der Konfigurationen von Verwaltungs Servern	Berücksichtigen Sie bei der Planung Verwaltungsserver (beispielsweise Updateserver), die für die Verwaltung von Remotedclients verwendet werden. <b>Hinweis:</b> Administratoren können DirectAccess-Client Computer, die sich außerhalb des Unternehmensnetzwerks befinden, Remote über das Internet verwalten.
Planen von Active Directory Anforderungen	Planen Sie Ihre Domänen Controller, Ihre Active Directory Anforderungen, Client Authentifizierung und mehrere Domänen Strukturen.
Planen Gruppenrichtlinie Objekt Erstellung	Entscheiden Sie, welche Gruppenrichtlinien Objekte in Ihrer Organisation erforderlich sind und wie die GPOs erstellt und bearbeitet werden.

## Planen der Netzwerktopologie und -einstellungen

Wenn Sie Ihr Netzwerk planen, müssen Sie die Netzwerkadapter Topologie, die Einstellungen für die IP-Adressierung und die Anforderungen für ISATAP berücksichtigen.

### Planen von Netzwerkadapters und IP-Adressierung

1. Identifizieren Sie die Netzwerkadapter Topologie, die Sie verwenden möchten. Der Remote Zugriff kann mit einer der folgenden Topologien eingerichtet werden:

- Mit zwei Netzwerkadapters: der Remote Zugriffs Server wird am Rand installiert, wobei ein Netzwerkadapter mit dem Internet und der andere mit dem internen Netzwerk verbunden ist.
- Mit zwei Netzwerkadapters: der Remote Zugriffs Server wird hinter einem NAT-Gerät, einer Firewall oder einem Router installiert, wobei ein Netzwerkadapter mit einem Umkreis Netzwerk und der andere mit dem internen Netzwerk verbunden ist.
- Mit einem Netzwerkadapter: der RAS-Server wird hinter einem NAT-Gerät installiert, und der einzige Netzwerkadapter wird mit dem internen Netzwerk verbunden.

2. Identifizieren Sie Ihre IP-Adressierungsanforderungen:

DirectAccess verwendet IPv6 mit IPsec, um eine sichere Verbindung zwischen DirectAccess-Clientcomputern und dem internen Unternehmensnetzwerk herzustellen. Jedoch erfordert DirectAccess nicht unbedingt Konnektivität mit dem IPv6-Internet oder nativen IPv6-Support auf internen Netzwerken. Stattdessen konfiguriert und verwendet es automatisch IPv6-Übergangs Technologien, um IPv6-Datenverkehr über das IPv4-Internet (IPv6-zu-IPv4, Teredo oder IP-HTTPS) und über Ihr ausschließlich-IPv4-Intranet (NAT64 oder ISATAP) zu Tunneln. Eine Übersicht über diese Übergangstechnologien finden Sie in folgenden Ressourcen:

- [IPv6-Übergangs Technologien](#)
- [IP-HTTPS-tunnelingprotokollspezifikation](#)

3. Konfigurieren Sie erforderliche Adapter und Adressen entsprechend folgender Tabelle. Konfigurieren Sie bei bereit Stellungen, die sich hinter einem NAT-Gerät mit einem einzelnen Netzwerkadapter befinden, Ihre IP-Adressen, indem Sie nur die Spalte **interner Netzwerkadapter** verwenden.

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER <sup>1</sup> , OBERHALB	ROUTINGANFORDERUNGE N
IPv4-Internet und IPv4-Intranet	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>: Zwei statische aufeinander folgende öffentliche IPv4-Adressen mit den entsprechenden Subnetzmasken (nur für Teredo erforderlich).</li> <li>-Eine Standard Gateway-IPv4-Adresse für Ihre Internet Firewall oder den ISP-Router (lokaler Internetdienstanbieter).</li> </ul> <p><b>Hinweis:</b> Der RAS-Server benötigt zwei aufeinander folgende öffentliche IPv4-Adressen, damit er als Teredo-Server fungieren kann und Windows-basierte Teredo-Clients den Remote Zugriffs Server verwenden können, um den Typ des NAT-Geräts zu erkennen.</p>	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>: Eine IPv4-Intranetadresse mit der entsprechenden Subnetzmaske.</li> <li>: Ein Verbindungs spezifisches DNS-Suffix für den Intranetnamespace. Zudem sollte ein DNS-Server auf der internen Schnittstelle konfiguriert werden. <b>Vorsicht:</b> Konfigurieren Sie kein Standard Gateway auf Intranetschnittstellen.</li> </ul>	<p>Gehen Sie folgendermaßen vor, um den Remote Zugriffs Server so zu konfigurieren, dass er alle Subnetze im internen IPv4-Netzwerk erreicht:</p> <ul style="list-style-type: none"> <li>-Listen Sie die IPv4-Adressräume für alle Speicherorte im Intranet auf.</li> <li>-Verwenden Sie die Befehle <code>route add -p</code> oder <code>netsh interface ipv4 add route</code>, um die IPv4-Addressbereiche als statische Routen in der IPv4-Routing Tabelle des Remote Zugriffs Servers hinzuzufügen.</li> </ul>

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv6-Internet und IPv6-Intranet	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>-Verwenden Sie die automatisch konfigurierte Adress Konfiguration, die von Ihrem ISP bereitgestellt wird.</li> <li>-Verwenden Sie den <code>route print</code> Befehl, um sicherzustellen, dass eine IPv6-Standardroute, die auf den ISP-Router zeigt, in der IPv6-Routing Tabelle vorhanden ist</li> <li>: Ermitteln Sie, ob der ISP- und der Intranetrouter standardmäßige Routereinstellungen verwenden, wie in RFC 4191 beschrieben, und wenn Sie eine höhere Standardeinstellung als ihre lokalen Intranetrouter verwenden. Wenn beide Fälle zutreffen, ist keine weitere Konfiguration für die Standardroute erforderlich. Die höhere Präferenz für den ISP-Router stellt sicher, dass die aktive IPv6-Standardroute des Remotezugriffsservers auf das IPv6-Internet zeigt.</li> </ul> <p>Wenn Sie über eine systemeigene IPv6-Infrastruktur verfügen, kann die Internetschnittstelle außerdem auch die Domänencontroller im Intranet erreichen, da der DirectAccess-Server ein IPv6-Router ist. Fügen Sie in diesem Fall Paketfilter zum Domänen Controller im Umkreis Netzwerk hinzu, die Verbindungen mit der IPv6-Adresse der Internet Schnittstelle des Remote Zugriffs Servers verhindern.</p>	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>Wenn Sie keine Standard Einstellungsebenen verwenden, konfigurieren Sie die Intranetschnittstellen mit dem</li> </ul> <pre>netsh interface ipv6 set InterfaceIndex ignoredefaultroutes=enabled</pre> <p>Befehl. Dieser Befehl stellt sicher, dass der IPv6-Routingtabelle keine weiteren Standardrouten hinzugefügt werden, die auf Intranetrouter zeigen. Sie können den interfacetten Index ihrer Intranetschnittstellen von der Anzeige des Befehls</p> <pre>netsh interface show interface</pre> <p>abrufen.</p>	<p>Wenn Sie ein IPv6-Intranet haben, führen Sie folgende Schritte aus, um den Remotezugriffsserver so zu konfigurieren, dass er alle IPv6-Speicherorte erreicht:</p> <ul style="list-style-type: none"> <li>-Auflisten der IPv6-Adressräume für alle Speicherorte im Intranet.</li> <li>-Verwenden Sie den</li> </ul> <pre>netsh interface ipv6 add route</pre> <p>-Befehl, um die IPv6-Adressbereiche als statische Routen in der IPv6-Routing Tabelle des Remote Zugriffs Servers hinzuzufügen.</p>

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv4-Internet und IPv6-Intranet	<p>Der RAS-Server leitet den IPv6-Standardrouten Datenverkehr mithilfe der Microsoft IPv6-zu-IPv4-Adapter Schnittstelle an ein IPv6-zu-IPv4-Relay im IPv4-Internet weiter. Wenn System eigenes IPv6 nicht im Unternehmensnetzwerk bereitgestellt wird, können Sie den folgenden Befehl verwenden, um einen RAS-Server für die IPv4-Adresse des Microsoft IPv6-zu-IPv4-Relay im IPv4-Internet zu konfigurieren:</p> <pre>netsh interface ipv6  6to4 set relay name=  &lt;ipaddress&gt;  state=enabled</pre> <p>.</p>		

#### NOTE

- Wenn dem DirectAccess-Client eine öffentliche IPv4-Adresse zugewiesen wurde, wird die IPv6-zu-IPv4-relaytechnologie verwendet, um eine Verbindung mit dem Intranet herzustellen. Wenn dem Client eine private IPv4-Adresse zugewiesen ist, wird Teredo verwendet. Wenn der DirectAccess-Client weder mit IP6-zu-IP4 noch mit Teredo eine Verbindung mit dem DirectAccess-Server herstellen kann, wird IP-HTTPS verwendet.
- Um Teredo zu verwenden, müssen Sie zwei aufeinander folgende IP-Adressen auf dem nach außen verfügbaren Netzwerkadapter konfigurieren.
- Sie können Teredo nicht verwenden, wenn der Remote Zugriffs Server nur über einen Netzwerkadapter verfügt.
- Systemeigene IPv6-Clientcomputer können über eine systemeigene IPv6 eine Verbindung zum Remotezugriffsserver herstellen, und es ist keine Übergangstechnologie erforderlich.

#### Planen von ISATAP-Anforderungen

ISATAP ist für die Remote Verwaltung von directaccessclients erforderlich, damit DirectAccess-Verwaltungs Server eine Verbindung mit DirectAccess-Clients im Internet herstellen können. ISATAP ist nicht erforderlich, um Verbindungen zu unterstützen, die von DirectAccess-Client Computern zu IPv4-Ressourcen im Unternehmensnetzwerk initiiert werden. Für diese Zwecke wird NAT64/DNS64 verwendet. Wenn Ihre Bereitstellung ISATAP erfordert, verwenden Sie die folgende Tabelle, um Ihre Anforderungen zu ermitteln.

ISATAP-BEREITSTELLUNGS Szenario	VORAUSSETZUNGEN
---------------------------------	-----------------

ISATAP-BEREITSTELLUNGS SZENARIO	VORAUSSETZUNGEN
Vorhandenes natives IPv6-Intranet (keine ISATAP erforderlich)	<p>Bei einer vorhandenen nativen IPv6-Infrastruktur geben Sie das Präfix der Organisation während der Remote Zugriffs Bereitstellung an, und der RAS-Server konfiguriert sich nicht selbst als ISATAP-Router. Gehen Sie wie folgt vor:</p> <ol style="list-style-type: none"> <li>um sicherzustellen, dass DirectAccess-Clients über das Intranet erreichbar sind, müssen Sie das IPv6-Routing so ändern, dass der Standardrouten Datenverkehr an den Remote Zugriffs Server weitergeleitet wird. Wenn Ihr Intranet-IPv6-Addressraum eine andere Adresse als ein einzelnes IPv6-Adress Präfix mit 48 Bit verwendet, müssen Sie während der Bereitstellung das relevante IPv6-Präfix für die Organisation angeben.</li> <li>Wenn Sie zurzeit mit dem IPv6-Internet verbunden sind, müssen Sie den Standardrouten Datenverkehr so konfigurieren, dass er an den RAS-Server weitergeleitet wird, und dann die entsprechenden Verbindungen und Routen auf dem RAS-Server konfigurieren, sodass die Standardroute der Datenverkehr wird an das Gerät weitergeleitet, das mit dem IPv6-Internet verbunden ist.</li> </ol>
Vorhandene ISATAP-Bereitstellung	<p>Wenn Sie über eine vorhandene ISATAP-Infrastruktur verfügen, werden Sie während der Bereitstellung aufgefordert, das 48-Bit-Präfix der Organisation zu erhalten, und der RAS-Server konfiguriert sich nicht selbst als ISATAP-Router. Um sicherzustellen, dass DirectAccess-Clients über das Intranet erreichbar sind, müssen Sie die IPv6-Routing Infrastruktur so ändern, dass der Standardrouten Datenverkehr an den Remote Zugriffs Server weitergeleitet wird. Diese Änderung muss auf dem vorhandenen ISATAP-Router erfolgen, auf dem die Intranetclients bereits den Standard Datenverkehr weiterleiten müssen.</p>
Keine vorhandene IPv6-Konnektivität	<p>Wenn der Remote Zugriffs-Setup-Assistent erkennt, dass der Server über keine native oder ISATAP-basierte IPv6-Konnektivität verfügt, wird automatisch ein IPv6-zu-IPv4-basiertes 48-Bit-Präfix für das Intranet abgeleitet und der RAS-Server als ISATAP-Router für IPv6 bereitgestellt. Konnektivität mit ISATAP-Hosts in Ihrem Intranet. (Ein IPv6-zu-IPv4-basiertes Präfix wird nur verwendet, wenn der Server öffentliche Adressen hat; andernfalls wird das Präfix automatisch aus einem eindeutigen lokalen Adressbereich generiert.)</p> <p>Gehen Sie folgendermaßen vor, um ISATAP zu verwenden:</p> <ol style="list-style-type: none"> <li>registrieren Sie den ISATAP-Namen auf einem DNS-Server für jede Domäne, auf der Sie ISATAP-basierte Konnektivität aktivieren möchten, damit der ISATAP-Name vom internen DNS-Server zur internen IPv4-Adresse des Remote Zugriffs Servers aufgelöst werden kann.</li> <li>standardmäßig blockieren DNS-Server unter Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003 die Auflösung des ISATAP-Namens mithilfe der globalen Abfrage Sperr Liste. Um ISATAP zu aktivieren, müssen Sie den ISATAP-Namen aus der Sperr Liste entfernen. Weitere Informationen finden Sie unter <a href="#">Entfernen von ISATAP aus der globalen DNS-Abfragesperrliste</a>.</li> </ol> <p>Windows-basierte ISATAP-Hosts, die den ISATAP-Namen auflösen können, konfigurieren automatisch eine Adresse mit</p>

## ISATAP-BEREITSTELLUNGS SZENARIO

dem Remote Zugriffs Server wie folgt:  
**VORAUSSETZUNGEN**

1. eine ISATAP-basierte IPv6-Adresse auf einer ISATAP-Tunnelingschnittstelle
2. eine 64-Bit-Route, die Konnektivität mit den anderen ISATAP-Hosts im Intranet bereitstellt.
3. eine IPv6-Standardroute, die auf den Remote Zugriffs Server zeigt. Die Standardroute stellt sicher, dass Intranet-ISATAP-Hosts DirectAccess-Clients erreichen können.

Wenn Ihre Windows-basierten ISATAP-Hosts eine ISATAP-basierte IPv6-Adresse erhalten, beginnen Sie mit der Verwendung von ISATAP-gekapselten Datenverkehr, um zu kommunizieren, ob das Ziel auch ein ISATAP-Host ist. Da ISATAP für das gesamte Intranet ein einzelnes 64-Bit-Subnetz verwendet, erfolgt die Kommunikation von einem segmentierten IPv4-Kommunikationsmodell mit einem einzigen subnetzkommunikationsmodell mit IPv6. Dies kann sich auf das Verhalten einiger Active Directory Domain Services (AD DS) und der Anwendungen auswirken, die auf die Konfiguration der Active Directory Sites und Dienste zurückgreifen. Wenn Sie z. b. das Snap-in "Active Directory Sites und Dienste" verwendet haben, um Standorte, IPv4-basierte Subnetze und standortübergreifende Transporte zum Weiterleiten von Anforderungen an Server innerhalb von Standorten zu konfigurieren, wird diese Konfiguration von ISATAP-Hosts nicht verwendet.

1. Wenn Sie Active Directory Standorte und Dienste für die Weiterleitung an Standorten für ISATAP-Hosts konfigurieren möchten, müssen Sie für jedes IPv4-Subnetzobjekt ein entsprechendes IPv6-Subnetzobjekt konfigurieren, in dem das IPv6-Adress Präfix für das Subnetz denselben Bereich von ISATAP-Host ausdrückt. Adressen als IPv4-Subnetz. Beispiel: für das IPv4-Subnetz 192.168.99.0/24 und das 64-Bit-ISATAP-Adress Präfix 2002:836b: 1:8000::/64 ist das entsprechende IPv6-Adress Präfix für das IPv6-Subnetzobjekt 2002:836b: 1:8000:0: 5EFE: 192.168.99.0/120. Für eine beliebige IPv4-Präfix Länge (im Beispiel auf 24 festgelegt) können Sie die entsprechende IPv6-Präfix Länge aus der Formel 96 + IPv4PrefixLength bestimmen.
2. Fügen Sie für die IPv6-Adressen von DirectAccess-Clients Folgendes hinzu:
  - Bei Teredo-basierten DirectAccess-Clients: ein IPv6-Subnetz für den Bereich 2001:0: WWXX: YYZZ::/64, bei dem WWXX: YYZZ die Doppelpunkt-hexadezimale Version der ersten IPv4-Adresse des Remote Zugriffs Servers mit Internet Zugriff ist. .
  - Für IP-HTTPS-basierte DirectAccess-Clients: ein IPv6-Subnetz für den Bereich 2002: WWXX: YYZZ: 8100::/56, bei dem WWXX: YYZZ die Doppelpunkt-hexadezimal Version der ersten IPv4-Adresse (w. x. y. z) des Remote Zugriffs Servers ist. .
  - Für IPv6-zu-IPv4-basierte DirectAccess-Clients: eine Reihe von IPv6-zu-IPv4-basierten IPv6-Präfixen, die mit 2002 beginnen: und stellen die regionalen, öffentlichen IPv4-Adress Präfixe dar, die von Internet Assigned Numbers Authority (IANA) und regionalen Registrierungen

<b>ISATAP-BEREITSTELLUNGS SZENARIO</b>	<p>verwaltet werden. Das IP6-zu-IP4-basierte <b>VORAUSSETZUNGEN</b>, Präfix für das öffentliche IPv4-Adresspräfix w.x.y.z/n ist 2002:WWXX:YYZZ::/[16 +n], wobei WWXX:YYZZ die Hexadezimalnotation mit Doppelpunkt von w.x.y.z ist.</p> <p>Der Bereich 7.0.0.0/8 wird z. B. von der ARIN (American Registry for Internet Numbers) für Nordamerika verwaltet. Das entsprechende IPv6-zu-IPv4-basierte Präfix für diesen öffentlichen IPv6-Adressbereich ist 2002:700::/24. Weitere Informationen zum öffentlichen IPv4-Adressraum finden Sie unter <a href="#">IANA-IPv4-Adressraum Registrierung</a>.</p>
--	--

#### **IMPORTANT**

Stellen Sie sicher, dass Sie nicht über öffentliche IP-Adressen auf der internen Schnittstelle des DirectAccess-Servers verfügen. Wenn Sie über eine öffentliche IP-Adresse auf der internen Schnittstelle verfügen, kann die Konnektivität über ISATAP fehlschlagen.

#### **Planen der Firewallanforderungen**

Wenn sich der Remotezugriffsserver hinter einer Edge-Firewall befindet, sind folgende Ausnahmen für Remotezugriff-Datenverkehr erforderlich, wenn sich der Remotezugriffsserver auf dem IPv4-Internet befindet:

- Für IP-HTTPS: TCP (Transmission Control Protocol)-Zielport 443 und TCP-Quellport 443 ausgehend.
- Für Teredo-Datenverkehr: der UDP-Zielport 3544 (User Datagram Protocol), eingehend und UDP-Quellport 3544 ausgehend.
- Für IPv6-zu-IPv4-Datenverkehr: eingehende und ausgehende IP-Adresse 41.

#### **NOTE**

Bei Teredo- und IP6-zu-IP4-Datenverkehr sollten diese Ausnahmen für beide aufeinander folgenden öffentlichen IPv4-Adressen mit Internetzugriff auf dem RAS-Server angewendet werden.

Bei IP-HTTPS müssen die Ausnahmen auf die Adresse angewendet werden, die auf dem öffentlichen DNS-Server registriert ist.

- Wenn Sie den Remote Zugriff mit einem einzigen Netzwerkadapter bereitstellen und den Netzwerkadressen Server auf dem Remote Zugriffs Server installieren, TCP-Port 62000.

#### **NOTE**

Diese Ausnahme wird auf dem RAS-Server verwendet, und die vorherigen Ausnahmen befinden sich auf der Edge-Firewall.

Die folgenden Ausnahmen sind für RAS-Datenverkehr erforderlich, wenn sich der RAS-Server im IPv6-Internet befindet:

- IP-Protokoll 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend.
- ICMPv6 eingehender und ausgehender Datenverkehr (nur bei Verwendung von Teredo).

Wenn Sie zusätzliche Firewalls verwenden, wenden Sie die folgenden internen netzwerkfirewallausnahmen für RAS-Datenverkehr an:

- Für ISATAP: das eingehende und ausgehende Protokoll 41
- Für den gesamten IPv4/IPv6-Datenverkehr: TCP/UD
- Für Teredo: ICMP für den gesamten IPv4/IPv6-Datenverkehr

### Planen der Zertifikatanforderungen

Es gibt drei Szenarien, die Zertifikate erfordern, wenn Sie einen einzelnen Remote Zugriffs Server bereitstellen.

- **IPSec-Authentifizierung:** die Zertifikat Anforderungen für IPSec beinhalten ein Computer Zertifikat, das von DirectAccess-Client Computern verwendet wird, wenn Sie die IPSec-Verbindung mit dem RAS-Server herstellen, und ein Computer Zertifikat, das von RAS-Servern zum Einrichten von IPSec-Verbindungen mit DirectAccess-Clients verwendet wird.

Für DirectAccess in Windows Server 2012 ist die Verwendung dieser IPSec-Zertifikate nicht obligatorisch. Als Alternative kann der RAS-Server als Proxy für die Kerberos-Authentifizierung fungieren, ohne dass Zertifikate erforderlich sind. Wenn die Kerberos-Authentifizierung verwendet wird, funktioniert Sie über SSL, und das Kerberos-Protokoll verwendet das Zertifikat, das für IP-HTTPS konfiguriert wurde. Für einige Unternehmens Szenarien (einschließlich Bereitstellung für mehrere Standorte und einmalige Kenn Wort Authentifizierung) ist die Verwendung der Zertifikat Authentifizierung und nicht die Kerberos-Authentifizierung erforderlich.

- **IP-HTTPS-Server:** Wenn Sie den Remote Zugriff konfigurieren, wird der Remote Zugriffs Server automatisch als IP-HTTPS-Weblistener konfiguriert. Die IP-HTTPS-Website erfordert ein Websitezertifikat, und Clientcomputer müssen in der Lage sein, die CRL-Website (Certificate Revocation List, Zertifikatsperrlisten) für das Zertifikat zu kontaktieren.
- **Netzwerkadressen Server:** der Netzwerkadressen Server ist eine Website, mit der erkannt wird, ob sich Client Computer im Unternehmensnetzwerk befinden. Der Netzwerkadressenserver erfordert ein Websitezertifikat. DirectAccess-Clients müssen die CRL-Website für das Zertifikat kontaktieren können.

Die Zertifizierungsstellen Anforderungen für die einzelnen Szenarien sind in der folgenden Tabelle zusammengefasst.

IPSEC-AUTHENTIFIZIERUNG	IP-HTTPS-SERVER	NETZWERKADRESSEN SERVER
Eine interne Zertifizierungsstelle ist erforderlich, um Computer Zertifikate für den RAS-Server und Clients für die IPSec-Authentifizierung auszugeben, wenn Sie das Kerberos-Protokoll nicht für die Authentifizierung verwenden.	Interne Zertifizierungsstelle: Sie können eine interne Zertifizierungsstelle zum Ausstellen des IP-HTTPS-Zertifikats verwenden. Sie müssen jedoch sicherstellen, dass der CRL-Verteilungspunkt extern verfügbar ist.	Interne Zertifizierungsstelle: Sie können eine interne Zertifizierungsstelle verwenden, um das Netzwerkadressen Server-Website Zertifikat auszustellen. Stellen Sie sicher, dass der Sperrlisten-Verteilungspunkt eine hohe Verfügbarkeit vom internen Netzwerk aus hat.
	Selbst signiertes Zertifikat: Sie können ein selbst signiertes Zertifikat für den IP-HTTPS-Server verwenden. Ein selbstsigniertes Zertifikat kann nicht in Bereitstellungen für mehrere Standorte verwendet werden.	Selbst signiertes Zertifikat: Sie können ein selbst signiertes Zertifikat für die Netzwerkadressen Server-Website verwenden. In bereit Stellungen mit mehreren Standorten können Sie jedoch kein selbst signiertes Zertifikat verwenden.

IPSEC-AUTHENTIFIZIERUNG	IP-HTTPS-SERVER	NETZWERKADRESSEN SERVER
	Öffentliche Zertifizierungsstelle: Es wird empfohlen, eine öffentliche Zertifizierungsstelle zum Ausstellen des IP-HTTPS-Zertifikats zu verwenden. Dadurch wird sichergestellt, dass der CRL-Verteilungs Punkt extern verfügbar ist.	

#### Planen von Computerzertifikaten für IPsec-Authentifizierung

Wenn Sie die Zertifikat basierte IPSec-Authentifizierung verwenden, müssen der RAS-Server und die Clients ein Computer Zertifikat abrufen. Die einfachste Möglichkeit zum Installieren der Zertifikate ist die Verwendung Gruppenrichtlinie zum Konfigurieren der automatischen Registrierung von Computer Zertifikaten. Dadurch wird sichergestellt, dass alle Domänenmitglieder ein Zertifikat von einer Unternehmenszertifizierungsstelle erhalten. Wenn Sie keine Unternehmens Zertifizierungsstelle in Ihrer Organisation eingerichtet haben, finden Sie weitere Informationen unter [Active Directory Certificate Services](#).

Für dieses Zertifikat gelten die folgenden Anforderungen:

- Das Zertifikat muss über die Client Authentifizierung erweiterte Schlüssel Verwendung (Extended Key Usage, EKU) verfügen.
- Die Client-und Server Zertifikate müssen sich auf das gleiche Stamm Zertifikat beziehen. Das Stammzertifikat muss in den DirectAccess-Konfigurationseinstellungen ausgewählt sein.

#### Planen von Zertifikaten für IP-HTTPS

Der Remotezugriffsserver fungiert als IP-HTTPS-Listener, und Sie müssen manuell ein HTTPS-Websitezertifikat auf dem Server installieren. Beachten Sie Folgendes bei der Planung:

- Die Verwendung einer öffentlichen Zertifizierungsstelle wird empfohlen, damit Zertifikatsperrlisten schneller verfügbar sind.
- Geben Sie im Feld Betreff die IPv4-Adresse des Internet Adapters des Remote Zugriffs Servers oder den voll qualifizierten Namen der IP-HTTPS-URL an (die ConnectTo-Adresse). Falls sich der Remotezugriffsserver hinter einem NAT-Gerät befindet, sollte der öffentliche Name oder die Adresse des NAT-Geräts angegeben werden.
- Der allgemeine Name des Zertifikats sollte dem Namen der IP-HTTPS-Website entsprechen.
- Verwenden Sie für das Feld **Erweiterte Schlüssel Verwendung** die Serverauthentifizierungs-Objekt Kennung (OID).
- Geben Sie im Feld **Sperrlisten-Verteilungspunkte** einen Zertifikatsperrlisten-Verteilungspunkt an, auf den mit dem Internet verbundene DirectAccess-Clients zugreifen können.

#### NOTE

Dies ist nur für Clients erforderlich, auf denen Windows 7 ausgeführt wird.

- Das IP-HTTPS-Zertifikat muss einen privaten Schlüssel enthalten.
- Das IP-HTTPS-Zertifikat muss direkt in den persönlichen Speicher importiert werden.
- Die Namen von IP-HTTPS-Zertifikaten können Platzhalter enthalten.

#### Planen von Websitezertifikaten für den Netzwerkadressenserver

Beachten Sie bei der Planung der Netzwerkadressen Server-Website Folgendes:

- Im Feld **Antragsteller** muss eine IP-Adresse der Intranetschnittstelle des Netzwerkadressenservers oder der FQDN der Netzwerkadressen-URL angegeben sein.
- Verwenden Sie für das Feld **Erweiterte Schlüssel Verwendung** die Serverauthentifizierungs-OID.
- Verwenden Sie für das Feld **CRL-Verteilungs Punkte** einen Zertifikat Sperr Listen-Verteilungs Punkt, auf den DirectAccess-Clients, die mit dem Intranet verbunden sind, zugreifen können. Der Zertifikatsperllisten-Verteilungspunkt sollte nicht von außerhalb des internen Netzwerks zugänglich sein.

#### **NOTE**

Stellen Sie sicher, dass die Zertifikate für IP-HTTPS und den Netzwerkadressen Server einen Antragsteller Namen aufweisen. Wenn das Zertifikat einen alternativen Namen verwendet, wird es nicht vom RAS-Assistenten akzeptiert.

#### **Planen der DNS-Anforderungen**

In diesem Abschnitt werden die DNS-Anforderungen für Clients und Server in einer Remote Zugriffs Bereitstellung erläutert.

##### **DirectAccess-Clientanfragen**

DNS wird verwendet, um Anforderungen von DirectAccess-Clientcomputern aufzulösen, die sich nicht im internen Netzwerk befinden. DirectAccess-Clients versuchen, eine Verbindung mit dem DirectAccess-Netzwerkadressen Server herzustellen, um zu bestimmen, ob Sie sich im Internet oder im Unternehmensnetzwerk befinden.

- Wenn die Verbindung erfolgreich hergestellt wurde, werden die Clients im Intranet festgelegt, DirectAccess wird nicht verwendet, und Client Anforderungen werden mithilfe des DNS-Servers aufgelöst, der auf dem Netzwerkadapter des Client Computers konfiguriert ist.
- Wenn keine Verbindung hergestellt werden kann, wird davon ausgegangen, dass sich die Clients im Internet befinden. DirectAccess-Clients verwenden die Richtlinientabelle für die Namensauflösung, um zu ermitteln, welcher DNS-Server beim Auflösen von Namensanforderungen verwendet werden soll. Sie können angeben, dass Clients DirectAccess-DNS64 oder einen anderen internen DNS-Server für die Auflösung von Namen verwenden.

Wenn Sie eine Namensauflösung durchführen, wird die NRPT von DirectAccess-Clients verwendet, um festzulegen, wie eine Anfrage behandelt werden soll. Clients fordern einen voll qualifizierten Namen oder einen Namen mit einer einzelnen Bezeichnung an, z. b. <https://internal>. Wenn ein Name mit einer einzelnen Bezeichnung gefordert ist, wird ein DNS-Suffix angehängt, um einen FQDN zu bilden. Wenn die DNS-Abfrage mit einem Eintrag in der NRPT und DNS4 übereinstimmt oder ein Intranet-DNS-Server für den Eintrag angegeben wurde, wird die Abfrage für die Namensauflösung mithilfe des angegebenen Servers gesendet. Wenn eine Übereinstimmung vorhanden ist, aber kein DNS-Server angegeben ist, wird eine Ausnahme Regel und eine normale Namensauflösung angewendet.

Wenn ein neues Suffix zur NRPT in der Remote Zugriffs-Verwaltungskonsole hinzugefügt wird, können die Standard-DNS-Server für das Suffix automatisch erkannt werden, indem Sie auf die Schaltfläche " **erkennen** " klicken. Die automatische Erkennung funktioniert wie folgt:

- Wenn das Unternehmensnetzwerk IPv4-basiert ist oder IPv4 und IPv6 verwendet, ist die Standardadresse die DNS64-Adresse des internen Adapters auf dem Remote Zugriffs Server.
- Wenn das Unternehmensnetzwerk IPv6-basiert ist, ist die Standardadresse die IPv6-Adresse der DNS-Server auf dem Unternehmensnetzwerk.

##### **Infrastrukturserver**

- **Netzwerkadressen Server**

DirectAccess-Clients versuchen, den Netzwerkadressenserver zu erreichen, um zu bestimmen, ob sie sich auf dem internen Netzwerk befinden. Clients im internen Netzwerk müssen in der Lage sein, den Namen

des Netzwerkadressen Servers aufzulösen, und Sie müssen daran gehindert werden, den Namen zu beheben, wenn Sie sich im Internet befinden. Um dies zu gewährleisten, wird der FQDN des Netzwerkadressenservers standardmäßig als Ausnahmeregel zum NRPT hinzugefügt. Außerdem werden bei der Konfiguration von RAS folgende Regeln automatisch erstellt:

- Eine DNS-Suffixregel für die Stamm Domäne oder den Domänen Namen des Remote Zugriffs Servers und die IPv6-Adressen, die den Intranet-DNS-Servern entsprechen, die auf dem RAS-Server konfiguriert sind. Wenn der Remotezugriffsserver z. B. Mitglied der Domäne corp.contoso.com ist, wird für das DNS-Suffix .corp.contoso.com eine Regel erstellt.
- Eine Ausnahmeregel für den FQDN des Netzwerkadressenservers. Wenn die Netzwerkadressen Server-URL z. b. <https://nls.corp.contoso.com> ist, wird eine Ausnahme Regel für den voll qualifizierten Namen (NLS.Corp.contoso.com) erstellt.

- **IP-HTTPS-Server**

Der RAS-Server fungiert als IP-HTTPS-Listener und verwendet das Serverzertifikat zur Authentifizierung bei IP-HTTPS-Clients. Der IP-HTTPS-Name muss von DirectAccess-Clients aufgelöst werden können, die öffentliche DNS-Server verwenden.

#### Verbindungsprüfer

RAS erstellt einen Standard-Webtest, der von DirectAccess-Clientcomputern dazu verwendet wird, die Konnektivität zum internen Netzwerk zu prüfen. Damit der Test wie erwartet funktioniert, müssen folgende Namen manuell in dem DNS registriert werden:

- **DirectAccess-WebProbe Host** sollte in die interne IPv4-Adresse des RAS-Servers oder die IPv6-Adresse in einer reinen IPv6-Umgebung aufgelöst werden.
- **DirectAccess-corpconnectivityhost** sollte in die lokale Host Adresse (Loopback) aufgelöst werden. Sie sollten A- und AAAA-Einträge erstellen. Der Wert des A-Datensatzes ist 127.0.0.1, und der Wert des AAAA-Datensatzes wird aus dem NAT64-Präfix mit den letzten 32 Bits als 127.0.0.1 erstellt. Das NAT64-Präfix kann durch Ausführen des Windows PowerShell-Cmdlets **Get-netnattransitionconfiguration** abgerufen werden.

#### NOTE

Dies gilt nur in reinen IPv4-Umgebungen. Erstellen Sie in einer Umgebung mit IPv4 Plus IPv6 oder einer reinen IPv6-Umgebung nur einen AAAA-Datensatz mit der Loopback-IP-Adresse:: 1.

Mithilfe anderer Webadressen über HTTP oder Ping können Sie zusätzliche Verbindungs Prüfer erstellen. Für jeden Verbindungsprüfer muss ein DNS-Eintrag vorhanden sein.

#### DNS-Serveranforderungen

- Für DirectAccess-Clients müssen Sie einen DNS-Server verwenden, auf dem Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 oder ein beliebiger DNS-Server ausgeführt wird, der IPv6 unterstützt.
- Sie sollten einen DNS-Server verwenden, der dynamische Updates unterstützt. Sie können DNS-Server verwenden, die keine dynamischen Updates unterstützen, aber die Einträge müssen manuell aktualisiert werden.
- Der voll qualifizierte Verwaltungspunkt für die CRL-Verteilungs Punkte muss mithilfe von Internet-DNS-Servern aufgelöst werden können. Wenn sich beispielsweise der URL-<https://crl.contoso.com/crl/corp-DC1-CA.crl> im Feld **CRL-Verteilungs Punkte** des IP-HTTPS-Zertifikats des RAS-Servers befindet, müssen Sie sicherstellen, dass der voll qualifizierte Name crld.contoso.com mithilfe von Internet-DNS-Servern aufgelöst werden kann.

#### Planen der lokalen Namensauflösung

Beachten Sie Folgendes, wenn Sie eine lokale Namensauflösung planen:

#### NRPT

In den folgenden Situationen müssen Sie möglicherweise zusätzliche Regeln der Richtlinien Tabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) erstellen:

- Sie müssen weitere DNS-Suffixe für den Intranetnamespace hinzufügen.
- Wenn die voll qualifizierten Domänen Namen der CRL-Verteilungs Punkte auf dem Intranetnamespace basieren, müssen Sie Ausnahmeregeln für die voll qualifizierten Domänen Namen der CRL-Verteilungs Punkte hinzufügen.
- Wenn Sie über eine Split-Brain-DNS-Umgebung verfügen, müssen Sie Ausnahmeregeln für die Namen von Ressourcen hinzufügen, für die DirectAccess-Clients im Internet auf die Internetversion anstatt auf die Intranetversion zugreifen sollen.
- Wenn Sie Datenverkehr über Ihre Intranet-Webproxyserver an eine externe Website weiterleiten, ist die externe Website nur über das Intranet verfügbar. Er verwendet die Adressen der Webproxyserver, um eingehende Anforderungen zuzulassen. Fügen Sie in diesem Fall eine Ausnahme Regel für den voll qualifizierten Domänen Namen der externen Website hinzu, und geben Sie an, dass die Regel den Intranet-Webproxyserver anstelle der IPv6-Adressen der Intranet-DNS-Server verwendet.

Nehmen wir beispielsweise an, Sie testen eine externe Website mit dem Namen Test.contoso.com. Dieser Name kann nicht über Internet-DNS-Server aufgelöst werden, aber der Webproxyserver von Configuration Manager weiß, wie der Name aufgelöst werden kann und wie Anforderungen für die Website an den externen Webserver umgeleitet werden. Um den Sitezugriff durch Benutzer zu verhindern, die sich nicht im Contoso-Intranet befinden, lässt die externe Website nur Anforderungen von der IPv4-Internetadresse des Contoso-Webproxys zu. Daher können Intranetbenutzer auf die Website zugreifen, weil Sie den Webproxy von "Web" verwenden, DirectAccess-Benutzer jedoch nicht, weil Sie den Webproxy von "Web" nicht verwenden. Wenn eine NRPT-Ausnahmeregel für test.contoso.com konfiguriert wird, die den Contoso-Webproxy verwendet, werden Webseitenanforderungen für test.contoso.com über das IPv4-Internet zum Intranet-Webproxyserver weitergeleitet.

#### Einteilige Namen

Namen mit einer einzelnen Bezeichnung, wie z. b. <https://paycheck>, werden manchmal für Intranetserver verwendet. Wenn ein einzelner Bezeichnungs Name angefordert und eine DNS-Suffixsuchliste konfiguriert wird, werden die DNS-Suffixe in der Liste an den Namen der einzigen Bezeichnung angehängt. Wenn z. b. ein Benutzer auf einem Computer, der Mitglied der Corp.contoso.com-Domänen Typen ist, im Webbrower <https://paycheck>, lautet der als Name erstellte FQDN Paycheck.Corp.contoso.com. Standardmäßig basiert das angefügte Suffix auf dem primären DNS-Suffix des Client Computers.

#### NOTE

In einem separaten Namespace Szenario (in dem ein oder mehrere Domänen Computer ein DNS-Suffix haben, das nicht der Active Directory Domäne entspricht, der die Computer angehören), sollten Sie sicherstellen, dass die Suchliste so angepasst ist, dass Sie alle erforderlichen Suffixe enthält. Standardmäßig konfiguriert der Remote Zugriffs-Assistent den Active Directory DNS-Namen als primäres DNS-Suffix auf dem Client. Stellen Sie sicher, dass Sie das DNS-Suffix hinzufügen, das von den Clients für die Namensauflösung verwendet wird.

Wenn in Ihrer Organisation mehrere Domänen und Windows Internet Name Service (WINS) bereitgestellt werden und Sie eine Remote Verbindung herstellen, können Einzel Namen wie folgt aufgelöst werden:

- Durch Bereitstellen einer WINS-Forward-Lookupzone im DNS. Wenn Sie versuchen, Computername.DNS.zone1.Corp.contoso.com aufzulösen, wird die Anforderung an den WINS-Server weitergeleitet, der nur den Computernamen verwendet. Der Client geht davon aus, dass er eine reguläre DNS a Records-Anforderung ausgibt, es handelt sich jedoch tatsächlich um eine NetBIOS-Anforderung.

Weitere Informationen finden Sie unter [Verwalten einer Forward-Lookupzone](#).

- Durch Hinzufügen eines DNS-Suffixes (z. B. DNS.zone1.Corp.contoso.com) zum Standard Domänen-Gruppenrichtlinien Objekt.

#### Split-Brain-DNS

Split-Brain-DNS bezieht sich auf die Verwendung derselben DNS-Domäne für die Internet- und Intranetnamensauflösung.

Bei Split-Brain-DNS-bereit Stellungen müssen Sie die vollständig im Internet und im Intranet duplizierten voll qualifizierten Domänen Namen auflisten und entscheiden, welche Ressourcen der DirectAccess-Client erreichen soll: die Intranet- oder die Internet Version. Wenn DirectAccess-Clients die Internet Version erreichen möchten, müssen Sie der NRPT für jede Ressource den entsprechenden FQDN als Ausnahme Regel hinzufügen.

Wenn Sie in einer Split-Brain-DNS-Umgebung beide Versionen der Ressource verfügbar sein sollen, konfigurieren Sie Ihre Intranetressourcen mit Namen, die nicht die im Internet verwendeten Namen duplizieren. Weisen Sie Ihre Benutzer dann an, den alternativen Namen zu verwenden, wenn Sie auf die Ressource im Intranet zugreifen. Konfigurieren Sie z. B. www.Internal.contoso.com als internen Namen von www.contoso.com.

In einer Umgebung ohne Split-Brain-DNS unterscheidet sich der Internetnamespace vom Intranetnamespace. Die Contoso Corporation verwendet z. B. im Internet {1}contoso.com{2} und im Intranet {3}corp.contoso.com{4}. Da alle Intranetressourcen das DNS-Suffix corp.contoso.com verwenden, leitet die NRPT-Regel für corp.contoso.com alle DNS-Namensabfragen für Intranetressourcen an Intranet-DNS-Server weiter. DNS-Abfragen für Namen mit dem Suffix "contoso.com" stimmen nicht mit der Corp.contoso.com-Intranetnamespace-Regel in der NRPT und werden an Internet-DNS-Server gesendet. Bei einer Bereitstellung ohne Split-Brain-DNS ist für die NRPT keine zusätzliche Konfiguration erforderlich, da keine Doppelung der FQDNs für Intranet- und Internetressourcen auftritt. DirectAccess-Clients können auf Internet- und Intranetressourcen für Ihre Organisation zugreifen.

#### Planen des Namens der lokalen Namensauflösung für DirectAccess-Clients

Wenn ein Name nicht mit DNS aufgelöst werden kann, kann der DNS-Client Dienst in Windows Server 2012, Windows 8, Windows Server 2008 R2 und Windows 7 die lokale Namensauflösung verwenden, mit der Link-Local-Multicast-Namensauflösung (LLMNR) und NetBIOS über TCP/IP-Protokollen, um den Namen im lokalen Subnetz aufzulösen. Die lokale Namensauflösung ist in der Regel für Peer-zu-Peer-Verbindungen erforderlich, wenn sich der Computer in privaten Netzwerken befindet, z. B. in einem Heimnetzwerk mit einem einzelnen Subnetz.

Wenn der DNS-Client Dienst eine lokale Namensauflösung für intranetservernamen ausführt und der Computer mit einem freigegebenen Subnetz im Internet verbunden ist, können böswillige Benutzer LLMNR und NetBIOS über TCP/IP-Nachrichten erfassen, um intranetservernamen zu ermitteln. Auf der Seite DNS des Setup-Assistenten für Infrastruktur Server können Sie das lokale namens Auflösungsverhalten anhand der von den Intranet-DNS-Servern empfangenen Antworttypen konfigurieren. Die folgenden Optionen sind verfügbar:

- **Lokale Namensauflösung verwenden, wenn der Name nicht im DNS vorhanden ist:** diese Option ist die sicherste, da der DirectAccess-Client die lokale Namensauflösung nur für Servernamen durchführt, die nicht durch Intranet-DNS-Server aufgelöst werden können. Wenn die Intranet-DNS-Server erreicht werden können, werden die Namen der Intranetserver aufgelöst. Wenn die Intranet-DNS-Server nicht erreicht werden können, oder wenn andere DNS-Fehler auftreten, werden die Intranetservernamen nicht über die lokale Namensauflösung ins Subnetz durchgelassen.
- **Verwenden Sie die lokale Namensauflösung, wenn der Name nicht im DNS vorhanden ist oder DNS-Server nicht erreichbar sind, wenn sich der Client Computer in einem privaten Netzwerk befindet (empfohlen):** diese Option wird empfohlen, da Sie die lokale Namensauflösung in einem privaten Netzwerk nur dann zulässt, wenn die Intranet-DNS-Server nicht erreichbar sind.
- **Verwenden Sie die lokale Namensauflösung für alle Arten von DNS-Auflösungs Fehlern (am wenigsten sicher):** Dies ist die am wenigsten sichere Option, da die Namen von Intranet-Netzwerkservern über die lokale Namensauflösung in das lokale Subnetz gelangt sind.

## **Planen der Netzwerkadressen Server-Konfiguration**

Der Netzwerkadressenserver ist eine Website, die erkennt, ob sich DirectAccess-Clients im Unternehmensnetzwerk befinden. Clients im Unternehmensnetzwerk verwenden DirectAccess nicht zum erreichen interner Ressourcen. Stattdessen stellen Sie direkt eine Verbindung her.

Die Netzwerkadressen Server-Website kann auf dem Remote Zugriffs Server oder einem anderen Server in Ihrer Organisation gehostet werden. Wenn Sie den Netzwerkadressen Server auf dem Remote Zugriffs Server hosten, wird die Website automatisch erstellt, wenn Sie den Remote Zugriff bereitstellen. Wenn Sie den Netzwerkadressen Server auf einem anderen Server hosten, auf dem ein Windows-Betriebssystem ausgeführt wird, müssen Sie sicherstellen, dass Internetinformationsdienste (IIS) auf diesem Server installiert ist und dass die Website erstellt wird. Der Remote Zugriff konfiguriert keine Einstellungen auf dem Netzwerkadressen Server.

Stellen Sie sicher, dass die Netzwerkadressen Server-Website die folgenden Anforderungen erfüllt:

- Verfügt über ein HTTPS-Serverzertifikat.
- Bietet hohe Verfügbarkeit für Computer im internen Netzwerk.
- Ist für DirectAccess-Client Computer im Internet nicht zugänglich.
- 

Beachten Sie außerdem die folgenden Anforderungen für-Clients, wenn Sie die Netzwerkadressen Server-Website einrichten:

- DirectAccess-Clientcomputer müssen der Zertifizierungsstelle vertrauen, die das Serverzertifikat zur Netzwerkadressenserver-Website ausgegeben hat.
- DirectAccess-Clientcomputer auf dem internen Netzwerk müssen in der Lage sein, den Namen der Netzwerkadressenserver-Website aufzulösen.

### **Planen von Zertifikaten für den Netzwerkadressen Server**

Beachten Sie Folgendes, wenn Sie das für den Netzwerkadressen Server zu verwendende Website Zertifikat abrufen:

- Im Feld **Antragsteller** muss die IP-Adresse der Intranetschnittstelle des Netzwerkadressenservers oder der FQDN der Netzwerkadressen-URL angegeben sein.
- Verwenden Sie für das Feld **Erweiterte Schlüssel Verwendung** die Serverauthentifizierungs-OID.
- Das Netzwerkadressen Server-Zertifikat muss anhand einer Zertifikat Sperr Liste (CRL) überprüft werden. Verwenden Sie für das Feld **CRL-Verteilungs Punkte** einen Zertifikat Sperr Listen-Verteilungs Punkt, auf den DirectAccess-Clients, die mit dem Intranet verbunden sind, zugreifen können. Der Zertifikatsperrlisten-Verteilungspunkt sollte nicht von außerhalb des internen Netzwerks zugänglich sein.

### **Planen von DNS für den Netzwerkadressen Server**

DirectAccess-Clients versuchen, den Netzwerkadressenserver zu erreichen, um zu bestimmen, ob sie sich auf dem internen Netzwerk befinden. Clients im internen Netzwerk müssen in der Lage sein, den Namen des Netzwerkadressenservers aufzulösen, befinden sie sich jedoch im Internet, dürfen sie den Namen nicht auflösen. Um dies zu gewährleisten, wird der FQDN des Netzwerkadressenservers standardmäßig als Ausnahmeregel zum NRPT hinzugefügt.

## **Konfiguration der Plan Verwaltungs Server**

DirectAccess-Clients initiieren die Kommunikation mit Verwaltungs Servern, die Dienste wie Windows Update und Antivirus-Updates bereitstellen. DirectAccess-Clients verwenden auch das Kerberos-Protokoll, um sich gegenüber Domänen Controllern zu authentifizieren, bevor Sie auf das interne Netzwerk zugreifen. Während der Remoteverwaltung von DirectAccess-Clients kommunizieren Verwaltungsserver mit Clientcomputern, um Verwaltungsfunktionen wie zum Beispiel Software- oder Hardware-Bestandsbewertungen durchzuführen. Der Remotezugriff kann automatisch bestimmte Verwaltungsserver erkennen, zum Beispiel:

- Domänen Controller: die automatische Ermittlung von Domänen Controllern wird für die Domänen mit Client Computern und für alle Domänen in derselben Gesamtstruktur wie der Remote Zugriffs Server ausgeführt.
- Microsoft Endpoint Configuration Manager-Server

Domänen Controller und Configuration Manager Server werden automatisch erkannt, wenn DirectAccess erstmalig konfiguriert wird. Die erkannten Domänen Controller werden nicht in der-Konsole angezeigt, aber die Einstellungen können mithilfe von Windows PowerShell-Cmdlets abgerufen werden. Wenn Domänen Controller oder Configuration Manager Server geändert werden, wird durch Klicken auf **Updateverwaltung Server** in der-Konsole die Management Server Liste aktualisiert.

## **Verwaltungs Serveranforderungen**

- Verwaltungs Server müssen über den Infrastruktur Tunnel erreichbar sein. Wenn Sie Remotezugriff konfigurieren, werden diese beim Hinzufügen von Servern zur Verwaltungsserverliste automatisch über diesen Tunnel erreichbar gemacht.
- Verwaltungs Server, die Verbindungen zu DirectAccess-Clients initiieren, müssen IPv6 vollständig unterstützen, durch eine systemeigene IPv6-Adresse oder durch Verwendung einer von ISATAP zugewiesenen Adresse.

## **Planen von Active Directory Anforderungen**

Der Remote Zugriff verwendet Active Directory wie folgt:

- **Authentifizierung:** der Infrastruktur Tunnel verwendet die NTLMv2-Authentifizierung für das Computer Konto, das eine Verbindung mit dem RAS-Server herstellt, und das Konto muss sich in einer Active Directory Domäne befinden. Der intranettunnel verwendet die Kerberos-Authentifizierung für den Benutzer zum Erstellen des intranettunnels
- **Gruppenrichtlinie Objekte:** der Remote Zugriff sammelt Konfigurationseinstellungen in Gruppenrichtlinie Objekte (GPOs), die auf RAS-Server, Clients und interne Anwendungsserver angewendet werden.
- **Sicherheitsgruppen:** der Remote Zugriff verwendet Sicherheitsgruppen, um DirectAccess-Client Computer zu erfassen und zu identifizieren. GPOs werden auf die erforderlichen Sicherheitsgruppen angewendet.

Wenn Sie eine Active Directory Umgebung für eine Remote Zugriffs Bereitstellung planen, berücksichtigen Sie die folgenden Anforderungen:

- Mindestens ein Domänen Controller ist auf dem Betriebssystem Windows Server 2012, Windows Server 2008 R2 Windows Server 2008 oder Windows Server 2003 installiert.

Wenn sich der Domänen Controller in einem Umkreis Netzwerk befindet (und daher über den Netzwerkadapter mit Internet Zugriff des Remote Zugriffs Servers erreichbar ist), verhindern Sie, dass der RAS-Server den Remote Zugriffs Server erreicht. Sie müssen auf dem Domänen Controller Paketfilter hinzufügen, um die Konnektivität mit der IP-Adresse des Internet Adapters zu verhindern.

- Der Remotezugriffsserver muss Domänenmitglied sein.
- DirectAccess-Clients müssen Domänenmitglieder sein. Clients können folgenden Domänen angehören:
  - Domänen, die zur gleichen Gesamtstruktur wie der Remotezugriffsserver gehören.
  - Domänen mit bidirektonaler Vertrauensstellung zur Remotezugriffsserverdomäne.
  - Eine beliebige Domäne in einer Gesamtstruktur, die über eine bidirektionale Vertrauensstellung mit der Gesamtstruktur der RAS-Server Domäne verfügt.

#### **NOTE**

- Der Remotezugriffsserver kann nicht als Domänencontroller verwendet werden.
- Der Active Directory Domänen Controller, der für den Remote Zugriff verwendet wird, darf nicht vom externen Internet Adapter des Remote Zugriffs Servers aus erreichbar sein (der Adapter darf sich nicht im Domänen Profil der Windows-Firewall befinden).

#### **Planen der Clientauthentifizierung**

Beim Remote Zugriff unter Windows Server 2012 können Sie zwischen der integrierten Kerberos-Authentifizierung wählen, bei der Benutzernamen und Kenn Wörter verwendet werden, oder der Verwendung von Zertifikaten für die IPSec-Computer Authentifizierung.

**Kerberos-Authentifizierung:** Wenn Sie sich für die Verwendung Active Directory Anmelde Informationen für die Authentifizierung entscheiden, verwendet DirectAccess zuerst die Kerberos-Authentifizierung für den Computer und dann die Kerberos-Authentifizierung für den Benutzer. Wenn Sie diesen Authentifizierungsmodus verwenden, verwendet DirectAccess einen einzigen Sicherheitstunnel, der Zugriff auf den DNS-Server, den Domänen Controller und einen anderen Server im internen Netzwerk bietet.

**IPSec-Authentifizierung:** Wenn Sie die zweistufige Authentifizierung oder den Netzwerk Zugriffsschutz verwenden, verwendet DirectAccess zwei Sicherheitstunnel. Der Remote Zugriffs-Setup-Assistent konfiguriert die Verbindungs Sicherheitsregeln in der Windows-Firewall mit erweiterter Sicherheit. Diese Regeln geben beim Aushandeln der IPSec-Sicherheit für den RAS-Server die folgenden Anmelde Informationen an:

- Der Infrastruktur Tunnel verwendet die Anmelde Informationen des Computer Zertifikats für die erste Authentifizierung und Benutzer Anmelde Informationen (NTLMv2) für die zweite Authentifizierung. Benutzer Anmelde Informationen erzwingen die Verwendung von authentifiziertes Internetprotokoll (AuthIP) und ermöglichen den Zugriff auf einen DNS-Server und einen Domänen Controller, bevor der DirectAccess-Client die Kerberos-Anmelde Informationen für den intranettunnel verwenden kann.
- Der intranettunnel verwendet die Anmelde Informationen des Computer Zertifikats für die erste Authentifizierung und die Anmelde Informationen des Benutzers (Kerberos V5) für die zweite Authentifizierung.

#### **Planen mehrerer Domänen**

Die Liste der Verwaltungsserver sollte die Domänencontroller von allen Domänen umfassen, welche Sicherheitsgruppen enthalten, die DirectAccess-Clientcomputer beinhalten. Es sollten alle Domänen enthalten sein, die Benutzerkonten enthalten, die möglicherweise als DirectAccess-Clients konfigurierte Computer verwenden. Dadurch wird sichergestellt, dass Benutzer, die sich nicht in derselben Domäne wie der von ihnen genutzte Clientcomputer befinden, mit einem Domänencontroller in der Benutzerdomäne authentifiziert werden.

Diese Authentifizierung erfolgt automatisch, wenn sich die Domänen in derselben Gesamtstruktur befinden. Wenn eine Sicherheitsgruppe mit Client Computern oder Anwendungsservern in verschiedenen Gesamtstrukturen vorhanden ist, werden die Domänen Controller dieser Gesamtstrukturen nicht automatisch erkannt.

Gesamtstrukturen werden ebenfalls nicht automatisch erkannt. Sie können den Task **Updateverwaltung Server** in der **Remote Zugriffs Verwaltung** ausführen, um diese Domänen Controller zu erkennen.

Wenn möglich, sollten allgemeine Domänen Namen Suffixe während der Remote Zugriffs Bereitstellung zur NRPT hinzugefügt werden. Wenn es zum Beispiel zwei Domänen gibt, domain1.corp.contoso.com und domain2.corp.contoso.com, können Sie, anstatt zwei Einträge zur NRPT hinzuzufügen, auch einen allgemeinen DNS-Suffix-Eintrag hinzufügen, bei dem das Domänennamensuffix corp.contoso.com ist. Dies geschieht automatisch für Domänen im selben Stammverzeichnis. Domänen, die sich nicht im selben Stamm befinden, müssen manuell hinzugefügt werden.

#### **Planen Gruppenrichtlinie Objekt Erstellung**

Wenn Sie den Remote Zugriff konfigurieren, werden DirectAccess-Einstellungen in Gruppenrichtlinie Objekte

(GPOs) gesammelt. Zwei Gruppenrichtlinien Objekte werden mit DirectAccess-Einstellungen aufgefüllt und wie folgt verteilt:

- **DirectAccess-Client-GPO:** dieses Gruppenrichtlinien Objekt enthält Client Einstellungen, einschließlich der IPv6-Übergangstechnologie Einstellungen, NRPT-Einträge und Verbindungs Sicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit. Das Gruppenrichtlinienobjekt wird auf die für die Clientcomputer angegebenen Sicherheitsgruppen angewendet.
- **DirectAccess-Server-Gruppenrichtlinien Objekt:** dieses Gruppenrichtlinien Objekt enthält die DirectAccess-Konfigurationseinstellungen, die auf alle Server angewendet werden, die Sie als RAS-Server in der Bereitstellung konfiguriert haben. Sie enthält auch Verbindungs Sicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit.

#### **NOTE**

Die Konfiguration von Anwendungsservern wird bei der Remote Verwaltung von DirectAccess-Clients nicht unterstützt, da Clients nicht auf das interne Netzwerk des DirectAccess-Servers, auf dem sich die Anwendungsserver befinden, zugreifen können. Schritt 4 im Konfigurationsbildschirm des RAS-Setups steht für diese Art von Konfiguration nicht zur Verfügung.

Sie können GPOs automatisch oder manuell konfigurieren.

**Automatisch:** Wenn Sie angeben, dass GPOs automatisch erstellt werden, wird für jedes Gruppenrichtlinien Objekt ein Standardname angegeben.

**Manuell:** Sie können GPOs verwenden, die vom Active Directory-Administrator vordefiniert wurden.

Beachten Sie beim Konfigurieren der Gruppenrichtlinien Objekte die folgenden Warnungen:

- Es können keine anderen Gruppenrichtlinienobjekte mehr konfiguriert werden, nachdem DirectAccess auf die Verwendung bestimmter Gruppenrichtlinienobjekte konfiguriert wurde.
- Verwenden Sie das folgende Verfahren, um alle Remote Zugriffs-Gruppenrichtlinie Objekte zu sichern, bevor Sie DirectAccess-Cmdlets ausführen:

#### [\*\*Sichern und Wiederherstellen der Remote Zugriffs Konfiguration.\*\*](#)

- Unabhängig davon, ob Sie automatisch oder manuell konfigurierte Gruppenrichtlinien Objekte verwenden, müssen Sie eine Richtlinie für die Erkennung langsamer Verbindungen hinzufügen, wenn die Clients 3G verwenden werden. Der Pfad für Richtlinie: **Konfigurieren der Erkennung von Gruppenrichtlinie langsamen Verbindungen :**

#### [\*\*Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Gruppenrichtlinie.\*\*](#)

- Wenn die korrekten Berechtigungen zum Verknüpfen der Gruppenrichtlinien Objekte nicht vorhanden sind, wird eine Warnung ausgegeben. Der Remote Zugriffs Vorgang wird fortgesetzt, es findet jedoch keine Verknüpfung statt. Wenn diese Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, selbst wenn die Berechtigungen zu einem späteren Zeitpunkt hinzugefügt werden. Stattdessen muss der Administrator die Links manuell erstellen.

#### **Automatisch erstellte Gruppenrichtlinien Objekte**

Beachten Sie beim verwenden automatisch erstellter Gruppenrichtlinien Objekte Folgendes:

Automatisch erstellte Gruppenrichtlinien Objekte werden gemäß dem Speicherort und Verknüpfungs Ziel wie folgt angewendet:

- Für das Gruppenrichtlinien Objekt DirectAccess-Server wird der Speicherort und der Verknüpfungs Zielpunkt mit der Domäne mit dem RAS-Server angezeigt.
- Wenn die Gruppenrichtlinien Objekte für Client und Anwendungsserver erstellt werden, wird der

Speicherort auf eine einzelne Domäne festgelegt. Der GPO-Name wird in jeder Domäne gesucht, und die Domäne wird mit DirectAccess-Einstellungen aufgefüllt, falls vorhanden.

- Das Verknüpfungsziel wird auf den Stamm der Domäne festgelegt, in der das Gruppenrichtlinienobjekt erstellt wurde. Für jede Domäne, die Clientcomputer oder Anwendungsserver enthält, wird ein Gruppenrichtlinienobjekt erstellt, und das Gruppenrichtlinienobjekt wird mit dem Stamm der entsprechenden Domäne verknüpft.

Beim verwenden automatisch erstellter Gruppenrichtlinien Objekte zum Anwenden von DirectAccess-Einstellungen benötigt der RAS-Server Administrator die folgenden Berechtigungen:

- Berechtigungen zum Erstellen von Gruppenrichtlinien Objekten für jede Domäne.
- Berechtigungen zum Verknüpfen mit allen ausgewählten Client Domänen Stamm.
- Berechtigungen zum Verknüpfen mit den Server-GPO-Domänen Stämmen.
- Sicherheits Berechtigungen zum Erstellen, bearbeiten, löschen und Ändern der Gruppenrichtlinien Objekte.
- GPO-Leseberechtigungen für jede erforderliche Domäne. Diese Berechtigung ist nicht erforderlich, wird jedoch empfohlen, da Sie den Remote Zugriff ermöglicht, um sicherzustellen, dass GPOs mit doppelten Namen nicht vorhanden sind, wenn GPOs erstellt werden.

#### **Manuell erstellte Gruppenrichtlinien Objekte**

Beachten Sie beim Verwenden manuell erstellter Gruppenrichtlinienobjekte Folgendes:

- Die Gruppenrichtlinienobjekte sollten vorhanden sein, bevor Sie den Remotezugriffs-Setup-Assistenten ausführen.
- Zum Anwenden von DirectAccess-Einstellungen benötigt der RAS-Server Administrator vollständige Sicherheits Berechtigungen zum Erstellen, bearbeiten, löschen und Ändern der manuell erstellten Gruppenrichtlinien Objekte.
- Es wird eine Suche nach einem Link zum GPO in der gesamten Domäne durchgeführt. Wenn das Gruppenrichtlinienobjekt in der Domäne nicht verknüpft ist, wird im Domänenstamm automatisch eine Verknüpfung erstellt. Wenn die zum Erstellen der Verknüpfung erforderlichen Berechtigungen nicht verfügbar sind, wird eine Warnung ausgegeben.

#### **Wiederherstellen eines gelöschten Gruppenrichtlinienobjekts**

Wenn ein Gruppenrichtlinien Objekt auf einem RAS-Server, Client oder Anwendungsserver versehentlich gelöscht wurde, wird die folgende Fehlermeldung angezeigt: **Gruppenrichtlinien Objekt (GPO-Name) wurde nicht gefunden.**

Wenn eine Sicherung verfügbar ist, können Sie das Gruppenrichtlinienobjekt aus der Sicherung wiederherstellen.

Wenn keine Sicherung verfügbar ist, müssen Sie die Konfigurationseinstellungen entfernen und Sie neu konfigurieren.

So entfernen Sie Konfigurationseinstellungen

- Führen Sie das Windows PowerShell-Cmdlet **Uninstall-remoteaccess** aus.
- Öffnen Sie die **Remote Zugriffs Verwaltung**.
- In der angezeigten Fehlermeldung werden Sie darauf hingewiesen, dass das Gruppenrichtlinienobjekt nicht gefunden werden konnte. Klicken Sie auf **Konfigurationseinstellungen entfernen**. Nach Abschluss des Abschlusses wird der Server in einen nicht konfigurierten Zustand wieder hergestellt, und Sie können die Einstellungen neu konfigurieren.

# Schritt 2 Planen der Bereitstellung des Remote Zugriffs

09.04.2020 • 11 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nachdem Sie die Infrastruktur geplant haben, die Sie zum Einrichten des einzelnen RAS-Servers für die Remote Verwaltung von DirectAccess-Clients verwenden möchten, können Sie die Einstellungen planen, die vom Setup-Assistenten für den Remote Zugriff verwendet werden.

## NOTE

Bevor Sie mit diesen Aufgaben fortfahren, finden Sie weitere Informationen unter [Schritt 1: Planen der Infrastruktur für den Remote Zugriff](#).

AUFGABE	BESCHREIBUNG
<a href="#">Planen einer Strategie für die Client Bereitstellung</a>	Legen Sie fest, welche verwalteten Computer als DirectAccess-Clients konfiguriert werden sollen.
<a href="#">Planen einer Bereitstellungs Strategie für den Remote Zugriffs Server</a>	Planen Sie die Bereitstellung des Remotezugriffsservers.
<a href="#">Planen der Konfigurationen der Infrastruktur Server</a>	Planen Sie die Infrastruktur Server in der Remote Zugriffs Bereitstellung, einschließlich DirectAccess-Netzwerkadressen Server, DNS-Server und DirectAccess-Verwaltungs Server.

## Planen einer Strategie für die Client Bereitstellung

Bei der Planung Ihrer Clientbereitstellung müssen drei Entscheidungen getroffen werden:

1. Ist DirectAccess nur für mobile Computer oder für alle Computer in einer angegebenen Sicherheitsgruppe verfügbar?

Wenn Sie DirectAccess-Clients im DirectAccess-Client-Setup-Assistenten konfigurieren, können Sie festlegen, dass nur Mobile Computer in angegebenen Sicherheitsgruppen mithilfe von DirectAccess eine Verbindung mit dem Server herstellen können. Wenn Sie nur den Zugriff für mobile Computer zulassen, konfiguriert der Remotezugriff automatisch einen WMI-Filter, um sicherzustellen, dass das Gruppenrichtlinienobjekt des DirectAccess-Clients nur auf mobile Computer in den angegebenen Sicherheitsgruppen angewendet wird. Der Remotezugriffsadministrator benötigt Berechtigungen zum Erstellen oder Bearbeiten der WMI-Filter für die Gruppenrichtlinie, um diese Einstellung zu aktivieren.

2. In welchen Sicherheitsgruppen sollen die DirectAccess-Clientcomputer enthalten sein?

DirectAccess-Einstellungen sind im DirectAccess-Client Gruppenrichtlinie-Objekt (GPO) enthalten. Das Gruppenrichtlinienobjekt wird auf Computer angewendet, die in den Sicherheitsgruppen enthalten sind, die Sie in dem DirectAccess-Client-Setup-Assistenten angegeben haben. Sie können Sicherheitsgruppen angeben, die in einer beliebigen unterstützten Domäne enthalten sind.

Bevor Sie den Remote Zugriff konfigurieren, müssen Sie die Sicherheitsgruppen erstellen. Nachdem Sie die

Remote Zugriffs Bereitstellung fertiggestellt haben, können Sie der Sicherheitsgruppe Computer hinzufügen. Wenn Sie jedoch Client Computer hinzufügen, die sich in einer anderen Domäne als der Sicherheitsgruppe befinden, wird das Client-Gruppenrichtlinien Objekt nicht auf diese Clients angewendet. Wenn Sie z. B. SG1 in Domäne A für DirectAccess-Clients erstellt haben und später Clients von Domäne b zu dieser Gruppe hinzufügen, wird das Client-Gruppenrichtlinien Objekt nicht auf Clients in Domäne b angewendet.

Um dieses Problem zu vermeiden, erstellen Sie eine neue Client Sicherheitsgruppe für jede Domäne, die Client Computer enthält. Wenn Sie keine neue Sicherheitsgruppe erstellen möchten, führen Sie alternativ das Windows PowerShell-Cmdlet **Add-daclient** mit dem Namen des neuen Gruppenrichtlinien Objekts für die neue Domäne aus.

### 3. Welche Einstellungen werden für den DirectAccess-netzwerkkonnektivitätsassistent konfiguriert?

Der DirectAccess-netzwerkkonnektivitätsassistent wird auf Client Computern ausgeführt und stellt zusätzliche Informationen über die DirectAccess-Verbindung mit Endbenutzern bereit. Im DirectAccess-Client-Setup-Assistenten können Sie Folgendes konfigurieren:

- **Konnektivitätsverifier**

Ein Standardwebtest wird erstellt, den Clients verwenden, um die Verbindung zum internen Netzwerk zu prüfen. Der Standardname lautet `https://directaccess-WebProbeHost.<domain_name>`. Der Name sollte manuell im DNS registriert werden. Sie können andere Konnektivitätsprobleme erstellen, die andere Webadressen über HTTP oder Ping verwenden. Für jeden Verbindungsprüfer muss ein DNS-Eintrag vorhanden sein.

- **Helpdesk-e-Mail-Adresse**

Wenn bei Endbenutzern DirectAccess-Konnektivitätsprobleme auftreten, können Sie eine e-Mail mit Diagnoseinformationen an den Remote Zugriffs Administrator senden, die das Problem beheben können.

- **DirectAccess-Verbindungs Name**

Sie können einen DirectAccess-Verbindungs Namen angeben, um Endbenutzern zu helfen, die DirectAccess-Verbindung auf Ihrem Computer zu identifizieren.

- **DirectAccess-Clients die Verwendung der lokalen Namensauflösung gestatten**

Clients benötigen eine Möglichkeit zum lokalen Auflösen von Namen. Wenn Sie zulassen, dass DirectAccess-Clients die lokale Namensauflösung verwenden, können Endbenutzer zum Auflösen von Namen lokale DNS-Server verwenden. Wenn Endbenutzer lokale DNS-Server für die Namensauflösung verwenden möchten, sendet DirectAccess keine Auflösungsanforderungen für einzelne Bezeichnungsnamen an den internen DNS-Server des Unternehmens. Stattdessen wird die lokale Namensauflösung verwendet (mit der Link-Local-Multicast-Namensauflösung (LLMNR) und NetBIOS über TCP/IP-Protokollen).

## Planen einer Bereitstellungs Strategie für den Remote Zugriffs Server

Bei der Planung der Bereitstellung des Remote Zugriffs Servers müssen folgende Entscheidungen getroffen werden:

- **Netzwerktopologie**

Beim Bereitstellen eines Remote Zugriffs Servers sind zwei Topologien verfügbar:

- **Zwei Adapter:** mit zwei Netzwerkadapters kann der Remote Zugriff mit einem Netzwerkadapter konfiguriert werden, der direkt mit dem Internet verbunden ist, und mit dem anderen, der mit dem

internen Netzwerk verbunden ist. Alternativ dazu wird der Server hinter einem Edgegerät installiert, z. b. einer Firewall oder einem Router. In dieser Konfiguration ist ein Netzwerkadapter mit dem Umkreis Netzwerk und der andere mit dem internen Netzwerk verbunden.

- **Einzelner Netzwerkadapter:** in dieser Konfiguration wird der RAS-Server hinter einem Edgegerät installiert, z. b. einer Firewall oder einem Router. Der Netzwerkadapter ist mit dem internen Netzwerk verbunden.

- **Leistungsverlauf für Netzwerkadapter**

Der Setup-Assistent für den Remote Zugriffs Server erkennt automatisch die Netzwerkadapter, die auf dem Remote Zugriffs Server konfiguriert sind. Vergewissern Sie sich, dass die richtigen Adapter ausgewählt sind.

- **IP-HTTPS-Zertifikat**

Der Setup-Assistent für den Remotezugriffsserver erkennt automatisch ein Zertifikat, das für die IP-HTTPS-Verbindung geeignet ist. Der Antragstellernname von Ihnen gewählten Zertifikats muss mit der ConnectTo-Adresse übereinstimmen. Wenn Sie selbst signierte Zertifikate verwenden, können Sie ein Zertifikat verwenden, das automatisch vom Remote Zugriffs Server erstellt wird.

- **IPv6-Präfixe**

Wenn der Setup-Assistent für den Remotezugriffsserver erkennt, dass IPv6 auf den Netzwerkadapters bereitgestellt wurde, füllt er automatisch IPv6-Präfixe für das interne Netzwerk auf. Ein IPv6-Präfix zum Zuweisen für die DirectAccess-Clientcomputer und ein IPv6-Präfix zum Zuweisen für die VPN-Clientcomputer. Wenn die automatisch generierten Präfixe nicht mit Ihrer systemeigenen IPv6- oder ISATAP-Infrastruktur übereinstimmen, müssen Sie sie manuell ändern.

- **Authentifizierung**

Sie können eine der folgenden Methoden zum Authentifizieren von DirectAccess-Clients auf dem RAS-Server auswählen:

- **Benutzeroauthentifizierung:** Sie können es Benutzern ermöglichen, sich mit Active Directory Anmelde Informationen oder mit zweistufiger Authentifizierung zu authentifizieren.
- **Computer Authentifizierung:** Sie können die Computer Authentifizierung für die Verwendung von Zertifikaten konfigurieren. Oder der Remote Zugriffs Server kann als Proxy für die Kerberos-Authentifizierung fungieren, ohne dass Zertifikate erforderlich sind.
- **Windows 7-Clients** Standardmäßig können Client Computer, auf denen Windows 7 ausgeführt wird, keine Verbindung mit einer Remote Zugriffs Bereitstellung unter Windows Server 2012 herstellen. Wenn Sie über Clients verfügen, auf denen Windows 7 in Ihrer Organisation ausgeführt wird und die den Remote Zugriff auf interne Ressourcen benötigen, können Sie Ihnen gestatten, eine Verbindung herzustellen. Clientcomputer, die auf interne Ressourcen zugreifen sollen, müssen Mitglied einer Sicherheitsgruppe sein, die Sie im DirectAccess-Client-Setup-Assistenten angeben.

**NOTE**

Wenn Sie es Clients mit Windows 7 gestatten, eine Verbindung mithilfe von DirectAccess herzustellen, müssen Sie die Computer Zertifikat Authentifizierung verwenden.

- **VPN-Konfiguration**

Bevor Sie den Remote Zugriff konfigurieren, entscheiden Sie, ob Sie VPN-Zugriff auf Remote Clients bereitstellen möchten. Sie sollten VPN-Zugriff bereitstellen, wenn Sie in Ihrer Organisation über Client Computer verfügen, die keine DirectAccess-Konnektivität unterstützen (z. b. Wenn Sie nicht verwaltet werden oder wenn ein Betriebssystem ausgeführt wird, für das DirectAccess nicht unterstützt wird). Mithilfe

des Setup-Assistenten für den Remote Zugriffs Server können Sie konfigurieren, wie IP-Adressen zugewiesen werden (mithilfe von DHCP oder aus einem statischen Adresspool) und wie VPN-Clients authentifiziert werden (mithilfe von Active Directory oder einem RADIUS-Server).

## Planen der Konfigurationen der Infrastruktur Server

Der Remote Zugriff erfordert drei Arten von Infrastruktur Servern:

- **Netzwerkadressen Server**
- **DNS-Server**
- **Verwaltungs Server**

## Siehe auch

- [Schritt 1: Planen der Infrastruktur für den Remote Zugriff](#)

# Installieren und Konfigurieren der Bereitstellung für die Remote Verwaltung von DirectAccess-Clients

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält eine Einführung in die Konfigurationsschritte, die für die Bereitstellung eines einzelnen Remote Zugriffs Servers erforderlich sind, der für die Remote Verwaltung von DirectAccess-Clients verwendet werden kann.

- [Schritt 1: Konfigurieren der Infrastruktur für den Remote Zugriff](#): in diesem Thema wird beschrieben, wie Sie Netzwerk-und Servereinstellungen, Zertifikat Anforderungen, DNS-Einstellungen, die Bereitstellung des Netzwerkadressen Servers, DirectAccess-Verwaltungs Server, Active Directory Einstellungen und Gruppenrichtlinie Objekte konfigurieren.
- [Schritt 2: Konfigurieren des Remote Zugriffs Servers](#): in diesem Thema wird beschrieben, wie Sie DirectAccess-Client Computer, Server Einstellungen, Infrastruktur-und Anwendungsserver konfigurieren.
- [Schritt 3: Überprüfen der Bereitstellung](#): in diesem Thema wird beschrieben, wie Sie die Bereitstellung überprüfen.

# Schritt 1 Konfigurieren der Remote Zugriffs Infrastruktur

09.04.2020 • 36 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Durch Windows Server 2012 werden DirectAccess und RRAS (Routing and Remote Access Service, Routing- und RAS-Dienst) zu einer einzigen Remotezugriffsrolle zusammengefasst.

In diesem Thema wird beschrieben, wie Sie die Infrastruktur konfigurieren, die für eine erweiterte Remote Zugriffs Bereitstellung mit einem einzelnen Remote Zugriffs Server in einer gemischten IPv4-und IPv6-Umgebung erforderlich ist. Vergewissern Sie sich vor Beginn der Bereitstellungs Schritte, dass Sie die in [Schritt 1: Planen der Remote Zugriffs Infrastruktur](#)beschriebenen Planungsschritte abgeschlossen haben.

AUFGABE	BESCHREIBUNG
Konfigurieren von Servernetzwerkeinstellungen	Konfigurieren Sie die Servernetzwerkeinstellungen auf dem Remotezugriffsserver.
Konfigurieren des Routings im Unternehmensnetzwerk	Konfigurieren Sie das Routing im Unternehmensnetzwerk, damit der Datenverkehr ordnungsgemäß weitergeleitet wird.
Konfigurieren von Firewalls	Konfigurieren Sie bei Bedarf zusätzliche Firewalls.
Konfigurieren von Zertifizierungsstellen und Zertifikaten	Konfigurieren Sie bei Bedarf eine Zertifizierungsstelle (Certification Authority, ca) und alle anderen Zertifikat Vorlagen, die in der Bereitstellung erforderlich sind.
Konfigurieren des DNS-Servers	Konfigurieren Sie DNS-Einstellungen für den Remotezugriffsserver.
Konfigurieren von Active Directory	Fügen Sie Client Computer und RAS-Server der Active Directory Domäne hinzu.
Konfigurieren der Gruppenrichtlinienobjekte	Konfigurieren Sie bei Bedarf Gruppenrichtlinie Objekte (GPOs) für die Bereitstellung.
Konfigurieren von Sicherheitsgruppen	Konfigurieren Sie Sicherheitsgruppen, die DirectAccess-Clientcomputer und weitere Sicherheitsgruppen enthalten, die für die Bereitstellung erforderlich sind.
Konfigurieren des Netzwerkadressenservers	Konfigurieren Sie den Netzwerkadressenserver, dazu gehört auch die Installation des Netzwerkadressenserver-Websitezertifikats.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

# Konfigurieren von Servernetzwerk Einstellungen

Abhängig davon, ob Sie den Remote Zugriffs Server am Rand oder hinter einem NAT-Gerät (Network Address Translation, Netzwerk Adressübersetzung) platzieren möchten, sind die folgenden Einstellungen für die Netzwerkschnittstellen Adresse für eine einzelne Server Bereitstellung in einer Umgebung mit IPv4 und IPv6 erforderlich. Sämtliche IP-Adressen können im **Netzwerk- und Freigabecenter** von Windows mit der Option **Adaptereinstellungen ändern** konfiguriert werden.

## Edge-Topologie:

Folgendes wird benötigt:

- Zwei aufeinander folgende öffentliche statische IPv4-oder IPv6-Adressen mit Internet Zugriff.

### NOTE

Zwei aufeinander folgende öffentliche IPv4-Adressen sind für Teredo erforderlich. Falls Sie Teredo nicht verwenden, können Sie eine einzelne, öffentliche, statische IPv4-Adresse konfigurieren.

- Eine einzelne, interne, statische IPv4- oder IPv6-Adresse

## Hinter dem NAT-Gerät (zwei Netzwerkadapter) :

Erfordert eine einzelne, interne, statische IPv4-oder IPv6-Adresse mit Netzwerk Zugriff.

## Hinter dem NAT-Gerät (ein Netzwerkadapter) :

Erfordert eine einzelne statische IPv4-oder IPv6-Adresse.

Wenn der RAS-Server über zwei Netzwerkadapter verfügt (eine für das Domänen Profil und die andere für ein öffentliches oder privates Profil), aber Sie eine einzelne Netzwerkadapter Topologie verwenden, lautet die Empfehlung wie folgt:

1. Stellen Sie sicher, dass der zweite Netzwerkadapter ebenfalls im Domänen Profil klassifiziert ist.
2. Wenn der zweite Netzwerkadapter aus irgendeinem Grund nicht für das Domänen Profil konfiguriert werden kann, muss die DirectAccess IPSec-Richtlinie mithilfe des folgenden Windows PowerShell-Befehls manuell auf alle Profile festgelegt werden:

```
$gposession = Open-NetGPO -PolicyStore <Name of the server GPO>
Set-NetIPsecRule -DisplayName <Name of the IPsec policy> -GPOSession $gposession -Profile Any
Save-NetGPO -GPOSession $gposession
```

Die Namen der IPSec-Richtlinien, die in diesem Befehl verwendet werden sollen, sind **DirectAccess-daservertoinfranrd** und **DirectAccess-DaServerToCorp**.

# Konfigurieren des Routings im Unternehmensnetzwerk

Konfigurieren Sie das Routing im Unternehmensnetzwerk wie folgt:

- Wenn in der Organisation eine systemeigene IPv6-Adresse bereitgestellt wird, fügen Sie ihr eine Route hinzu, damit die Router im internen Netzwerk den IPv6-Datenverkehr zurück über den Remotezugriffsserver leiten.
- Konfigurieren Sie die IPv4- und IPv6-Routen der Organisation manuell auf den Remotezugriffsservern. Fügen Sie eine veröffentlichte Route hinzu, sodass der gesamte Datenverkehr mit dem IPv6-Präfix (/48) an das interne Netzwerk weitergeleitet wird. Fügen Sie außerdem für IPv4-Datenverkehr explizite Routen hinzu,

damit IPv4-Datenverkehr an das interne Netzwerk weitergeleitet wird.

## Konfigurieren von Firewalls

Wenden Sie die folgenden Firewallausnahmen für RAS-Datenverkehr an, je nachdem, welche Netzwerkeinstellungen Sie ausgewählt haben.

### RAS-Server im IPv4-Internet

Wenden Sie die folgenden Firewallausnahmen mit Internet Zugriff für RAS-Datenverkehr an, wenn der RAS-Server sich im IPv4-Internet befindet:

- **Teredo-Datenverkehr**

UDP-Zielport 3544 (User Datagram Protocol) eingehend und UDP-Quellport 3544 ausgehend. Wenden Sie diese Ausnahme für beide aufeinander folgenden öffentlichen IPv4-Adressen auf dem Remote Zugriffs Server an.

- **IPv6-zu-IPv4-Verkehr**

IP-Protokoll 41 eingehend und ausgehend. Wenden Sie diese Ausnahme für beide aufeinander folgenden öffentlichen IPv4-Adressen auf dem Remote Zugriffs Server an.

- **IP-HTTPS-Datenverkehr**

Der TCP-Zielport 443 (Transmission Control Protocol) und der TCP-Quellport 443 ausgehend. Hat der RAS-Server nur einen Netzwerkadapter und der Netzwerkadressenserver ist auf dem RAS-Server, wird auch TCP-Port 62000 benötigt. Wenden Sie diese Ausnahmen nur auf die Adresse an, auf die der externe Name des Servers aufgelöst wird.

**NOTE**

Diese Ausnahme wird auf dem Remote Zugriffs Server konfiguriert. Alle anderen Ausnahmen werden auf der Edge-Firewall konfiguriert.

### RAS-Server im IPv6-Internet

Wenden Sie die folgenden Firewallausnahmen mit Internet Zugriff für RAS-Datenverkehr an, wenn der RAS-Server sich im IPv6-Internet befindet:

- IP-Protokoll 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend.
- Internet Control Message Protocol für IPv6 (ICMPv6)-Datenverkehr eingehend und ausgehend: nur für Teredo-Implementierungen.

### RAS-Datenverkehr

Wenden Sie die folgenden internen netzwerkfirewallausnahmen für RAS-Datenverkehr an:

- ISATAP: eingehende und ausgehende Protokolle 41
- TCP/UDP für den gesamten IPv4-oder IPv6-Datenverkehr
- ICMP für den gesamten IPv4-oder IPv6-Datenverkehr

## Konfigurieren von Zertifizierungsstellen und Zertifikaten

Mit dem Remote Zugriff in Windows Server 2012 können Sie zwischen der Verwendung von Zertifikaten für die Computer Authentifizierung oder der Verwendung einer integrierten Kerberos-Authentifizierung mit

Benutzernamen und Kenn Wörtern wählen. Außerdem müssen Sie ein IP-HTTPS-Zertifikat auf dem Remote Zugriffs Server konfigurieren. In diesem Abschnitt wird erläutert, wie diese Zertifikate konfiguriert werden.

Weitere Informationen zum Einrichten einer Public Key-Infrastruktur (PKI) finden Sie unter [Active Directory Certificate Services](#).

## Konfigurieren der IPSec-Authentifizierung

Auf dem RAS-Server und allen DirectAccess-Clients ist ein Zertifikat erforderlich, damit die IPSec-Authentifizierung verwendet werden kann. Das Zertifikat muss von einer internen Zertifizierungsstelle (Certification Authority, ca) ausgestellt werden. RAS-Server und DirectAccess-Clients müssen der Zertifizierungsstelle vertrauen, die die Stamm-und zwischen Zertifikate ausgibt.

[So konfigurieren Sie die IPsec-Authentifizierung](#)

1. Entscheiden Sie sich bei der internen Zertifizierungsstelle, ob Sie die standardmäßige Computer Zertifikat Vorlage verwenden möchten, oder wenn Sie eine neue Zertifikat Vorlage erstellen möchten, wie unter [Erstellen von Zertifikat Vorlagen](#)beschrieben.

### NOTE

Wenn Sie eine neue Vorlage erstellen, muss Sie für die Client Authentifizierung konfiguriert werden.

2. Stellen Sie die Zertifikat Vorlage bei Bedarf bereit. Weitere Informationen finden Sie unter Bereitstellen von [Zertifikat Vorlagen](#).
3. Konfigurieren Sie bei Bedarf die Vorlage für die automatische Registrierung.
4. Konfigurieren Sie bei Bedarf die automatische Zertifikat Registrierung. Weitere Informationen finden Sie unter [Konfigurieren](#)der automatischen Zertifikat Registrierung.

## Konfigurieren von Zertifikat Vorlagen

Wenn Sie eine interne Zertifizierungsstelle zum Ausstellen von Zertifikaten verwenden, müssen Sie Zertifikat Vorlagen für das IP-HTTPS-Zertifikat und das Netzwerkadressen Server-Website Zertifikat konfigurieren.

[So konfigurieren Sie eine Zertifikatvorlage](#)

1. Erstellen Sie eine Zertifikatvorlage für die interne Zertifizierungsstelle, wie beschrieben in [Erstellen von Zertifikatvorlagen](#).
2. Stellen Sie die Zertifikatvorlage wie unter [Deploying Certificate Templates](#)beschrieben bereit.

Nachdem Sie Ihre Vorlagen vorbereitet haben, können Sie Sie zum Konfigurieren der Zertifikate verwenden. Weitere Informationen finden Sie in den folgenden Prozeduren:

- [Konfigurieren des IP-HTTPS-Zertifikats](#)
- [Konfigurieren des Netzwerkadressen Servers](#)

## Konfigurieren des IP-HTTPS-Zertifikats

Für den Remotezugriff ist zum Authentifizieren von IP-HTTPS-Verbindungen mit dem Remotezugriffsserver ein IP-HTTPS-Zertifikat erforderlich. Für das IP-HTTPS-Zertifikat sind drei Zertifikatoptionen verfügbar:

- **Publikums**

Wird von einem Drittanbieter bereitgestellt.

- **Private**

Das Zertifikat basiert auf der Zertifikat Vorlage, die Sie in [Konfigurieren von Zertifikat Vorlagen](#)erstellt haben. Hierfür ist ein Zertifikat Sperr Listen-Verteilungs Punkt erforderlich, der über einen öffentlich auflösbaren FQDN erreichbar ist.

- **Selbst signiert**

Für dieses Zertifikat ist ein CRL-Verteilungs Punkt erforderlich, der über einen öffentlich auflösbar FQDN erreichbar ist.

**NOTE**

Selbstsignierte Zertifikate können nicht in Bereitstellungen für mehrere Standorte verwendet werden.

Stellen Sie sicher, dass das für die IP-HTTPS-Authentifizierung verwendete Websitezertifikat die folgenden Anforderungen erfüllt:

- Der Name des Zertifikat Antragstellers sollte der extern auflösbar voll qualifizierte Domänen Name (FQDN) der IP-HTTPS-URL (die ConnectTo-Adresse) sein, die nur für die IP-HTTPS-Verbindungen des RAS-Servers verwendet wird.
- Der allgemeine Name des Zertifikats sollte dem Namen der IP-HTTPS-Website entsprechen.
- Geben Sie im Feld Betreff die IPv4-Adresse des externen Adapters des Remote Zugriffs Servers oder den voll qualifizierten Namen der IP-HTTPS-URL an.
- Verwenden Sie für das Feld **Erweiterte Schlüssel Verwendung** die Serverauthentifizierungs-Objekt Kennung (OID).
- Geben Sie im Feld **Sperrlisten-Verteilungspunkte** einen Zertifikatsperrlisten-Verteilungspunkt an, auf den mit dem Internet verbundene DirectAccess-Clients zugreifen können.
- Das IP-HTTPS-Zertifikat muss einen privaten Schlüssel enthalten.
- Das IP-HTTPS-Zertifikat muss direkt in den persönlichen Speicher importiert werden.
- Die Namen von IP-HTTPS-Zertifikaten können Platzhalter enthalten.

So installieren Sie das IP-HTTPS-Zertifikat von einer internen Zertifizierungsstelle

1. Auf dem Remote Zugriffs Server: Geben Sie auf dem **Start** BildschirmMMC. exeein, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-ins hinzufügen oder entfernen** auf **Zertifikate, Hinzufügen, Computerkonto, Weiter, Lokaler Computer, Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **alle Aufgaben**, klicken Sie auf **Neues Zertifikat anfordern**, und klicken Sie dann zweimal auf **weiter**.
6. Aktivieren Sie auf der Seite **Zertifikate anfordern** das Kontrollkästchen für die Zertifikat Vorlage, die Sie unter Konfigurieren von Zertifikat Vorlagen erstellt haben, und klicken Sie bei Bedarf auf Weitere Informationen, die für die Registrierung dieses Zertifikats erforderlich sind.
7. Klicken Sie im Dialogfeld **Zertifikateigenschaften** auf der Registerkarte **Antragsteller** im Bereich **Antragstellename** unter **Typ** auf **Allgemeiner Name**.
8. Geben Sie unter **Wert** die IPv4-Adresse des externen Adapters des Remote Zugriffs Servers oder den voll qualifizierten Namen der IP-HTTPS-URL an, und klicken Sie dann auf **Hinzufügen**.
9. Wählen Sie unter **Alternativer Name** für **Typ** die Option **DNS** aus.

10. Geben Sie unter **Wert** die IPv4-Adresse des externen Adapters des Remote Zugriffs Servers oder den voll qualifizierten Namen der IP-HTTPS-URL an, und klicken Sie dann auf **Hinzufügen**.
11. Auf der Registerkarte **Allgemein** unter **Anzeigename** können Sie einen Namen für das Zertifikat eingeben, sodass Sie es schneller identifizieren können.
12. Klicken Sie auf der Registerkarte **Erweiterungen** auf den Pfeil neben dem Feld **Erweiterte Schlüsselverwendung** und vergewissern Sie sich, dass in der Liste **Ausgewählte Optionen** Serverauthentifizierung angezeigt wird.
13. Klicken Sie auf **OK**, **Registrieren** und dann auf **Fertig stellen**.
14. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, ob das neue Zertifikat mit dem beabsichtigten Zweck der Server Authentifizierung registriert wurde.

## Konfigurieren des DNS-Servers

Sie müssen einen DNS-Eintrag für die Netzwerkadressenserver-Website für das interne Netzwerk in Ihrer Bereitstellung manuell konfigurieren.

### **So fügen Sie den Netzwerkadressen Server und den Webtest hinzu**

1. Auf dem internen Netzwerk-DNS-Server: Geben Sie auf dem **Start Bildschirmdnsmgmt. mscein**, und drücken Sie dann die **EINGABETASTE**.
2. Erweitern Sie im linken Bereich der **DNS-Manager**-Konsole die Forward-Lookupzone für Ihre Domäne. Klicken Sie mit der rechten Maustaste auf die Domäne, und klicken Sie auf **neuer Host (A oder AAAA)**.
3. Geben Sie im Dialogfeld **neuer Host** in das Feld **Name (verwendet übergeordneter Domänen Name)** den DNS-Namen für die Netzwerkadressen Server-Website ein (der Name, der von den DirectAccess-Clients zum Herstellen einer Verbindung mit dem Netzwerkadressen Server verwendet wird). Geben Sie im Feld **IP-Adresse** die IPv4-Adresse des Netzwerkadressen Servers ein, klicken Sie auf **Host hinzufügen**, und klicken Sie dann auf **OK**.
4. Geben Sie im Dialogfeld **neuer Host** in das Feld **Name (verwendet übergeordneter Domänen Name, falls leer)** den DNS-Namen für den Webtest ein (der Name für den Standardweb Test ist DirectAccess-WebProbe Host). Geben Sie in das Feld **IP-Adresse** die IPv4-Adresse des Webtests ein und klicken Sie dann auf **Host hinzufügen**.
5. Wiederholen Sie diesen Vorgang für directaccess-corpconnectivityhost und manuell erstellte Verbindungsprüfer. Klicken Sie im Dialogfeld **DNS** auf **OK**.
6. Klicken Sie auf **Fertig**.

### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address
<network_location_server_IPv4_address>
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address
<network_location_server_IPv6_address>
```

Außerdem müssen Sie die DNS-Einträge für folgende Elemente konfigurieren:

- Der IP-HTTPS-Server

DirectAccess-Clients müssen in der Lage sein, den DNS-Namen des Remote Zugriffs Servers aus dem Internet aufzulösen.

- **CRL-Sperr Überprüfung**

DirectAccess verwendet Zertifikat Sperr Überprüfungen für die IP-HTTPS-Verbindung zwischen DirectAccess-Clients und dem RAS-Server sowie für die HTTPS-basierte Verbindung zwischen dem DirectAccess-Client und dem Netzwerkadressen Server. In beiden Fällen müssen DirectAccess-Clients in der Lage sein, auf den Zertifikatsperllisten-Verteilungspunkt zuzugreifen und ihn aufzulösen.

- **ISATAP**

ISATAP (Inner Site Automatic Tunnel Adressierungs Protokoll) verwendet Tunnel, um DirectAccess-Clients das Herstellen einer Verbindung mit dem RAS-Server über das IPv4-Internet zu ermöglichen, wobei IPv6-Pakete in einem IPv4-Header gekapselt werden. Es kann vom Remotezugriff verwendet werden, um IPv6-Konnektivität mit ISATAP-Hosts im gesamten Intranet bereitzustellen. In einer nicht systemeigenen IPv6-Netzwerkumgebung konfiguriert sich der RAS-Server automatisch als ISATAP-Router. Auflösungsunterstützung für den ISATAP-Namen ist nicht erforderlich.

## Konfigurieren von Active Directory

Der Remotezugriffsserver und alle DirectAccess-Clientcomputer müssen zu einer Active Directory-Domäne zusammengeführt werden. DirectAccess-Clientcomputer müssen Mitglied folgender Domänenentypen sein:

- Domänen, die zur gleichen Gesamtstruktur wie der Remotezugriffsserver gehören.
- Domänen, die zu Gesamtstrukturen mit einer bidirektionalen Vertrauensstellung zur Remotezugriffsserver-Gesamtstruktur gehören.
- Domänen mit bidirektonaler Vertrauensstellung zur Remotezugriffsserverdomäne.

### **So fügen Sie den RAS-Server einer Domäne hinzu**

1. Klicken Sie im Server-Manager auf **Lokaler Server**. Klicken Sie im Detailbereich auf den Link neben **Computername**.
2. Klicken Sie im Dialogfeld **Systemeigenschaften** auf die Registerkarte **Computername** und klicken Sie dann auf **Ändern**.
3. Geben Sie im Feld **Computername** den Namen des Computers ein, wenn Sie beim Hinzufügen des Servers zur Domäne auch den Computernamen ändern. Klicken Sie unter **Mitglied vonauf Domäne**, und geben Sie dann den Namen der Domäne ein, der Sie den Server hinzufügen möchten (z. b. Corp.contoso.com), und klicken Sie dann auf **OK**.
4. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Benutzers mit Berechtigungen zum Hinzufügen von Computern zur Domäne ein, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **OK**, wenn das Begrüßungsdialogfeld für die Domäne angezeigt wird.
6. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
7. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
8. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.

### **So fügen Sie Clientcomputer zur Domäne hinzu**

1. Geben Sie auf dem **Start BildschirmExplorer** **exeein**, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie mit der rechten Maustaste auf das Computersymbol und klicken Sie dann auf **Eigenschaften**.

3. Klicken Sie auf der Seite **System** auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie im Dialogfeld **Systemeigenschaften** auf der Registerkarte **Computername** auf **Ändern**.
5. Geben Sie im Feld **Computername** den Namen des Computers ein, wenn Sie beim Hinzufügen des Servers zur Domäne auch den Computernamen ändern. Klicken Sie unter **Mitglied von** auf **Domäne**, und geben Sie dann den Namen der Domäne ein, für die der Beitritt des Servers durchgeführt werden soll (z. B. corp.contoso.com), und klicken Sie dann auf **OK**.
6. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Benutzers mit Berechtigungen zum Hinzufügen von Computern zur Domäne ein, und klicken Sie dann auf **OK**.
7. Klicken Sie auf **OK**, wenn das Begrüßungsdialogfeld für die Domäne angezeigt wird.
8. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
9. Klicken Sie im Dialogfeld **System Eigenschaften** auf schließen.
10. Klicken Sie bei Aufforderung auf **Jetzt neu starten**.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

##### **NOTE**

Sie müssen Domänen Anmelde Informationen bereitstellen, nachdem Sie den folgenden Befehl eingegeben haben.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

## Konfigurieren von GPOs

Zum Bereitstellen des Remote Zugriffs benötigen Sie mindestens zwei Gruppenrichtlinie Objekte. Ein Gruppenrichtlinie Objekt enthält Einstellungen für den RAS-Server und eine enthält Einstellungen für DirectAccess-Client Computer. Wenn Sie den Remote Zugriff konfigurieren, erstellt der Assistent automatisch die erforderlichen Gruppenrichtlinie Objekte. Wenn Ihre Organisation jedoch eine Benennungs Konvention erzwingt oder Sie nicht über die erforderlichen Berechtigungen zum Erstellen oder Bearbeiten von Gruppenrichtlinie Objekten verfügen, müssen Sie vor dem Konfigurieren des Remote Zugriffs erstellt werden.

Informationen zum Erstellen von Gruppenrichtlinie Objekten finden Sie unter [Erstellen und Bearbeiten eines Gruppenrichtlinie Objekts](#).

Ein Administrator kann die DirectAccess-Gruppenrichtlinie Objekte manuell mit einer Organisationseinheit (OU) verknüpfen. Berücksichtigen Sie die folgenden Aspekte:

1. Verknüpfen Sie die erstellten Gruppenrichtlinien Objekte mit den entsprechenden Organisationseinheiten, bevor Sie DirectAccess konfigurieren.
2. Wenn Sie DirectAccess konfigurieren, sollten Sie eine Sicherheitsgruppe für die Clientcomputer angeben.
3. Die GPOs werden automatisch konfiguriert, unabhängig davon, ob der Administrator über Berechtigungen zum Verknüpfen der Gruppenrichtlinien Objekte mit der Domäne verfügt.

4. Wenn die Gruppenrichtlinien Objekte bereits mit einer Organisationseinheit verknüpft sind, werden die Verknüpfungen nicht entfernt, Sie sind jedoch nicht mit der Domäne verknüpft.
5. Für Server-Gruppenrichtlinien Objekte muss die Organisationseinheit das Server Computer Objekt enthalten. andernfalls wird das Gruppenrichtlinien Objekt mit dem Stamm der Domäne verknüpft.
6. Wenn die Organisationseinheit zuvor durch Ausführen des DirectAccess-Setup-Assistenten nicht verknüpft wurde, kann der Administrator die DirectAccess-GPOs nach Abschluss der Konfiguration mit den erforderlichen Organisationseinheiten verknüpfen und den Link zur Domäne entfernen.

Weitere Informationen finden Sie unter [Verknüpfen eines Gruppenrichtlinie Objekts](#).

#### **NOTE**

Wenn ein Gruppenrichtlinie Objekt manuell erstellt wurde, ist es möglich, dass das Gruppenrichtlinie Objekt während der DirectAccess-Konfiguration nicht verfügbar ist. Das Gruppenrichtlinie Objekt wurde möglicherweise nicht auf dem Domänen Controller repliziert, der dem Verwaltungs Computer am nächsten liegt. Der Administrator kann warten, bis die Replikation beendet ist, oder die Replikation wird erzwungen.

## Konfigurieren von Sicherheitsgruppen

Die DirectAccess-Einstellungen, die auf dem Client Computer Gruppenrichtlinie Objekt enthalten sind, werden nur auf Computer angewendet, die Mitglieder der Sicherheitsgruppe sind, die Sie beim Konfigurieren des Remote Zugriffs angeben.

### **So erstellen Sie eine Sicherheitsgruppe für DirectAccess-Clients**

1. Geben Sie auf dem **Start** BildschirmDSA. **msc**, und drücken Sie dann die **EINGABETASTE**.
2. Erweitern Sie in der Konsole **Active Directory-Benutzer und -Computers** im linken Bereich die Domäne, die die Sicherheitsgruppe enthält, klicken Sie mit der rechten Maustaste auf **Benutzer**, zeigen Sie auf **Neu** und klicken Sie dann auf **Gruppe**.
3. Geben Sie im Dialogfeld **Neues Objekt - Gruppe** unter **Gruppenname** den Namen für die Sicherheitsgruppe ein.
4. Klicken Sie unter **Gruppenbereich** auf **Global**, unter **Gruppentyp** auf **Sicherheit** und anschließend auf **OK**.
5. Doppelklicken Sie auf die Sicherheitsgruppe DirectAccess-Client Computer, und klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **Mitglieder**.
6. Auf der Registerkarte **Mitglieder** klicken Sie auf **Hinzufügen**.
7. Wählen Sie im Dialogfeld zum **Auswählen von Benutzern, Kontakten Computern oder Dienstkonten** die Clientcomputer aus, für die DirectAccess aktiviert werden soll, und klicken Sie anschließend auf **OK**.

### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

## Konfigurieren des Netzwerkadressen Servers

Der Netzwerkadressen Server sollte sich auf einem Server mit hoher Verfügbarkeit befinden, und er benötigt ein gültiges Secure Sockets Layer (SSL)-Zertifikat, das von den DirectAccess-Clients als vertrauenswürdig eingestuft wird.

**NOTE**

Wenn sich die Netzwerkadressen Server-Website auf dem RAS-Server befindet, wird beim Konfigurieren des Remote Zugriffs automatisch eine Website erstellt, die an das von Ihnen bereitgestellte Serverzertifikat gebunden ist.

Für das Netzwerkadressenserver-Zertifikat sind zwei Zertifikatoptionen verfügbar:

- **Private**

**NOTE**

Das Zertifikat basiert auf der Zertifikat Vorlage, die Sie in [Konfigurieren von Zertifikat Vorlagen](#) erstellt haben.

- **Selbst signiert**

**NOTE**

Selbstsignierte Zertifikate können nicht in Bereitstellungen für mehrere Standorte verwendet werden.

Unabhängig davon, ob Sie ein privates Zertifikat oder ein selbst signiertes Zertifikat verwenden, benötigen Sie Folgendes:

- Ein Websitezertifikat für den Netzwerkadressenserver. Der Zertifikatantragsteller sollte die URL des Netzwerkadressenservers sein.
- Ein Zertifikat Sperr Listen-Verteilungs Punkt mit hoher Verfügbarkeit im internen Netzwerk.

**So installieren Sie das Netzwerkadressenserver-Zertifikat von einer internen Zertifizierungsstelle**

1. Auf dem Server, auf dem die Netzwerkadressen Server-Website gehostet wird: Geben Sie auf dem **Start BildschirmMMC** ein, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-ins hinzufügen oder entfernen** auf **Zertifikate, Hinzufügen, Computerkonto, Weiter, Lokaler Computer, Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **alle Aufgaben**, klicken Sie auf **Neues Zertifikat anfordern**, und klicken Sie zweimal auf **weiter**.
6. Aktivieren Sie auf der Seite **Zertifikate anfordern** das Kontrollkästchen für die Zertifikat Vorlage, die Sie unter Konfigurieren von Zertifikat Vorlagen erstellt haben, und klicken Sie bei Bedarf auf **Weitere Informationen**, die für die Registrierung **dieses Zertifikats erforderlich** sind.
7. Klicken Sie im Dialogfeld **Zertifikateigenschaften** auf der Registerkarte **Antragsteller** im Bereich **Antragstellename** unter **Typ** auf **Allgemeiner Name**.
8. Geben Sie in das Feld **Wert** den FQDN der Netzwerkadressenserver-Website ein und klicken Sie dann auf **Hinzufügen**.
9. Wählen Sie unter **Alternativer Name** für **Typ** die Option **DNS** aus.

10. Geben Sie in das Feld **Wert** den FQDN der Netzwerkadressenserver-Website ein und klicken Sie dann auf **Hinzufügen**.
11. Auf der Registerkarte **Allgemein** unter **Anzeigename** können Sie einen Namen für das Zertifikat eingeben, sodass Sie es schneller identifizieren können.
12. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
13. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, ob das neue Zertifikat mit dem beabsichtigten Zweck der Server Authentifizierung registriert wurde.

#### **So konfigurieren Sie den Netzwerkadressenserver**

1. Richten Sie eine Website auf einem Server mit hoher Verfügbarkeit ein. Für die Website sind keine Inhalte erforderlich, für einen Test sollten Sie jedoch eine Standardseite definieren, die eine Meldung anzeigen, wenn Clients eine Verbindung zu der Website aufbauen.

Dieser Schritt ist nicht erforderlich, wenn die Netzwerkadressen Server-Website auf dem Remote Zugriffs Server gehostet wird.

2. Binden Sie ein HTTPS-Serverzertifikat an die Website. Der allgemeine Name des Zertifikats sollte mit dem Namen der Netzwerkadressenserver-Website übereinstimmen. Vergewissern Sie sich, dass die DirectAccess-Clients der ausstellenden Zertifizierungsstelle vertrauen.

Dieser Schritt ist nicht erforderlich, wenn die Netzwerkadressen Server-Website auf dem Remote Zugriffs Server gehostet wird.

3. Richten Sie eine CRL-Site ein, die Hochverfügbarkeit im internen Netzwerk beschleunigt.

Auf die Sperrlisten-Verteilungspunkte wurde folgendermaßen zugegriffen:

- Webserver, die eine HTTP-basierte URL verwenden, z. b.: <https://crl.corp.contoso.com/crl/corp-APP1-CA.crl>
- Dateiserver, auf die über einen UNC-Pfad (Universal Naming Convention) zugegriffen wird, z. b. \\crl.Corp.contoso.com\crl\corp-App1-ca.crl

Wenn der interne CRL-Verteilungs Punkt nur über IPv6 erreichbar ist, müssen Sie eine Verbindungs Sicherheitsregel für die Windows-Firewall mit erweiterter Sicherheit konfigurieren. Dadurch wird der IPSec-Schutz von dem IPv6-Adressraum Ihres Intranets zu den IPv6-Adressen der CRL-Verteilungs Punkte ausgenommen.

4. Stellen Sie sicher, dass DirectAccess-Clients im internen Netzwerk den Namen des Netzwerkadressen Servers auflösen können und dass DirectAccess-Clients im Internet den Namen nicht auflösen können.

## Siehe auch

- [Schritt 2: Konfigurieren des Remote Zugriffs Servers](#)

# Schritt 2 Konfigurieren des Remote Zugriffs Servers

09.04.2020 • 15 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie die Client- und Servereinstellungen konfigurieren, die für die Remote Verwaltung von DirectAccess-Clients erforderlich sind. Stellen Sie vor Beginn der Bereitstellungs Schritte sicher, dass Sie die in [Schritt 2 Planen der Remote Zugriffs Bereitstellung](#) beschriebenen Planungsschritte abgeschlossen haben.

AUFGABE	BESCHREIBUNG
Installieren der Remotezugriffsrolle	Installieren Sie die Remotezugriffsrolle.
Konfigurieren des Bereitstellungstypen	Konfigurieren Sie den Bereitstellungstypen als DirectAccess und VPN, nur DirectAccess, oder nur VPN
Konfigurieren von DirectAccess-Clients	Konfigurieren Sie den Remotezugriffsserver mit den Sicherheitsgruppen, die die DirectAccess-Clients enthalten.
Konfigurieren des Remotezugriffsservers	Konfigurieren Sie die Einstellungen des Remote Zugriffs Servers.
Konfigurieren des Infrastrukturserver	Konfigurieren Sie die Infrastrukturserver, die in der Organisation eingesetzt werden.
Konfigurieren von Anwendungsservern	Konfigurieren Sie die Anwendungsserver so, dass Authentifizierung und Verschlüsselung erforderlich sind.
Zusammenfassung der Konfiguration und alternative Gruppenrichtlinienobjekte	Zeigen Sie die Zusammenfassung der Remotezugriffskonfiguration an und ändern Sie bei Bedarf die Gruppenrichtlinienobjekte.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## Installieren der Remote Zugriffs Rolle

Sie müssen die Remote Zugriffs Rolle auf einem Server in Ihrer Organisation installieren, der als Remote Zugriffs Server fungiert.

### So installieren Sie die Remotezugriffsrolle

#### So installieren Sie die Remote Zugriffs Rolle auf DirectAccess-Servern

1. Klicken Sie auf dem DirectAccess-Server in der Server-Manager-Konsole im Dashboard auf Rollen und Features hinzufügen.
2. Klicken Sie dreimal auf Weiter , um zur Anzeige für die Serverrollenauswahl zu gelangen.

3. Wählen Sie im Dialogfeld **Server Rollen auswählen** die Option **Remote Zugriff aus**, und klicken Sie dann auf **weiter**.
4. Klicken Sie drei Mal auf **weiter**.
5. Wählen Sie im Dialogfeld **Rollen Dienste auswählen** die Option **DirectAccess und VPN (RAS)** aus, und klicken Sie dann auf **Features hinzufügen**.
6. Wählen Sie **Routing, webanwendungsproxy** aus, klicken Sie auf **Features hinzufügen** und dann auf **weiter**.
7. Klicken Sie auf **Weiter** und dann auf **Installieren**.
8. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

## Konfigurieren des Bereitstellungs Typs

Es gibt drei Optionen, die Sie zum Bereitstellen des Remote Zugriffs über die Remote Zugriffs-Verwaltungskonsole verwenden können:

- DirectAccess und VPN
- Nur DirectAccess
- Nur VPN

#### **NOTE**

In diesem Handbuch wird die einzige Methode für die Bereitstellung von DirectAccess in den Beispiel Prozeduren verwendet.

#### **So konfigurieren Sie den Bereitstellungstypen**

1. Öffnen Sie auf dem Remote Zugriffs Server die Remote Zugriffs-Verwaltungskonsole: Geben Sie auf dem **Start** Bildschirm ein, geben Sie **Remote Zugriffs-Verwaltungskonsole** ein, und drücken Sie dann die **EINGABETASTE**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remotezugriffs-Verwaltungskonsole im mittleren Bereich auf **Remotezugriffs-Setup-Assistenten ausführen**.
3. Wählen Sie im Dialogfeld **Remote Zugriff konfigurieren** die Option **DirectAccess und VPN**, nur **DirectAccess** oder nur **VPN** aus.

## Konfigurieren von DirectAccess-Clients

Damit ein Clientcomputer zur Verwendung von DirectAccess bereitgestellt werden kann, muss er zur ausgewählten Sicherheitsgruppe gehören. Nachdem DirectAccess konfiguriert wurde, werden Client Computer in der Sicherheitsgruppe bereitgestellt, um die DirectAccess-Gruppenrichtlinie Objekte (GPOs) für die Remote

Verwaltung zu empfangen.

#### So konfigurieren Sie DirectAccess-Clients

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 1 Remoteclients** auf **Konfigurieren**.
2. Klicken Sie im DirectAccess-Client-Setup-Assistenten auf der Seite **Bereitstellungs Szenario** auf **DirectAccess nur für die Remote Verwaltung** bereitstellen, und klicken Sie dann auf **weiter**.
3. Klicken Sie auf der Seite **Gruppen auswählen** auf **Hinzufügen**.
4. Wählen Sie im Dialogfeld **Gruppen auswählen** die Sicherheitsgruppen aus, die die DirectAccess-Client Computer enthalten, und klicken Sie dann auf **weiter**.
5. Vorgehensweise auf der Seite **Netzwerkkonnektivitäts-Assistent**:
  - Fügen Sie in der Tabelle die Ressourcen hinzu, die verwendet werden, um die Konnektivität zum internen Netzwerk zu ermitteln. Wenn keine weiteren Ressourcen konfiguriert werden, wird automatisch ein Standardwebtest erstellt. Stellen Sie beim Konfigurieren der webtestorte zum Ermitteln der Konnektivität mit dem Unternehmensnetzwerk sicher, dass mindestens ein HTTP-basierter Test konfiguriert ist. Das Konfigurieren eines Ping-Tests ist nicht ausreichend, und es kann zu einer ungenauen Ermittlung des Verbindungsstatus führen. Dies liegt daran, dass Ping von IPsec ausgenommen wird. Daher stellt Ping nicht sicher, dass die IPSec-Tunnel ordnungsgemäß eingerichtet werden.
  - Fügen Sie eine Helpdesk-E-Mail-Adresse hinzu, damit Benutzer Informationen absenden können, wenn bei ihnen Verbindungsprobleme auftreten.
  - Geben Sie einen Anzeigenamen für die DirectAccess-Verbindung ein.
  - Aktivieren Sie bei Bedarf das Kontrollkästchen **DirectAccess-Clients ermöglichen, die lokale Namensauflösung zu verwenden**.

#### NOTE

Wenn die lokale Namensauflösung aktiviert ist, können Benutzer, die die NCA ausführen, Namen mithilfe von DNS-Servern auflösen, die auf dem DirectAccess-Client Computer konfiguriert sind.

6. Klicken Sie auf **Fertig stellen**.

## Konfigurieren des Remote Zugriffs Servers

Zum Bereitstellen des Remote Zugriffs müssen Sie den Server, der als RAS-Server fungiert, mit den folgenden Einstellungen konfigurieren:

1. Korrigieren von Netzwerkadapters
2. Eine öffentliche URL für den Remote Zugriffs Server, mit dem Client Computer eine Verbindung herstellen können (die ConnectTo-Adresse)
3. Ein IP-HTTPS-Zertifikat mit einem Betreff, der mit der ConnectTo-Adresse übereinstimmt.
4. IPv6-Einstellungen
5. Client Computer Authentifizierung

#### So konfigurieren Sie den Remotezugriffsserver

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 2 RAS-Server** auf **Konfigurieren**.

2. Klicken Sie im Setup-Assistenten für den RAS-Server auf der Seite **Netzwerktopologie** auf die Bereitstellungstopologie, die in Ihrer Organisation verwendet wird. Geben Sie unter **Geben Sie den öffentlichen Namen oder die öffentliche IPv4-Adresse** an den öffentlichen Namen für die Bereitstellung ein (dieser Name stimmt mit dem Antragstellernamen des IP-HTTPS-Zertifikats überein, z. B. edge1.contoso.com), und klicken Sie dann auf **Weiter**.

3. Auf der Seite **Netzwerkadapter** erkennt der Assistent automatisch Folgendes:

- Netzwerkadapter für die Netzwerke in der Bereitstellung. Falls der Assistent nicht die korrekten Netzwerkadapter erkennt, wählen Sie die korrekten Adapter manuell aus.
- IP-HTTPS-Zertifikat. Dies basiert auf dem öffentlichen Namen für die Bereitstellung, die Sie im vorherigen Schritt des Assistenten festgelegt haben. Wenn der Assistent das korrekte IP-HTTPS-Zertifikat nicht erkennt, klicken Sie auf **Durchsuchen**, um das richtige Zertifikat manuell auszuwählen.

4. Klicken Sie auf **Weiter**.

5. Auf der Seite **Präfix Konfiguration** (Diese Seite ist nur sichtbar, wenn IPv6 im internen Netzwerk erkannt wird) werden vom Assistenten automatisch die IPv6-Einstellungen erkannt, die im internen Netzwerk verwendet werden. Wenn für Ihre Bereitstellung zusätzliche Präfixe erforderlich sind, konfigurieren Sie die IPv6-Präfixe für das interne Netzwerk, ein IPv6-Präfix zum Zuweisen für DirectAccess-Clientcomputer und ein IPv6-Präfix zum Zuweisen für VPN-Clientcomputer.

6. Vorgehensweise auf der Seite **Authentifizierung**:

- In Bereitstellungen für mehrere Standorte oder die zweistufige Authentifizierung müssen Sie die Computerzertifikatauthentifizierung verwenden. Aktivieren Sie das Kontrollkästchen **Computer Zertifikate verwenden**, um die Computer Zertifikat Authentifizierung zu verwenden, und wählen Sie das IPSec-Stamm Zertifikat aus.
- Damit Client Computer mit Windows 7 über DirectAccess eine Verbindung herstellen können, aktivieren Sie das Kontrollkästchen **Aktivieren von Windows 7-Client Computern zum Herstellen einer Verbindung über DirectAccess**. Für diesen Bereitstellungstypen müssen Sie ebenfalls die Computerzertifikatauthentifizierung verwenden.

7. Klicken Sie auf **Fertig stellen**.

## Konfigurieren der Infrastruktur Server

Um die Infrastruktur Server in einer Remote Zugriffs Bereitstellung zu konfigurieren, müssen Sie Folgendes konfigurieren:

- Netzwerkadressenserver
- DNS-Einstellungen, einschließlich der Suchliste für DNS-Suffixe
- Alle Verwaltungs Server, die nicht automatisch vom Remote Zugriff erkannt werden

### So konfigurieren Sie die Infrastrukturserver

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 3 Infrastrukturserver** auf **Konfigurieren**.
2. Klicken Sie im Assistenten zum Einrichten des Infrastrukturservers auf der Seite **Netzwerkadressenserver** auf die Option, die dem Speicherort des Netzwerkadressenservers in Ihrer Bereitstellung entspricht.
  - Wenn sich der Netzwerkadressen Server auf einem Remoteweb Server befindet, geben Sie die URL ein, und klicken Sie dann auf überprüfen, bevor Sie fortfahren.

- Wenn der Netzwerkadressenserver nicht auf einem Remotewebservice installiert ist, klicken Sie auf **Durchsuchen**, um das entsprechende Zertifikat zu suchen und klicken Sie dann auf **Weiter**.
3. Geben Sie auf der Seite **DNS** in der Tabelle zusätzliche namens Suffixe ein, die als NRPT-Ausnahmen (Name Resolution Policy Table) angewendet werden. Wählen Sie die entsprechende Option für die lokale Namensauflösung, und klicken Sie dann auf **Weiter**.
  4. Auf der Seite **DNS-Suffixsuchliste** erkennt der Remote Zugriffs Server automatisch Domänen Suffixe in der Bereitstellung. Verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um die Liste der Domänen Suffixe zu erstellen, die Sie verwenden möchten. Um ein neues Domänensuffix unter **Neues Suffix** hinzuzufügen, müssen Sie dass Suffix eingeben und anschließend auf **Hinzufügen** klicken. Klicken Sie auf **Weiter**.
  5. Fügen Sie auf der Seite **Verwaltung** Verwaltungs Server hinzu, die nicht automatisch erkannt werden, und klicken Sie dann auf **weiter**. Der Remote Zugriff fügt automatisch Domänen Controller und Configuration Manager Server hinzu.
  6. Klicken Sie auf **Fertig stellen**.

## Anwendungsserver konfigurieren

Bei einer vollständigen Remote Zugriffs Bereitstellung ist das Konfigurieren von Anwendungsservern eine optionale Aufgabe. In diesem Szenario für die Remote Verwaltung von DirectAccess-Clients werden Anwendungsserver nicht verwendet, und dieser Schritt ist ausgegraut, um anzugeben, dass er nicht aktiv ist. Klicken Sie auf **Fertig stellen**, um die Konfiguration anzuwenden.

## Konfigurations Zusammenfassung und Alternative GPOs

Wenn die Konfiguration des Remotezugriffs abgeschlossen ist, wird das Dialogfeld **Überprüfung des Remotezugriffs** angezeigt. Sie können alle zuvor ausgewählten Einstellungen überprüfen, dazu gehören:

- **GPO-Einstellungen**

Der Name des Gruppenrichtlinien Objekts für den DirectAccess-Server und der Name des Gruppenrichtlinien Objekts sind aufgeführt. Sie können auf den Link **ändern** neben der Überschrift **GPO-Einstellungen** klicken, um die GPO-Einstellungen zu ändern.

- **Remote Clients**

Die DirectAccess-Client Konfiguration wird angezeigt, einschließlich der Sicherheitsgruppe, der Verbindungs Prüfer und des DirectAccess-Verbindungs namens.

- **RAS-Server**

Die DirectAccess-Konfiguration wird angezeigt, einschließlich des öffentlichen Namens und der Adresse, der Netzwerkadapter Konfiguration und der Zertifikat Informationen.

- **Infrastruktur Server**

Diese Liste enthält die Netzwerkadressenserver-URL, DNS-Suffixe, die von DirectAccess-Clients verwendet werden sowie Verwaltungsserverinformationen.

## Siehe auch

- [Schritt 3: Überprüfen der Bereitstellung](#)

# Virtual Private Networking (VPN)

09.04.2020 • 4 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows 10

## RAS-Gateway als einzelner Mandanten-VPN-Server

In Windows Server 2016 ist die Remote Zugriffs-Server Rolle eine logische Gruppierung der folgenden verwandten Netzwerk Zugriffs Technologien.

- RAS-Dienst (RAS)
- Routing
- Webanwendungsproxy

Diese Technologien sind die Rollen Dienste der Remote Zugriffs-Server Rolle.

Wenn Sie die Remote Zugriffs-Server Rolle mit dem Assistenten zum Hinzufügen von Rollen und Features oder mit Windows PowerShell installieren, können Sie einen oder mehrere dieser drei Rollen Dienste installieren.

Wenn Sie den **DirectAccess-und VPN-Rollen Dienst (RAS)** installieren, stellen Sie das **RAS-Gateway** bereit. Sie können das RAS-Gateway als ein virtuelles privates Netzwerk (VPN) mit einem Mandanten RAS-Gateway bereitstellen, das viele erweiterte Features und erweiterte Funktionen bereitstellt.

### NOTE

Sie können das RAS-Gateway auch als mehr Instanzen fähigen VPN-Server für die Verwendung mit Software-Defined Networking (SDN) oder als DirectAccess-Server bereitstellen. Weitere Informationen finden Sie unter [RAS-Gateway](#), [Software-Defined Networking \(SDN\)](#) und [DirectAccess](#).

## Verwandte Themen

- [Always on von VPN-Features und-Funktionen](#): in diesem Thema erfahren Sie mehr über die Features und Funktionen von Always on VPN.
- [Konfigurieren von VPN-Geräte Tunneln in Windows 10](#): Always on-VPN bietet Ihnen die Möglichkeit, ein dediziertes VPN-Profil für das Gerät oder den Computer zu erstellen. Always on-VPN-Verbindungen umfassen zwei Arten von Tunneln: *Geräte Tunnel* und *Benutzer Tunnel*. Der Geräte Tunnel wird für Konnektivitätsszenarien vor der Anmeldung und für Geräteverwaltung verwendet. Der Benutzer Tunnel ermöglicht Benutzern den Zugriff auf Organisations Ressourcen über VPN-Server.
- [Always on-VPN-Bereitstellung für Windows Server 2016 und Windows 10](#): enthält Anweisungen zum Bereitstellen des Remote Zugriffs als ein einzelnes Mandanten-VPN-RAS-Gateway für Punkt-zu-Standort-VPN-Verbindungen, mit denen Ihre Remote Mitarbeiter mit Always on VPN-Verbindungen eine Verbindung mit Ihrem Unternehmensnetzwerk herstellen können. Es wird empfohlen, dass Sie die Entwurfs- und Bereitstellungs Handbücher für jede der in dieser Bereitstellung verwendeten Technologien überprüfen.
- [Technische Anleitung zu Windows 10-VPN](#): erläutert die Entscheidungen, die Sie für Windows 10-Clients in Ihrer Enterprise-VPN-Lösung treffen werden, und wie Sie die Bereitstellung konfigurieren. Verweise auf den VPnv2-Konfigurations Dienstanbieter (CSP) finden Sie unter Konfigurations Anweisungen für die Verwaltung mobiler Geräte (Mobile Device Management, MDM) mithilfe von Microsoft InTune und der VPN-Profil Vorlage für Windows 10.

- [Erstellen von VPN-Profilen in Configuration Manager](#): in diesem Thema erfahren Sie, wie Sie in Configuration Manager VPN-Profile erstellen.
- [Konfigurieren von Windows 10-Client Always on-VPN-Verbindungen](#): in diesem Thema werden die profileXML-Optionen und das-Schema beschrieben und das profileXML-VPN erstellt. Nachdem Sie die Serverinfrastruktur eingerichtet haben, müssen Sie die Windows 10-Client Computer für die Kommunikation mit dieser Infrastruktur über eine VPN-Verbindung konfigurieren.
- [VPN-Profil Optionen](#): in diesem Thema werden die VPN-Profileinstellungen in Windows 10 beschrieben und erfahren, wie Sie VPN-Profile mithilfe von InTune oder Configuration Manager konfigurieren. Sie können alle VPN-Einstellungen in Windows 10 konfigurieren, indem Sie den profileXML-Knoten im VPnv2-CSP verwenden.

# Konfigurieren von VPN-Geräte Tunneln in Windows 10

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows 10, Version 1709

Always on-VPN bietet Ihnen die Möglichkeit, ein dediziertes VPN-Profil für das Gerät oder den Computer zu erstellen. Always on-VPN-Verbindungen umfassen zwei Arten von Tunnels:

- Der *Geräte Tunnel* stellt eine Verbindung mit angegebenen VPN-Servern her, bevor sich Benutzer am Gerät anmelden. Konnektivitätsszenarios und Geräte Verwaltungsaufgaben vor der Anmeldung verwenden den Geräte Tunnel.
- Der *Benutzer Tunnel* stellt nur dann eine Verbindung her, nachdem sich ein Benutzer am Gerät angemeldet hat. Der Benutzer Tunnel ermöglicht Benutzern den Zugriff auf Organisations Ressourcen über VPN-Server.

Anders als bei einem *Benutzer Tunnel*, der nur eine Verbindung herstellt, nachdem sich ein Benutzer am Gerät oder Computer anmeldet, ermöglicht der *Geräte Tunnel* dem VPN das Herstellen von Verbindungen, bevor sich der Benutzer anmeldet. Sowohl *Geräte Tunnel* als auch *Benutzer Tunnel* arbeiten unabhängig von Ihren VPN-Profilen, können gleichzeitig verbunden werden und können gegebenenfalls verschiedene Authentifizierungsmethoden und andere VPN-Konfigurationseinstellungen verwenden. Der Benutzer Tunnel unterstützt SSTP und IKEv2, und der Geräte Tunnel unterstützt IKEv2 nur ohne Unterstützung für das SSTP-Fallback.

Der Benutzer Tunnel wird auf in die Domäne eingebundenen, nicht in die Domäne eingebundenen (Arbeitsgruppen) oder Azure AD Geräte unterstützt, die für Unternehmens- und BYOD-Szenarien geeignet sind. Es ist in allen Windows-Editionen verfügbar, und die Plattformfunktionen stehen Drittanbietern mithilfe von UWP-VPN-Plug-in-Unterstützung zur Verfügung.

Der Geräte Tunnel kann nur auf in die Domäne eingebundenen Geräten konfiguriert werden, auf denen Windows 10 Enterprise oder Education Version 1709 oder höher ausgeführt wird. Die Kontrolle des Geräte Tunnels durch Drittanbieter wird nicht unterstützt.

## Anforderungen und Features für den Geräte Tunnel

Sie müssen die Computer Zertifikat Authentifizierung für VPN-Verbindungen aktivieren und eine Stamm Zertifizierungsstelle für die Authentifizierung eingehender VPN-Verbindungen definieren.

```
$VPNRootCertAuthority = "Common Name of trusted root certification authority"
$RootCACert = (Get-ChildItem -Path cert:LocalMachine\root | Where-Object {$_.Subject -Like
"**$VPNRootCertAuthority**" })
Set-VpnAuthProtocol -UserAuthProtocolAccepted Certificate, EAP -RootCertificateNameToAccept $RootCACert -
PassThru
```

FEATURES	REQUIREMENTS
<ul style="list-style-type: none"> <li>• Always connected (as long as there is network connectivity and the computer is not in a low power state)</li> <li>• Connects to your organization VPN servers before user logon</li> <li>• Can coexist with one active user tunnel</li> <li>• Transparent to the user</li> </ul>	<ul style="list-style-type: none"> <li>• The device must be a domain joined computer running Windows 10 Enterprise or Education version 1709 or later.</li> <li>• The tunnel is only configurable for the Windows built-in VPN solution and is established using IKEv2 with computer certificate authentication.</li> <li>• Only one device tunnel can be configured per device.</li> </ul>

## Konfiguration des VPN-Geräte Tunnels

Die Beispiel-XML-Datei unten bietet eine gute Anleitung für Szenarien, in denen nur vom Client initiierte Pull-Vorgänge über den Geräte Tunnel erforderlich sind. Datenverkehrs Filter werden genutzt, um den Geräte Tunnel nur auf den Verwaltungs Datenverkehr zu beschränken. Diese Konfiguration eignet sich gut für Windows Update, typische Gruppenrichtlinie (GP) und Microsoft Endpoint Configuration Manager Update Szenarios sowie VPN-Konnektivität für die erste Anmeldung ohne zwischengespeicherte Anmelde Informationen oder Szenarios zur Kenn Wort Zurücksetzung.

Für Server initiierte pushfälle, wie Windows-Remoteverwaltung (WinRM), Remote-gpupdate und Remote Configuration Manager Update Szenarios – Sie müssen eingehenden Datenverkehr für den Geräte Tunnel zulassen, sodass keine Datenverkehrs Filter verwendet werden können. Wenn Sie im Geräte Tunnel Profildaten Verkehrs Filter aktivieren, wird der eingehende Datenverkehr vom Geräte Tunnel verweigert. Diese Einschränkung wird in zukünftigen Versionen entfernt.

### **Beispiel-VPN-profileXML**

Im folgenden finden Sie ein Beispiel für die VPN-Profilerstellung.

```

<VPNProfile>
  <NativeProfile>
    <Servers>vpn.contoso.com</Servers>
    <NativeProtocolType>IKEv2</NativeProtocolType>
    <Authentication>
      <MachineMethod>Certificate</MachineMethod>
    </Authentication>
    <RoutingPolicyType>SplitTunnel</RoutingPolicyType>
      <!-- disable the addition of a class based route for the assigned IP address on the VPN interface -->
    <DisableClassBasedDefaultRoute>true</DisableClassBasedDefaultRoute>
  </NativeProfile>
  <!-- use host routes(/32) to prevent routing conflicts -->
  <Route>
    <Address>10.10.0.2</Address>
    <PrefixSize>32</PrefixSize>
    </Route>
    <Route>
      <Address>10.10.0.3</Address>
      <PrefixSize>32</PrefixSize>
      </Route>
      <!-- traffic filters for the routes specified above so that only this traffic can go over the device tunnel -->
    <TrafficFilter>
      <RemoteAddressRanges>10.10.0.2, 10.10.0.3</RemoteAddressRanges>
    </TrafficFilter>
    <!-- need to specify always on = true -->
    <AlwaysOn>true</AlwaysOn>
    <!-- new node to specify that this is a device tunnel -->
    <DeviceTunnel>true</DeviceTunnel>
    <!--new node to register client IP address in DNS to enable manage out -->
    <RegisterDNS>true</RegisterDNS>
  </Route>
</VPNProfile>

```

Abhängig von den Anforderungen der einzelnen Bereitstellungs Szenarios ist ein weiteres VPN-Feature, das mit dem Geräte Tunnel konfiguriert werden kann, die [Erkennung vertrauenswürdiger Netzwerke](#).

```

<!-- inside/outside detection -->
<TrustedNetworkDetection>corp.contoso.com</TrustedNetworkDetection>

```

## Bereitstellung und Tests

Sie können Geräte Tunnel mithilfe eines Windows PowerShell-Skripts und mithilfe der Windows-Verwaltungsinstrumentation (WMI)-Bridge konfigurieren. Der Always on VPN-Geräte Tunnel muss im Kontext des **lokalen System** Kontos konfiguriert werden. Um dies zu erreichen, muss [PsExec](#) verwendet werden, eines der in der [Sysinternals](#) -Dienstprogramme enthaltenen [phocker](#) .

Richtlinien für die Bereitstellung einer pro-Gerät- `(.\Device)` im Vergleich zu einer pro-Benutzer- `(.\User)` Profil finden Sie unter [Verwenden von PowerShell-Skripts mit dem WMI-Bridge Anbieter](#).

Führen Sie den folgenden Windows PowerShell-Befehl aus, um zu überprüfen, ob ein Geräte Profil erfolgreich bereitgestellt wurde:

```
Get-VpnConnection -AllUserConnection
```

In der Ausgabe wird eine Liste der Geräte-Wide VPN-Profile angezeigt, die auf dem Gerät bereitgestellt werden.

### Windows PowerShell-Beispielskript

Sie können das folgende Windows PowerShell-Skript verwenden, um ein eigenes Skript für die Profilerstellung zu

erstellen.

```
Param(
    [string]$xmlFilePath,
    [string]$ProfileName
)

$a = Test-Path $xmlFilePath
echo $a

$ProfileXML = Get-Content $xmlFilePath

echo $XML

$ProfileNameEscaped = $ProfileName -replace ' ', '%20'

$Version = 201606090004

$ProfileXML = $ProfileXML -replace '<', '&lt;'
$ProfileXML = $ProfileXML -replace '>', '&gt;'
$ProfileXML = $ProfileXML -replace '"', '&quot;'

$nodeCSPURI = './Vendor/MSFT/VPNv2'
$namespaceName = "root\cimv2\mdm\dmmap"
$className = "MDM_VPNv2_01"

$session = New-CimSession

try
{
    $newInstance = New-Object Microsoft.Management.Infrastructure.CimInstance $className, $namespaceName
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ParentID", "$nodeCSPURI", 'String', 'Key')
    $newInstance.CimInstanceProperties.Add($property)
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("InstanceID", "$ProfileNameEscaped", 'String', 'Key')
    $newInstance.CimInstanceProperties.Add($property)
    $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ProfileXML", "$ProfileXML", 'String', 'Property')
    $newInstance.CimInstanceProperties.Add($property)

    $session.CreateInstance($namespaceName, $newInstance)
    $Message = "Created $ProfileName profile."
    Write-Host "$Message"
}
catch [Exception]
{
    $Message = "Unable to create $ProfileName profile: $_"
    Write-Host "$Message"
    exit
}
$Message = "Complete."
Write-Host "$Message"
```

## Zusätzliche Ressourcen

Im folgenden finden Sie weitere Ressourcen zur Unterstützung Ihrer VPN-Bereitstellung.

### VPN-Client Konfigurations Ressourcen

Im folgenden finden Sie VPN-Client Konfigurations Ressourcen.

- [Erstellen von VPN-Profilen in Configuration Manager](#)
- [Konfigurieren von Windows 10-Client Always on-VPN-Verbindungen](#)
- [VPN-Profil Optionen](#)

## Remote Zugriffs-Server Gateway-Ressourcen

Im folgenden finden Sie RAS-gatewayressourcen (Remote Access Server).

- Konfigurieren von RRAS mit einem Computer Authentifizierungszertifikat
- Problembehandlung IKEv2 VPN-Verbindungen
- Konfigurieren des IKEv2-basierten Remote Zugriffs

### IMPORTANT

Wenn Sie den Geräte Tunnel mit einem Microsoft RAS-Gateway verwenden, müssen Sie den RRAS-Server für die Unterstützung der IKEv2-Computer Zertifikat Authentifizierung konfigurieren, indem Sie die Authentifizierungsmethode "Computer Zertifikat Authentifizierung für IKEv2 zulassen" aktivieren, wie [hier](#)beschrieben. Wenn diese Einstellung aktiviert ist, wird dringend empfohlen, dass das PowerShell-Cmdlet `Set-vpnauthprotocol` zusammen mit dem optionalen Parameter `rootcertifikatenametoaccept` verwendet wird, um sicherzustellen, dass RRAS-IKEv2-Verbindungen nur für VPN-Client Zertifikate zulässig sind, die mit einer explizit definierten internen/privaten Stamm Zertifizierungsstelle verkettet sind. Alternativ dazu sollte der Speicher für **Vertrauenswürdige Stamm Zertifizierungsstellen** auf dem RRAS-Server geändert werden, um sicherzustellen, dass er keine öffentlichen Zertifizierungsstellen enthält, wie [hier](#)erläutert. Ähnliche Methoden müssen möglicherweise auch für andere VPN-Gateways in Erwägung gezogen werden.

# DirectAccess

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema finden Sie eine kurze Übersicht über DirectAccess, einschließlich Server- und Client-Betriebssystemen, die DirectAccess unterstützen, sowie Links zu weiteren DirectAccess-Dokumentationen für Windows Server 2016.

## NOTE

Zusätzlich zu diesem Thema ist die folgende DirectAccess-Dokumentation verfügbar.

- [DirectAccess-Bereitstellungs Pfade in Windows Server](#)
- [Erforderliche Komponenten für die Bereitstellung von DirectAccess](#)
- [DirectAccess: Nicht unterstützte Konfigurationen](#)
- [DirectAccess-Testumgebung: Leitfäden](#)
- [DirectAccess: Bekannte Probleme](#)
- [DirectAccess-Kapazitätsplanung](#)
- [DirectAccess-Offline-Domänen Beitritt](#)
- [Problembehandlung von DirectAccess](#)
- [Bereitstellen eines einzelnen DirectAccess-Servers mit dem Assistenten für die ersten Schritte](#)
- [Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#)
- [Hinzufügen von DirectAccess zu einer vorhandenen Remotezugriffsbereitstellung \(VPN\)](#)

DirectAccess ermöglicht Remote Benutzern die Konnektivität von Netzwerkressourcen, ohne herkömmliche VPN-Verbindungen (virtuelles privates Netzwerk) zu benötigen. Bei DirectAccess-Verbindungen sind Remote Client Computer immer mit Ihrer Organisation verbunden. Remote Benutzer müssen keine Verbindungen starten und Abbrechen, wie dies bei VPN-Verbindungen erforderlich ist. Außerdem können Ihre IT-Administratoren DirectAccess-Client Computer verwalten, wenn Sie ausgeführt werden und eine Internet Verbindung besteht.

## IMPORTANT

Versuchen Sie nicht, den Remote Zugriff auf einem virtuellen Computer (VM-) in Microsoft Azure bereitzustellen. Die Verwendung des Remote Zugriffs in Microsoft Azure wird nicht unterstützt. Sie können den Remote Zugriff auf einem virtuellen Azure-Computer nicht verwenden, um VPN, DirectAccess oder andere Remote Zugriffs Funktionen in Windows Server 2016 oder früheren Versionen von Windows Server bereitzustellen. Weitere Informationen finden Sie [unter Microsoft Server Software Support for Microsoft Azure Virtual Machines](#).

DirectAccess bietet Unterstützung nur für in die Domäne eingebundenen Clients, die die Betriebssystemunterstützung für DirectAccess einschließen.

DirectAccess wird von den folgenden Server Betriebssystemen unterstützt.

- Sie können alle Versionen von Windows Server 2016 als DirectAccess-Client oder DirectAccess-Server bereitstellen.
- Sie können alle Versionen von Windows Server 2012 R2 als DirectAccess-Client oder DirectAccess-Server bereitstellen.

- Sie können alle Versionen von Windows Server 2012 als DirectAccess-Client oder DirectAccess-Server bereitstellen.
- Sie können alle Versionen von Windows Server 2008 R2 als DirectAccess-Client oder DirectAccess-Server bereitstellen.

DirectAccess wird von den folgenden Client Betriebssystemen unterstützt.

- Windows 10 Enterprise
- Windows 10 Enterprise 2015 Long Term Servicing Branch (ltенb)
- Windows 8 und 8,1 Enterprise
- Windows 7 Ultimate
- Windows 7 Enterprise

# DirectAccess-Bereitstellungspfade in Windows Server

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema enthält eine Liste der Dokumentation für die beiden Haupt Bereitstellungs Pfade für den Remote Zugriff: " **Basic** " und " **Advanced** ".

Im folgenden Abschnitt finden Sie Informationen zu den Unterschieden zwischen den grundlegenden und erweiterten Bereitstellungs Pfaden von DirectAccess. Sie können auch die Dokumentations Links verwenden, um das Bereitstellungs Handbuch zu finden, das für Ihre Ziele am besten geeignet ist.

## Grundlegende DirectAccess-Bereitstellung

Bei einer einfachen DirectAccess-Bereitstellung wird DirectAccess mithilfe eines Assistenten mit den Standardeinstellungen konfiguriert, ohne dass Infrastruktur Einstellungen wie eine Zertifizierungsstelle oder Active Directory Sicherheitsgruppen konfiguriert werden müssen.

- Stellen [Sie mithilfe des Assistenten für die ersten Schritte einen einzelnen DirectAccess-Server](#) bereit. Sie können dieses Handbuch verwenden, um grundlegende DirectAccess-bereit Stellungen in einer Produktionsumgebung bereitzustellen.

## Bereitstellen von Advanced DirectAccess

Bei einer erweiterten DirectAccess-Bereitstellung stellen Sie einen einzelnen DirectAccess-Server bereit und konfigurieren Netzwerkinfrastruktur Server für die Unterstützung von DirectAccess.

- Stellen Sie [einen einzelnen DirectAccess-Server mit erweiterten Einstellungen](#) bereit. Mithilfe dieses Handbuchs können Sie DirectAccess mit erweiterten Einstellungen in einer Produktionsumgebung bereitstellen.

# Erforderliche Komponenten für die Bereitstellung von DirectAccess

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In der folgenden Tabelle sind die Voraussetzungen für die Verwendung der Konfigurations-Assistenten für die Bereitstellung von DirectAccess aufgeführt.

Szenario	Erforderliche Komponenten
<a href="#">Bereitstellen eines einzelnen DirectAccess-Servers mit dem Assistenten für die ersten Schritte</a>	<ul style="list-style-type: none"><li>-Die Windows-Firewall muss in allen Profilen aktiviert sein.</li><li>-Nur für Clients unterstützt, auf denen Windows 10® ausgeführt wird.</li><li>Windows® 8 und Windows® 8,1 Enterprise.</li><li>-Eine Public Key-Infrastruktur ist nicht erforderlich.</li><li>-Wird für die Bereitstellung der zweistufigen Authentifizierung nicht unterstützt. Für die Authentifizierung sind Domänenanmeldeinformationen erforderlich.</li><li>-Stellt DirectAccess automatisch für alle mobilen Computer in der aktuellen Domäne bereit.</li><li>-Der Datenverkehr an das Internet erfolgt nicht über DirectAccess. Die Konfiguration einer Tunnelerzwingung wird nicht unterstützt.</li><li>-Der DirectAccess-Server ist der Netzwerkadressen Server.</li><li>-Netzwerk Zugriffsschutz (Network Access Protection, NAP) wird nicht unterstützt.</li><li>Das Ändern von Richtlinien mithilfe einer anderen Funktion als der DirectAccess-Verwaltungskonsole oder Windows PowerShell-Cmdlets wird nicht unterstützt.</li><li>-Verwenden Sie für eine Konfiguration mit mehreren Standorten (jetzt oder in der Zukunft) zuerst die Anleitung unter <a href="#">Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen</a>.</li></ul>

## Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen

-Eine Public Key-Infrastruktur muss bereitgestellt werden.  
Weitere Informationen finden Sie unter [Test Umgebungs Anleitung Mini-Module: Basic PKI for Windows Server 2012](#).

-Die Windows-Firewall muss in allen Profilen aktiviert sein.

DirectAccess wird von den folgenden Server Betriebssystemen unterstützt.

-Sie können alle Versionen von Windows Server 2016 als DirectAccess-Client oder DirectAccess-Server bereitstellen.

-Sie können alle Versionen von Windows Server 2012 R2 als DirectAccess-Client oder DirectAccess-Server bereitstellen.

-Sie können alle Versionen von Windows Server 2012 als DirectAccess-Client oder DirectAccess-Server bereitstellen.

-Sie können alle Versionen von Windows Server 2008 R2 als DirectAccess-Client oder DirectAccess-Server bereitstellen.

DirectAccess wird von den folgenden Client Betriebssystemen unterstützt.

-Windows 10® Enterprise

-Windows 10® Enterprise 2015 Long Term Servicing Branch (ltionb)

-Windows® 8 und 8,1 Enterprise

-Windows® 7 Ultimate

-Windows® 7 Enterprise

-Tunnel Konfiguration erzwingen wird bei der kerbproxy-Authentifizierung nicht unterstützt.

Das Ändern von Richtlinien mithilfe einer anderen Funktion als der DirectAccess-Verwaltungskonsole oder Windows PowerShell-Cmdlets wird nicht unterstützt.

-Das Trennen von NAT64/DNS64-und IPHTTPS-Server Rollen auf einem anderen Server wird nicht unterstützt.

# DirectAccess nicht unterstützte Konfigurationen

27.03.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Überprüfen Sie die folgende Liste mit nicht unterstützten DirectAccess-Konfigurationen, bevor Sie mit der Bereitstellung beginnen, damit Sie die Bereitstellung nicht erneut starten müssen.

## Verteilung des Datei Replikations Dienstanbieter (FRS) von Gruppenrichtlinie Objekten (SYSVOL-Replikationen)

Stellen Sie DirectAccess nicht in Umgebungen bereit, in denen die Domänen Controller den Datei Replikations Dienst (File Replication Service, FRS) für die Verteilung von Gruppenrichtlinie Objekten (SYSVOL-Replikationen) ausführen. Die Bereitstellung von DirectAccess wird bei Verwendung von FRS nicht unterstützt.

Sie verwenden FRS, wenn Sie über Domänen Controller verfügen, auf denen Windows Server 2003 oder Windows Server 2003 R2 ausgeführt wird. Außerdem können Sie FRS verwenden, wenn Sie zuvor Windows 2000 Server oder Windows Server 2003-Domänen Controller verwendet haben und nie die SYSVOL-Replikation von FRS zu verteiltes Dateisystem Replikation (DFS-R) migriert haben.

Wenn Sie DirectAccess mit der FRS-SYSVOL-Replikation bereitstellen, riskieren Sie das unbeabsichtigte Löschen von DirectAccess-Gruppenrichtlinie Objekten, die den DirectAccess-Server und die Client Konfigurationsinformationen enthalten. Wenn diese Objekte gelöscht werden, kommt es bei der DirectAccess-Bereitstellung zu einem Ausfall, und Client Computer, die DirectAccess verwenden, sind nicht in der Lage, eine Verbindung mit Ihrem Netzwerk herzustellen.

Wenn Sie DirectAccess bereitstellen möchten, müssen Sie Domänen Controller verwenden, auf denen Betriebssysteme als Windows Server 2003 R2 ausgeführt werden, und Sie müssen DFS-R verwenden.

Informationen zum Migrieren von FRS zu DFS-R finden Sie unter [SYSVOL Replication Migration Guide: FRS to DFS-Replikation](#).

## Netzwerk Zugriffsschutz für DirectAccess-Clients

Der Netzwerk Zugriffsschutz (Network Access Protection, NAP) wird verwendet, um zu bestimmen, ob Remote Client Computer IT-Richtlinien erfüllen, bevor Sie Zugriff auf das Unternehmensnetzwerk erhalten. NAP wurde in Windows Server 2012 R2 als veraltet markiert und ist nicht in Windows Server 2016 enthalten. Aus diesem Grund wird das Starten einer neuen Bereitstellung von DirectAccess mit NAP nicht empfohlen. Es wird empfohlen, die Sicherheit von DirectAccess-Clients mit einer anderen Methode zu bestimmen.

## Unterstützung für mehrere Standorte für Windows 7-Clients

Wenn DirectAccess in einer Bereitstellung für mehrere Standorte konfiguriert ist, können Windows 10®, Windows 8,1 und Windows 8-Clients eine Verbindung mit dem nächstgelegenen Standort herstellen. Windows 7-® Client Computer verfügen nicht über die gleiche Funktion. Die Standort Auswahl für Windows 7-Clients wird zum Zeitpunkt der Richtlinien Konfiguration auf einen bestimmten Standort festgelegt, und diese Clients stellen unabhängig von Ihrem Standort stets eine Verbindung mit dem angegebenen Standort her.

## Benutzerbasierte Zugriffs Steuerung

DirectAccess-Richtlinien sind computerbasiert, Nichtbenutzer basiert. Das Angeben von DirectAccess-Benutzerrichtlinien zum Steuern des Zugriffs auf das Unternehmensnetzwerk wird nicht unterstützt.

## Anpassen der DirectAccess-Richtlinie

DirectAccess kann mit dem DirectAccess-Setup-Assistenten, der Remote Zugriffs-Verwaltungskonsole oder den Windows PowerShell-Cmdlets für den Remote Zugriff konfiguriert werden. Die Verwendung einer anderen Methode als dem DirectAccess-Setup-Assistenten zum Konfigurieren von DirectAccess, wie z. B. das direkte Ändern von DirectAccess-Gruppenrichtlinie Objekten oder das manuelle Ändern der Standardrichtlinien Einstellungen auf dem Server oder Client, wird nicht unterstützt. Diese Änderungen können zu einer nicht verwendbaren Konfiguration führen.

## Kerbproxy-Authentifizierung

Wenn Sie einen DirectAccess-Server mit dem Assistenten für die ersten Schritte konfigurieren, wird der DirectAccess-Server automatisch für die Verwendung der kerbproxy-Authentifizierung für die Computer- und Benutzerauthentifizierung konfiguriert. Aus diesem Grund sollten Sie den Assistenten für die ersten Schritte nur für bereit Stellungen mit einem Standort verwenden, bei denen nur Windows 10-®, Windows 8.1 oder Windows 8-Clients bereitgestellt werden.

Außerdem sollten die folgenden Funktionen nicht mit der kerbproxy-Authentifizierung verwendet werden:

- Lastenausgleich mit einem externen Load Balancer oder Windows Load Ausgleichsmodul
- Zweistufige Authentifizierung, bei der Smartcards oder ein einmal Kennwort (OTP) erforderlich sind

Die folgenden Bereitstellungs Pläne werden nicht unterstützt, wenn Sie die kerbproxy-Authentifizierung aktivieren:

- Multisite.
- DirectAccess-Unterstützung für Windows 7-Clients.
- Tunnel Erzwingung. Konfigurieren Sie beim Ausführen des Assistenten die folgenden Elemente, um sicherzustellen, dass die kerbproxy-Authentifizierung bei Verwendung von Tunnel Erzwingung nicht aktiviert ist:
  - Aktivieren des Erzwingens von Tunneln
  - Aktivieren von DirectAccess für Windows 7-Clients

### NOTE

Für die vorherigen bereit Stellungen sollten Sie den Assistenten für die erweiterte Konfiguration verwenden, der eine zweitunnel-Konfiguration mit einem Zertifikat basierten Computer und einer Benutzerauthentifizierung verwendet. Weitere Informationen finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).

## Verwenden von ISATAP

ISATAP ist eine Übergangstechnologie, die IPv6-Konnektivität in reinen IPv4-Unternehmensnetzwerken bereitstellt. Er ist auf kleine und mittelgroße Unternehmen mit einer einzelnen DirectAccess-Server Bereitstellung beschränkt und ermöglicht die Remote Verwaltung von DirectAccess-Clients. Wenn ISATAP eine Umgebung mit mehreren Standorten, Lastenausgleich oder mehreren Domänen bereitstellt, müssen Sie sie entfernen oder in eine systemeigene IPv6-Bereitstellung verschieben, bevor Sie DirectAccess konfigurieren.

## Endpunkt Konfiguration für IPHTTPS und einmal Kennwort (One-time

## password, OTP)

Wenn Sie IPHTTPS verwenden, muss die IPHTTPS-Verbindung auf dem DirectAccess-Server und nicht auf einem anderen Gerät (z. B. einem Load Balancer) beendet werden. Entsprechend muss die während der einmal Kennwort-Authentifizierung (PP) erstellte out-of-Band-Secure Sockets Layer (SSL)-Verbindung auf dem DirectAccess-Server beendet werden. Alle Geräte zwischen den Endpunkten dieser Verbindungen müssen im Pass-Through-Modus konfiguriert werden.

## Tunnel mit OTP-Authentifizierung erzwingen

Stellen Sie keinen DirectAccess-Server mit zweistufiger Authentifizierung mit OTP bereit, und erzwingen Sie Tunnelung, weil die OTP-Authentifizierung fehlschlägt. Zwischen dem DirectAccess-Server und dem DirectAccess-Client ist eine Out-of-Band-Secure Sockets Layer (SSL)-Verbindung erforderlich. Diese Verbindung erfordert eine Ausnahme, um den Datenverkehr außerhalb des DirectAccess-Tunnels zu senden. In einer Tunnel Erzwingungs Konfiguration muss sämtlicher Datenverkehr über einen DirectAccess-Tunnel geleitet werden, und nach der Tunnel Erstellung ist keine Ausnahme zulässig. Aus diesem Grund wird die OTP-Authentifizierung in einer erzwungenen Tunnel Konfiguration nicht unterstützt.

## Bereitstellen von DirectAccess mit einem schreibgeschützten Domänen Controller

DirectAccess-Server benötigen Zugriff auf einen Domänen Controller mit Lese-/Schreibzugriff und funktionieren nicht ordnungsgemäß mit einem schreibgeschützten Domänen Controller (Read-Only Domain Controller, RODC).

Ein Domänen Controller mit Lese-/Schreibzugriff ist aus vielen Gründen erforderlich, einschließlich der folgenden:

- Auf dem DirectAccess-Server ist ein Domänen Controller mit Lese-/Schreibzugriff erforderlich, um die Microsoft Management Console (MMC) für den Remote Zugriff zu öffnen.
- Der DirectAccess-Server muss sowohl den DirectAccess-Client als auch den DirectAccess-Server Gruppenrichtlinie Objekte (GPOs) lesen und schreiben.
- Der DirectAccess-Server liest und schreibt das Client-Gruppenrichtlinien Objekt speziell aus dem primären Domänen Controller Emulator (PDCE).

Stellen Sie DirectAccess aufgrund dieser Anforderungen nicht mit einem RODC bereit.

# DirectAccess-Test Lab-Handbücher

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Im folgenden finden Sie Links zu den Test Umgebungs Anleitungen für DirectAccess in Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012.

- [Test Umgebungs Anleitung: veranschaulichen von DirectAccess in einem Cluster mit Windows NLB](#)
- [Test Umgebungs Anleitung: veranschaulichen einer DirectAccess-Bereitstellung mit mehreren Standorten](#)
- [Test Umgebungs Anleitung: veranschaulichen von DirectAccess mit OTP-Authentifizierung und RSA SecurID](#)

# Testumgebungsanleitung: Vorführung von DirectAccess in einem Cluster mit Windows-Netzwerklastenausgleich

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der Remote Zugriff ist eine Server Rolle in den Betriebssystemen Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012, die Remote Benutzern den sicheren Zugriff auf interne Netzwerkressourcen über DirectAccess oder RRAS-VPN ermöglicht. Diese Anleitung enthält schrittweise Anweisungen zum Erweitern der [Testumgebungsanleitung zum Veranschaulichen von DirectAccess Single Server-Setup mit gemischten IPv4 und IPv6.](#), die den Netzwerklastenausgleich und die Clusterkonfiguration für DirectAccess veranschaulicht.

## Informationen zur Anleitung

Diese Anleitung enthält Anweisungen zum Konfigurieren und Veranschaulichen des Remotezugriffs mit sechs Servern und zwei Clientcomputern. Die vollständige Remotezugriffs-Testumgebung mit NLB simuliert ein Intranet, das Internet sowie ein Heimnetzwerk und veranschaulicht die Remotezugriffsfunktionalität in verschiedenen Internetverbindungsszenarios.

### IMPORTANT

Diese Testumgebung ist eine Machbarkeitsstudie mit der minimalen Anzahl an Computern. Die in dieser Anleitung beschriebene Konfiguration ist nur für Testzwecke geeignet und sollte nicht in einer Produktionsumgebung verwendet werden.

## Bekannte Probleme

Im Folgenden finden Sie bekannte Probleme beim Konfigurieren eines Clusterszenarios:

- Nach dem Konfigurieren von DirectAccess in einer ausschließlichen IPv4-Bereitstellung mit einem einzelnen Netzwerkadapter und nach automatischem Konfigurieren von Standard-DNS64 (die IPv6-Adresse mit „:3333::“) auf dem Netzwerkadapter wird der Benutzer bei dem Versuch, den Lastenausgleich über die Remotezugriffs-Verwaltungskonsole zu aktivieren, zur Eingabe einer IPv6-DIP-Adresse aufgefordert. Wenn eine IPv6-DIP-Adresse angegeben wird, tritt nach dem Klicken auf **Commit ausführen** ein Konfigurationsfehler mit folgender Fehlermeldung auf: Der Parameter ist falsch.

So lösen Sie dieses Problem:

1. Laden Sie die Sicherung herunter, und stellen Sie Skripts aus [Back up and Restore Remote Access Configuration](#) wieder her.
2. Sichern Sie die Remotezugriffs-GPOs mit dem heruntergeladenen Skript „Backup-RemoteAccess.ps1“.
3. Versuchen Sie, den Lastenausgleich bis zu dem Schritt zu aktivieren, bei dem ein Fehler auftritt. Erweitern Sie den Detailbereich im Dialogfeld „Lastenausgleich aktivieren“, klicken Sie mit der rechten Maustaste in den Detailbereich, und klicken Sie auf **Skript kopieren**.

4. Öffnen Sie Editor, und fügen Sie den Inhalt der Zwischenablage ein. Beispiel:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress
@('10.244.4.19/255.255.255.0','fdc4:29bd:abde:3333::2/128') -InternetVirtualIPAddress
@('fdc4:29bd:abde:3333::1/128', '10.244.4.21/255.255.255.0') -ComputerName
'DA1.domain1.corp.contoso.com' -Verbose
```

5. Schließen Sie alle offenen Remotezugriffs-Dialogfelder und die Remotezugriffs-Verwaltungskonsole.

6. Bearbeiten Sie den eingefügten Text, und entfernen Sie die IPv6-Adressen. Beispiel:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress @('10.244.4.19/255.255.255.0') -
InternetVirtualIPAddress @('10.244.4.21/255.255.255.0') -ComputerName
'DA1.domain1.corp.contoso.com' -Verbose
```

7. Führen Sie den Befehl aus dem vorherigen Schritt in einem PowerShell-Fenster mit erhöhten Rechten aus.

8. Wenn während der Ausführung des Cmdlets ein Fehler auftritt (nicht durch falsche Eingabewerte), führen Sie den Befehl „Restore-RemoteAccess.ps1“ aus, und befolgen Sie die Anweisungen, um sicherzustellen, dass die Integrität der ursprünglichen Konfiguration beibehalten wird.

9. Nun können Sie die Remotezugriffs-Verwaltungskonsole wieder öffnen.

# Übersicht über das Testumgebungsszenario für DirectAccess-Cluster-NLB

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

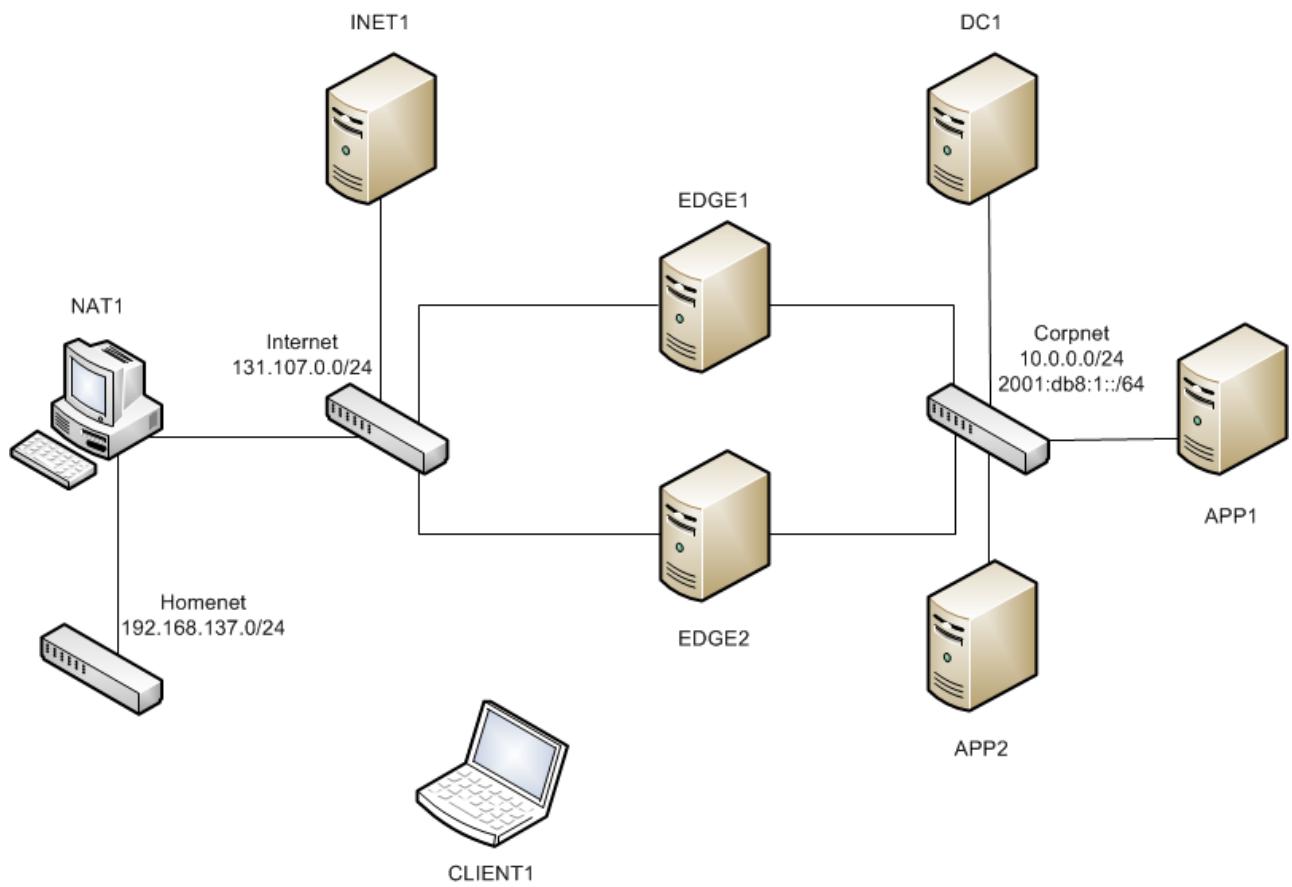
In diesem Test Labor Szenario wird DirectAccess mit folgenden Aufgaben bereitgestellt:

- **DC1**-ein Server, der als Domänen Controller, Domain Name System (DNS)-Server und DHCP-Server (Dynamic Host Configuration Protocol) konfiguriert ist.
- **Edge1**-ein Server im internen Netzwerk, der als erster RAS-Server in einem Remote Zugriffs Server-Cluster konfiguriert ist. Dieser Server verfügt über zwei Netzwerkadapter: eine Verbindung mit dem internen Netzwerk und die andere mit dem externen Netzwerk.
- **EDGE2**-ein Server im internen Netzwerk, der als zweiter RAS-Server in einem RAS-Server Cluster konfiguriert ist. Dieser Server verfügt über zwei Netzwerkadapter: eine Verbindung mit dem internen Netzwerk und die andere mit dem externen Netzwerk.
- **App1**-ein Server im internen Netzwerk, der als Web-und Dateiserver konfiguriert ist, und als Unternehmens-Stamm Zertifizierungsstelle (Certification Authority, ca)
- **APP2**-ein Computer im internen Netzwerk, der als einziger IPv4-Web-und-Dateiserver konfiguriert ist. Mithilfe dieses Computers werden die NAT64/DNS64-Funktionen hervorgehoben.
- **INET1**-ein Server, der als Internet-DNS und DHCP-Server konfiguriert ist.
- **NAT1**-ein Client Computer, der als NAT-Gerät (Network Address Translator) mithilfe der Freigabe von Internet Verbindungen konfiguriert ist.
- **CLIENT1**-ein Client Computer, der als DirectAccess-Client konfiguriert ist und zum Testen der DirectAccess-Konnektivität bei der Umstellung zwischen dem internen Netzwerk, dem simulierten Internet und einem Heimnetzwerk verwendet wird.

Die Testumgebung besteht aus drei Subnetzen, die Folgendes simulieren:

- Ein Heimnetzwerk mit dem Namen homenet (192.168.137.0/24), das durch eine NAT mit dem Internet verbunden ist.
- Das externe Netzwerk, das durch das Internet Subnetz (131.107.0.0/24) dargestellt wird.
- Ein internes Netzwerk mit dem Namen Corpnet (10.0.0.0/24; 2001: db8:1::/64), das vom Remote Zugriffs Server vom Internet getrennt ist.

Computer in jedem Subnetz stellen eine Verbindung entweder über einen physischen oder einen virtuellen Hub oder Switch her, wie in der folgenden Abbildung dargestellt.



# Konfigurationsanforderungen an die Testumgebung für DirectAccess-Cluster-NLB

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die folgenden Komponenten sind für die Konfiguration von DirectAccess in der Testumgebung erforderlich:

- Die Produkt-CD oder-Dateien für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.
- Sechs Computer oder virtuelle Computer, die die Mindesthardwareanforderungen für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012; erfüllen auf zwei Computern sind zwei Netzwerkadapter installiert.
- Die Produkt-CD oder-Dateien für Windows 10® oder Windows® 8.
- Zwei Computer oder virtuelle Computer, die die Mindesthardwareanforderungen für Windows 10® oder Windows® 8 erfüllen auf einem dieser Computer sind zwei Netzwerkadapter installiert.

# Schritte zum Konfigurieren der Testumgebung für DirectAccess-Cluster-NLB

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In den folgenden Schritten wird beschrieben, wie Sie die Remote Zugriffs Infrastruktur konfigurieren, die RAS-Server und -Clients konfigurieren und die DirectAccess-Konnektivität aus den Subnetzen Internet und homenet testen.

In dieser Test Umgebungs Anleitung erstellen Sie einen NLB-aktivierten Remote Zugriffs Cluster, indem Sie die folgenden Schritte ausführen:

- [Schritt 1: vervollständigen Sie die DirectAccess-Konfiguration.](#) Führen Sie alle Schritte in der [Test Umgebungs Anleitung zum Veranschaulichen der Einrichtung von DirectAccess Single Server mit gemischemtem IPv4 und IPv6aus.](#)
- [Schritt 2: Konfigurieren von Edge1.](#) Konfigurieren Sie die Remote Zugriffs Rolle auf Edge1 für den Lastenausgleich.
- [Schritt 3: Installieren und Konfigurieren von EDGE2.](#) EDGE2 fungiert als zweiter RAS-Server in einem Remote Zugriffs Cluster.
- [Schritt 4: Erstellen des Remote Zugriffs Clusters mit Netzwerk Lastenausgleich](#) Edge1 wird als erster Server in einem Remote Zugriffs Cluster konfiguriert. EDGE2 wird dem Cluster hinzugefügt, und NLB ist für den Cluster konfiguriert.
- [Schritt 5: Testen der DirectAccess-Konnektivität über das Internet und über den Cluster.](#) Nach Abschluss der NLB-und Cluster Konfiguration können Sie die DirectAccess-Client Konnektivität über den Cluster mit Lastenausgleich testen.
- [Schritt 6: Testen der DirectAccess-Client Konnektivität hinter einem NAT-Gerät.](#) Verschieben Sie den Client Computer hinter ein NAT-Gerät, um das Testen der DirectAccess-Client Konnektivität hinter einem Heim Router zu simulieren.
- [Schritt 7: Testen der Konnektivität bei der Rückkehr zum Unternehmensnetzwerk.](#) Stellen Sie sicher, dass der Client Computer bei der Rückkehr zu Corpnet weiterhin auf Unternehmensressourcen zugreifen kann.
- [Schritt 8: Erstellen einer Momentaufnahme der Konfiguration](#) Nachdem Sie die Testumgebung abgeschlossen haben, erstellen Sie eine Momentaufnahme des funktionierenden NLB-Clusters für den Remote Zugriff, damit Sie später wieder zurückkehren können, um weitere Szenarios zu testen.

# Schritt 1 vervollständigen der DirectAccess-Konfiguration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt besteht darin, alle Schritte in der [Test Umgebungs Anleitung zum Veranschaulichen der Einrichtung eines einzelnen Servers mit gemischemtem IPv4 und IPv6](#) auszuführen. Wenn Sie die Schritte in dieser Test Umgebungs Anleitung bereits ausgeführt und eine Momentaufnahme oder ein Datenträger Image der Testumgebung gespeichert haben, können Sie die Momentaufnahme oder das Image wiederherstellen und mit dem nächsten Schritt beginnen.

# Schritt 2 Edge1 konfigurieren

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Das folgende Verfahren wird auf dem DirectAccess-Server ausgeführt:

## So konfigurieren Sie DirectAccess auf Edge1

1. Geben Sie auf dem **Start Bildschirmramgmtui. exeein**, und drücken Sie dann die EINGABETASTE. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remote Zugriffs-Verwaltungskonsole im linken Bereich auf **Konfiguration**.
3. Klicken Sie im mittleren Bereich der Konsole im Bereich **Schritt 2 RAS-Server** auf **Bearbeiten**.
4. Klicken Sie im Setup-Assistenten für den **Remote Zugriffs Server** auf **Präfix Konfiguration**. Geben Sie auf der Seite **Präfix Konfiguration** unter **IPv6-Präfix, das DirectAccess-Client Computern zugewiesen ist** Folgendes ein : **2001: db8:1: 1000::/59**, und klicken Sie dann auf **weiter**.
5. Klicken Sie auf **Fertig stellen**.
6. Klicken Sie im mittleren Bereich der Konsole auf **Fertigstellen**.
7. Überprüfen Sie im Dialogfeld **Remote Zugriffs Überprüfung** die Konfigurationseinstellungen, und klicken Sie dann auf **übernehmen**. Klicken Sie im Dialogfeld **Anwenden der Einstellungen zum Einrichten des Remotezugriffs** auf **Schließen**.

# Schritt 3 installieren und Konfigurieren von EDGE2

09.04.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

EDGE2 ist das zweite Mitglied eines Remote Zugriffs Clusters. EDGE2 wird vor dem Aktivieren der Cluster Konfiguration installiert und konfiguriert.

Führen Sie die folgenden Schritte aus, um EDGE2 zu konfigurieren:

## Installieren des Betriebssystems auf EDGE2

1. Starten Sie auf EDGE2 die Installation von Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.
2. Befolgen Sie die Anweisungen, um die Installation abzuschließen, indem Sie Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 (vollständige Installation) und ein sicheres Kennwort für das lokale Administrator Konto angeben. Melden Sie sich mit dem lokalen Administratorkonto an.
3. Verbinden Sie EDGE2 mit einem Netzwerk, das über Internet Zugriff verfügt, und führen Sie Windows Update aus, um die neuesten Updates für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 zu installieren, und trennen Sie dann die Verbindung mit dem Internet.
4. Verbinden Sie einen Netzwerkadapter mit dem Subnetz "Corpnet" oder dem virtuellen Switch, der das Subnetz "Corpnet" darstellt, und der andere mit dem Internet Subnetz oder dem virtuellen Switch, der das Internet-Subnetz darstellt.

## Konfigurieren von TCP/IP-Eigenschaften

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **verkabelte Ethernet-Verbindung** auf den Link.
2. Klicken Sie im Fenster **Netzwerkverbindungen** mit der rechten Maustaste auf die Netzwerkverbindung, die mit dem Subnetz "Corpnet" oder dem virtuellen Switch verbunden ist, und klicken Sie dann auf **Umbenennen**.
3. Geben Sie **Corpnestein**, und drücken Sie dann die EINGABETASTE.
4. Klicken Sie mit der rechten Maustaste auf **Corpnet**, und klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)**, und klicken Sie dann auf **Eigenschaften**.
6. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie unter **IP-Adresse** den Namen **10.0.0.8** ein. Geben Sie im Feld **Subnetzmaske** den Wert **255.255.255.0** ein.
7. Klicken Sie auf **Folgende DNS-Serveradressen verwenden**. Geben Sie im Feld **Bevorzugter DNS-Server** den Wert **10.0.0.1** ein.
8. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
9. Geben Sie unter **DNS-Suffix für diese Verbindung** **Corp.contoso.com** ein, und klicken Sie zweimal auf **OK**.
10. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)**, und klicken Sie dann auf **Eigenschaften**.

11. Klicken Sie auf **folgende IPv6-Adresse verwenden**. Geben Sie in der **IPv6-Adresse** `2001: db8:1:: 8` ein. Geben Sie unter **Subnetzpräfix-Längeden** Wert `64`ein.
  12. Klicken Sie auf **Folgende DNS-Serveradressen verwenden**. Geben Sie unter **Bevorzugter DNS-Server** `2001: db8:1:: 1`ein.
  13. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
  14. Geben Sie unter **DNS-Suffix für diese Verbindung** `Corp.contoso.com`ein, klicken Sie zweimal auf **OK** , und klicken Sie dann auf **Schließen**.
  15. Klicken Sie im Fenster **Netzwerkverbindungen** mit der rechten Maustaste auf die Netzwerkverbindung, die mit dem Subnetz Internet verbunden ist, und klicken Sie dann auf **Umbenennen**.
  16. Geben Sie **Internet**ein, und drücken Sie die EINGABETASTE.
  17. Klicken Sie mit der rechten Maustaste auf **Internet**, und klicken Sie dann auf **Eigenschaften**.
  18. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)** , und klicken Sie dann auf **Eigenschaften**.
  19. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie in **IP-Adresse** `131.107.0.8`ein. Geben Sie `255.255.255.0`in **Subnetzmase**ein.
  20. Klicken Sie auf die Registerkarte **DNS**
  21. Geben Sie unter **DNS-Suffix für diese Verbindung** `ISP.example.com`ein, und klicken Sie dann zweimal auf **OK** , und klicken Sie dann auf **Schließen**.
  22. Schließen Sie das Fenster **Netzwerkverbindungen**.
  23. Zum Überprüfen der Netzwerkkommunikation zwischen EDGE2 und DC1 klicken Sie auf **Start**, geben Sie `cmd`ein, und drücken Sie dann die EINGABETASTE.
  24. Geben Sie im Eingabe Aufforderungs Fenster `ping dc1.Corp.contoso.com` ein, und drücken Sie die EINGABETASTE. Vergewissern Sie sich, dass vier Antworten von `10.0.0.1` oder der IPv6-Adresse `2001: db8:1:: 1` vorhanden sind.
  25. Schließen Sie das Eingabeaufforderungsfenster.
- ## EDGE2 umbenennen und der Domäne beitreten
1. Klicken Sie in der Server-Manager Konsole unter **lokaler Server**im Bereich **Eigenschaften** neben **Computer Name**auf den Link.
  2. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
  3. Geben Sie im Dialogfeld **Computername/Domänen Änderungen** im Feld **Computername** den Namen `EDGE2`ein. Klicken Sie im Bereich **Mitglied von** auf **Domäne**, geben Sie im Textfeld `Corp.contoso.com`ein, und klicken Sie dann auf **OK**.
  4. Geben Sie, wenn Sie zur Angabe eines Benutzernamens und eines Kennworts aufgefordert werden, `User1` und das zugehörige Kennwort ein, und klicken Sie dann auf **OK**.
  5. Klicken Sie, wenn das Begrüßungsdialogfeld für die Domäne `&quot;corp.contoso.com&quot;` angezeigt wird, auf **OK**.
  6. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
  7. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
  8. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.

9. Melden Sie sich nach dem Neustart als corp\user1 an.

## Installieren des IP-HTTPS-Zertifikats

1. Geben Sie auf dem **Start** BildschirmMMC. exeein, und drücken Sie dann die EINGABETASTE. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** auf **Zertifikate**, klicken Sie auf **Hinzufügen**, klicken Sie auf **Computer Konto**, klicken Sie auf **weiter**, klicken Sie auf **Fertigstellen** und dann auf **OK**.
4. Navigieren Sie im linken Bereich der Konsole zu **Zertifikate (lokaler Computer) \personal\zertifikate**. Klicken Sie mit der rechten Maustaste auf den Knoten **Zertifikate**, zeigen Sie auf **Alle Tasks**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
5. Klicken Sie im Assistenten für die Zertifikat Registrierung zweimal auf **weiter**.
6. Aktivieren Sie auf der Seite **Zertifikate anfordern** das Kontrollkästchen **Webserver**, und klicken Sie dann auf **Weitere Informationen sind erforderlich, um sich für dieses Zertifikat anzumelden**.
7. Klicken Sie im Dialogfeld **Zertifikat Eigenschaften** auf der Register Karte Antragsteller im Bereich **Antragsteller Name** in der Liste **Typ** auf **allgemeiner Name**.
8. Geben Sie **Edge1.contoso.com** in **value** ein, und klicken Sie dann auf **Hinzufügen**.
9. Klicken Sie im Bereich **alternativer Name** in der Liste **Typ** auf **DNS**.
10. Geben Sie **Edge1.contoso.com** in **value** ein, und klicken Sie dann auf **Hinzufügen**.
11. Geben Sie auf der Registerkarte **Allgemein** unter Anzeige **Name** den Namen **IP-HTTPS-Zertifikate** ein.
12. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
13. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, ob ein neues Zertifikat mit dem Namen **Edge1.contoso.com** mit dem vorgesehenen Zweck der Server Authentifizierung registriert wurde.
14. Schließen Sie das Konsolenfenster. Wenn Sie zum Speichern der Einstellungen aufgefordert werden, klicken Sie auf **Nein**.

## Installieren der Remote Zugriffs Rolle auf EDGE2

1. Klicken Sie in der Server-Manager-Konsole im **Dashboard** auf **Rollen und Features hinzufügen**.
2. Klicken Sie dreimal auf **Weiter**, um zur Anzeige für die Serverrollenauswahl zu gelangen.
3. Auf der **Serverrollen auswählen** die Option **RAS** klicken Sie auf **Features hinzufügen** und klicken Sie dann auf **Weiter**.
4. Klicken Sie fünfmal auf **Weiter**.
5. Klicken Sie im Dialogfeld **Installationsauswahl** bestätigen auf **Installieren**.
6. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.

# Schritt 4 Erstellen des Remote Zugriffs Clusters mit Netzwerk Lastenausgleich

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 ermöglichen Ihnen das Erstellen von Clustern von Remote Zugriffs Servern. Ein Cluster fungiert als einzelner logischer Server und ermöglicht eine zentralisierte Konfiguration und Verwaltung der Server im Cluster. Bei Verwendung des Netzwerk Lastenausgleichs (Network Load Balancing, NLB) wird die Unterstützung für bis zu 8 Remote Zugriffs Mitglieder in einem einzelnen Cluster unterstützt. RAS-Cluster bieten Hochverfügbarkeit und Lastenausgleich von Verbindungen zwischen DirectAccess-Clients und dem internen Netzwerk.

Die folgenden Prozeduren ermöglichen es Ihnen, einen Remote Zugriffs Cluster zu erstellen und zu testen:

1. Installieren Sie das Feature für den Netzwerk Lastenausgleich auf Edge1 und EDGE2. Vor dem Aktivieren des Lasten Ausgleichs müssen Sie das Feature für den Netzwerk Lastenausgleich sowohl auf Edge1 als auch auf EDGE2 installieren.
2. Aktivieren Sie den Lastenausgleich auf Edge1. Edge1 wurde ursprünglich im Einzel Server Modus installiert. Um den Lastenausgleich zu aktivieren, konfigurieren Sie neue externe und interne dedizierte IP-Adressen (Dips) für Edge1. Die vorherigen Dips auf Edge1 werden automatisch als virtuelle IP-Adressen (VIPs) für den Cluster konfiguriert. Die neue externe DIP ist z 131.107.0.10, die neue interne IPv4-DIP ist 10.0.0.10, die neue interne IPv6-DIP ist 2001: db8:1:: 10. Die Cluster-VIPs lauten 131.107.0.2 und 131.107.0.2 (extern), 10.0.0.2 und 2001: db8:1:: 2 (intern).
3. Fügen Sie dem Cluster mit Lastenausgleich EDGE2 hinzu. Nachdem Sie den Lastenausgleich aktiviert haben, können Sie dem Cluster jetzt EDGE2 hinzufügen, um einen Lastenausgleich und hohe Verfügbarkeit für DirectAccess-Clientverbindungen bereitzustellen.

## Erforderliche Komponenten

Wenn Sie diese Testumgebung auf virtuellen Computern erstellen, müssen Sie das Spoofing von Mac-Adressen auf Edge1 und EDGE2 aktivieren.

### Aktivieren des Spoofing von Mac-Adressen auf Edge1 und EDGE2

1. Führen Sie ein ordnungsgemäßes Herunterfahren auf Edge1 und EDGE2 aus.
2. Klicken Sie auf dem Computer, auf dem Ihre virtuellen Computer gehostet werden, im **Hyper-V-Manager** mit der rechten Maustaste auf Edge1, und klicken Sie dann auf **Einstellungen**
3. Klicken Sie im Dialogfeld **Einstellungen** in der Liste **Hardware** auf den Netzwerkadapter, der mit dem Unternehmensnetzwerk verbunden ist, und aktivieren Sie dann im Detailbereich das Kontrollkästchen **Spoofing von Mac-Adressen aktivieren**.
4. Klicken Sie in der Liste **Hardware** auf den Netzwerkadapter, der mit dem Internet verbunden ist, und aktivieren Sie dann im Detailbereich das Kontrollkästchen **Spoofing von Mac-Adressen aktivieren**.
5. Klicken Sie im Dialogfeld **Einstellungen** auf **OK**.
6. Wiederholen Sie diesen Vorgang aus Schritt 2 auf EDGE2.

# Installieren des Netzwerk Lastenausgleichs-Features auf Edge1 und EDGE2

Wenn Sie Edge1 und EDGE2 in einem Cluster konfigurieren möchten, müssen Sie das Feature für den Netzwerk Lastenausgleich sowohl für Edge1 als auch für EDGE2 installieren.

## So installieren Sie den Netzwerk Lastenausgleich

1. Klicken Sie auf Edge1 in der Server-Manager-Konsole im Dashboard auf **Rollen und Features hinzufügen**.
2. Klicken Sie viermal auf **weiter**, um zum Bildschirm für die Server Funktionsauswahl zu gelangen.
3. Klicken Sie im Dialogfeld **Features auswählen** auf **Netzwerk Lastenausgleich**, klicken Sie auf **Features hinzufügen**, klicken Sie auf **weiter**, und klicken Sie dann auf **Installieren**.
4. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.
5. Wiederholen Sie diesen Vorgang auf EDGE2.

## Aktivieren des Lasten Ausgleichs auf Edge1

Verwenden Sie dieses Verfahren, um den Lastenausgleich zu aktivieren und die neuen Dips auf Edge1 zu konfigurieren.

### Aktivieren des Lasten Ausgleichs

1. Klicken Sie auf Edge1 auf **Start**, geben Sie **ramgmtui. exeein**, und drücken Sie dann die EINGABETASTE. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remote Zugriffs-Verwaltungskonsole im linken Bereich auf **Konfiguration**, und klicken Sie dann im Bereich **Tasks** auf **Lastenausgleich aktivieren**.
3. Klicken Sie im Assistenten zum Aktivieren des Lasten Ausgleichs auf **weiter**.
4. Klicken Sie auf der Seite **Lasten Ausgleichs Methode** auf **Windows-Netzwerk Lastenausgleich (NLB) verwenden**, und klicken Sie dann auf **weiter**.
5. Geben Sie auf der Seite **externe dedizierte IP-Adressen** im Feld **IPv4-Adresse z 131.107.0.10** im Feld **Subnetzmaske** ein, vergewissern Sie sich, dass das Subnetzpräfix 255.255.255.0 lautet, und klicken Sie dann auf **weiter**.
6. Führen Sie auf der Seite **interne dedizierte IP-Adressen** die folgenden Schritte aus, und klicken Sie dann auf **weiter**:
  - a. Geben Sie im Feld **IPv4 -Adresse 10.0.0.10** ein, und vergewissern Sie sich, dass im Feld **Subnetzmaske** das Subnetzpräfix 255.255.255.0 lautet.
  - b. Geben Sie im Feld **IPv6-Adresse** den Wert **2001: db8:1:: 10** ein, und überprüfen Sie in der Länge des Subnetzprefixes, ob der Wert **64** lautet.
7. Klicken Sie auf der Seite **Zusammenfassung** auf **Commit**.
8. Klicken Sie im Dialogfeld **Lastenausgleich aktivieren** auf **Schließen**.
9. Klicken Sie im Assistenten zum Aktivieren des Lasten Ausgleichs auf **Schließen**.

## Hinzufügen von EDGE2 zum Cluster mit Lastenausgleich

Verwenden Sie dieses Verfahren, um dem NLB-Cluster EDGE2 hinzuzufügen.

#### NOTE

Warten Sie zwei Minuten, nachdem Sie die vorherigen Schritte abgeschlossen haben, bevor Sie fortfahren. Nachdem der Netzwerk Lastenausgleich aktiviert wurde, wird der Befehl "raconfigtask" ausgeführt und konfiguriert den Computer mit NLB-Einstellungen. Dieser Vorgang kann einige Minuten in Anspruch nehmen, und wenn der Administrator eine weitere NLB-bezogene Konfiguration ausführt, bevor der Task beendet wird, tritt bei dieser Konfiguration ein Fehler auf.

### Hinzufügen von EDGE2 zum Cluster

1. Klicken Sie auf dem Computer Edge1 oder Virtual Machine in der Remote Zugriffs-Verwaltungskonsole im Bereich **Tasks** unter **Cluster mit LastenAusgleich auf Server hinzufügen oder entfernen**.
2. Klicken Sie im Dialogfeld **Server hinzufügen oder entfernen** auf **Server hinzufügen**.
3. Geben Sie im Assistenten zum **Hinzufügen eines Servers** auf der Seite **Server auswählen** den Namen **EDGE2** ein, und klicken Sie dann auf **weiter**.
4. Vergewissern Sie sich, dass auf der Seite **Netzwerkadapter** unter **externer Adapter** die Option **Internet** ausgewählt ist, und stellen Sie im **internen Adaptersicher**, dass **Corpnet** ausgewählt ist. Klicken Sie im Dialogfeld **Windows-Sicherheit** auf **Durchsuchen**, stellen Sie sicher, dass **IP-HTTPS-Zertifikat** ausgewählt ist, klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.
5. Klicken Sie auf der Seite **Zusammenfassung** auf **Hinzufügen**.
6. Klicken Sie auf der Seite **Abschluss des Vorgangs** auf **Schließen**.
7. Klicken Sie im Dialogfeld **Server hinzufügen oder entfernen** auf **Commit**.
8. Klicken Sie im Dialogfeld zum **Hinzufügen und Entfernen von Servern** auf **Schließen**.
9. Geben Sie auf dem **Start Bildschirmnlbmgr. exeein**, und drücken Sie die EINGABETASTE. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
10. Klicken Sie im **Netzwerk Lastenausgleich-Manager** auf **interner da-Cluster**. Stellen Sie im Detailbereich sicher, dass sowohl **Edge1 (Corpnet)** als auch **EDGE2 (Corpnet)** den Status **konvergiert** haben.
11. Wenn ein Server nicht **konvergiert** ist, klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf den Server, zeigen Sie auf **Host steuern**, und klicken Sie dann auf **starten**.
12. Klicken Sie im **Netzwerk Lastenausgleich-Manager** auf **Internet-da-Cluster**. Stellen Sie sicher, dass im Detailbereich sowohl **Edge1 (Internet)** als auch **EDGE2 (Internet)** den Status **konvergiert** aufweisen.
13. Wenn ein Server nicht **konvergiert** ist, klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf den Server, zeigen Sie auf **Host steuern**, und klicken Sie dann auf **starten**.

# Schritt 5 Testen der DirectAccess-Konnektivität über das Internet und über den Cluster

09.04.2020 • 9 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

CLIENT1 ist jetzt für DirectAccess-Tests bereit.

- Testen Sie die DirectAccess-Konnektivität über das Internet. Verbinden Sie CLIENT1 mit dem simulierten Internet. Wenn eine Verbindung mit dem simulierten Internet besteht, werden dem Client öffentliche IPv4-Adressen zugewiesen. Wenn einem DirectAccess-Client eine öffentliche IPv4-Adresse zugewiesen wird, versucht er, mithilfe einer IPv6-Übergangstechnologie eine Verbindung mit dem RAS-Server herzustellen.
- Testen Sie die DirectAccess-Client Konnektivität über den Cluster. Testen Sie die Cluster Funktionalität. Bevor Sie mit dem Testen beginnen, wird empfohlen, dass Sie für mindestens fünf Minuten sowohl Edge1 als auch EDGE2 Herunterfahren. Hierfür gibt es eine Reihe von Gründen, einschließlich ARP-Cache Timeouts und Änderungen im Zusammenhang mit NLB. Wenn Sie die NLB-Konfiguration in einer Testumgebung überprüfen, benötigen Sie einen Patienten, da Änderungen an der Konfiguration nicht sofort in der Konnektivität widergespiegelt werden, bis eine Zeitspanne verstrichen ist. Dies ist wichtig, wenn Sie die folgenden Aufgaben durchführen.

## TIP

Es wird empfohlen, den Internet Explorer-Cache vor dem Ausführen dieses Verfahrens zu löschen und jedes Mal, wenn Sie die Verbindung über einen anderen RAS-Server testen, um sicherzustellen, dass Sie die Verbindung testen und nicht die Webseiten aus dem Cache abrufen.

## Testen der DirectAccess-Konnektivität über das Internet

1. Entfernen Sie die CLIENT1 vom Corpnet-Switch, und verbinden Sie Sie mit dem Internet-Switch. Warten Sie 30 Sekunden.
2. Geben Sie in einem Windows PowerShell-Fenster mit erhöhten Rechten **ipconfig/flushdns** ein, und drücken Sie EINGABETASTE. Dadurch werden namens Auflösungs Einträge geleert, die möglicherweise noch im Client-DNS-Cache vorhanden sind, wenn der Client Computer mit dem Unternehmensnetzwerk verbunden war.
3. Geben Sie im Windows PowerShell-Fenster **Get-dnsclientnrptpolicy** ein, und drücken Sie die EINGABETASTE.

In der Ausgabe werden die aktuellen Einstellungen der Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) angezeigt. Diese Einstellungen geben an, dass alle Verbindungen zu Corp.contoso.com vom RAS-DNS-Server mit der IPv6-Adresse "2001: db8:1:: 2" aufgelöst werden sollen. Beachten Sie außerdem den NRPT-Eintrag, dass eine Ausnahme für den Namen "nls.corp.contoso.com" vorhanden ist; Namen in der Ausnahmeliste werden vom Remote-Access-DNS-Server nicht beantwortet. Sie können an die IP-Adresse des RAS-DNS-Servers pingen, um die Konnektivität zum RAS-Server zu bestätigen. Beispielsweise können Sie den Ping 2001: db8:1:: 2 ausführen.

4. Geben Sie im Windows PowerShell-Fenster **Ping App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse für App1 angezeigt werden. Dies ist in diesem Fall "2001: db8:1:: 3".

5. Geben Sie im Windows PowerShell-Fenster **Ping App2** ein, und drücken Sie die EINGABETASTE. Sie sollten Antworten von der NAT64-Adresse erhalten, die von EDGE1 zu APP2 zugeordnet wurde (in diesem Fall "fdc9:9f4e:eb1b:7777::a00:4").

Die Möglichkeit zum Ping-APP2 ist wichtig, da der Erfolg anzeigt, dass Sie eine Verbindung mithilfe von NAT64/DNS64 herstellen konnten, da APP2 eine reine IPv4-Ressource ist.

6. Lassen Sie das Windows PowerShell-Fenster für das nächste Verfahren geöffnet.
7. Öffnen Sie Internet Explorer, geben Sie in der Internet Explorer-Adressleiste **https://app1/** ein, und drücken Sie die EINGABETASTE. Die Standard-IIS-Website auf APP1 wird angezeigt.
8. Geben Sie in der Internet Explorer-Adressleiste **https://app2/** ein, und drücken Sie die EINGABETASTE. Die Standardwebsite auf APP2 wird angezeigt.
9. Geben Sie auf dem **Start** Bildschirm\\app2\\file ein, und drücken Sie dann die EINGABETASTE. Doppelklicken Sie auf die neue Textdokumentdatei.

Dies zeigt, dass Sie eine Verbindung mit einem reinen IPv4-Server herstellen konnten, indem Sie SMB zum Abrufen einer Ressource in der Ressourcen Domäne verwenden.
10. Geben Sie auf dem **Start** BildschirmWF. mscein, und drücken Sie dann die EINGABETASTE.
11. Beachten Sie in der Konsole **Windows-Firewall mit erweiterter Sicherheit**, dass nur das **private** oder **öffentliche Profil** aktiv ist. Die Windows-Firewall muss aktiviert sein, damit DirectAccess ordnungsgemäß funktioniert. Wenn die Windows-Firewall deaktiviert ist, funktioniert die DirectAccess-Konnektivität nicht.
12. Erweitern Sie im linken Bereich der Konsole den Knoten **Überwachung**, und klicken Sie auf den Knoten **Verbindungs Sicherheitsregeln**. Es sollten die aktiven Verbindungs Sicherheitsregeln angezeigt werden: **DirectAccess Policy-clientdecorp**, **DirectAccess Policy-ClientToDNS64NAT64PrefixExemption**, **DirectAccess Policy-clientdeinfraund DirectAccess Policy-clienttonlaausgenommen**. Führen Sie im mittleren Bereich einen Bildlauf nach rechts durch, um die ersten **Authentifizierungsmethoden** und 2. **Authentifizierungsmethoden** Spalten anzuzeigen. Beachten Sie, dass die erste Regel (clientescorp) Kerberos V5 verwendet, um den intranettunnel einzurichten, und die dritte Regel (clientesinfrastructure) verwendet NTLMv2, um den Infrastruktur Tunnel einzurichten.
13. Erweitern Sie im linken Bereich der Konsole den Knoten **Sicherheits Zuordnungen**, und klicken Sie auf den Knoten **Hauptmodus**. Beachten Sie die Infrastruktur Tunnel-Sicherheits Zuordnungen mit NTLMv2 und der intranettunnel-Sicherheits Zuordnung mithilfe von Kerberos V5. Klicken Sie mit der rechten Maustaste auf den Eintrag, der **Benutzer (Kerberos V5)** als 2. **Authentifizierungsmethode** anzeigt, und klicken Sie auf **Eigenschaften**. Beachten Sie, dass auf der Registerkarte **Allgemein** die **zweite lokale Authentifizierungs-ID corp\user1** lautet, die angibt, dass sich user1 erfolgreich bei der Corp-Domäne mithilfe von Kerberos authentifizieren konnte.

## Testen der DirectAccess-Client Konnektivität über den Cluster

1. Führen Sie ein ordnungsgemäßes Herunterfahren auf EDGE2 aus.

Sie können den Netzwerk Lastenausgleich-Manager verwenden, um beim Ausführen dieser Tests den Status der Server anzuzeigen.

2. Geben Sie auf CLIENT1 im Windows PowerShell-Fenster **ipconfig/flushdns** ein, und drücken Sie die EINGABETASTE. Dadurch werden namens Auflösungs Einträge geleert, die möglicherweise noch im Client-DNS-Cache vorhanden sind.
3. Pingen Sie im Windows PowerShell-Fenster den Befehl App1 und APP2. Sie sollten Antworten von diesen beiden Ressourcen erhalten.

4. Geben Sie auf dem **Start** Bildschirm\\app2\\filesein. Der Ordner "freigegeben" sollte auf dem Computer "APP2" angezeigt werden. Die Möglichkeit zum Öffnen der Dateifreigabe auf APP2 gibt an, dass der zweite Tunnel, der die Kerberos-Authentifizierung für den Benutzer erfordert, ordnungsgemäß funktioniert.
5. Öffnen Sie Internet Explorer, und öffnen Sie dann die Websites <https://app1/> und <https://app2/>. Die Möglichkeit, beide Websites zu öffnen, bestätigt, dass der erste und der zweite Tunnel aktiv sind und funktionsfähig sind. Schließen Sie Internet Explorer.
6. Starten Sie den EDGE2-Computer.
7. Auf Edge1 führen Sie ein ordnungsgemäßes Herunterfahren aus.
8. Warten Sie fünf Minuten, und kehren Sie dann zu CLIENT1 zurück. Führen Sie die Schritte 2-5 aus. Dadurch wird bestätigt, dass CLIENT1 transparent ein Failover zu EDGE2 ausführen konnte, nachdem Edge1 nicht mehr zur Verfügung stand.

# Schritt 6 Testen der DirectAccess-Client Konnektivität hinter einem NAT-Gerät

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Wenn ein DirectAccess-Client hinter einem NAT-Gerät oder einem Webproxyserver mit dem Internet verbunden wird, verwendet der DirectAccess-Client entweder Teredo oder IP-HTTPS zur Verbindungsherstellung mit dem RAS-Server.

Wenn das NAT-Gerät ausgehenden UDP-Port 3544 für die öffentliche IP-Adresse des RAS-Servers aktiviert, wird Teredo verwendet. Wenn kein Teredo-Zugriff verfügbar ist, fällt der DirectAccess-Client auf IP-HTTPS über den ausgehenden TCP-Port 443 zurück, wodurch der Zugriff durch Firewalls oder Webproxyserver über den herkömmlichen SSL-Port ermöglicht wird.

Falls eine Authentifizierung für den Webproxy erforderlich ist, wird die IP-HTTPS-Verbindung fehlschlagen. IP-HTTPS-Verbindungen schlagen auch fehl, wenn vom Webproxy eine ausgehende SSL-Prüfung durchgeführt wird, da die HTTPS-Sitzung am Webproxy anstatt am RAS-Server beendet wird. In diesem Abschnitt führen Sie die gleichen Tests wie bei der Herstellung einer IP6-zu-IP4-Verbindung im vorherigen Abschnitt durch.

Die folgenden Verfahren werden auf beiden Clientcomputern ausgeführt:

1. Testen Sie die Teredo-Konnektivität. Der erste Satz von Tests wird ausgeführt, wenn der DirectAccess-Client für die Verwendung von Teredo konfiguriert ist. Das ist die automatische Einstellung, wenn das NAT-Gerät ausgehenden Zugriff auf den UDP-Port 3544 ermöglicht.
2. Testen Sie die IP-HTTPS-Konnektivität. Die zweite Testreihe wird durchgeführt, wenn der DirectAccess-Client für die Verwendung von IP-HTTPS konfiguriert ist. Um IP-HTTPS-Konnektivität vorzuführen, wird Teredo auf den Clientcomputern deaktiviert.

## TIP

Es wird empfohlen, den Internet Explorer-Cache zu löschen, bevor Sie diese Prozeduren ausführen, um sicherzustellen, dass Sie die Verbindung testen und nicht die Website Seiten aus dem Cache abrufen.

## Erforderliche Komponenten

Vor der Durchführung dieser Tests trennen Sie CLIENT1 vom Internet-Switch, und verbinden Sie ihn mit dem Homenet-Switch. Auf die Frage hin, welche Art von Netzwerk Sie für das aktuelle Netzwerk definieren möchten, wählen Sie **Heimnetzwerk**.

Starten Sie EDGE1 und EDGE2, sofern diese nicht bereits ausgeführt werden.

## Testen der Teredo-Konnektivität

1. Öffnen Sie auf CLIENT1 ein Windows PowerShell-Fenster mit erhöhten Rechten, geben Sie **ipconfig/all** ein, und drücken Sie EINGABETASTE.
2. Prüfen Sie die Ausgabe des Befehls "ipconfig".

CLIENT1 ist jetzt hinter einem NAT-Gerät mit dem Internet verbunden und hat eine private IPv4-Adresse

erhalten. Wenn sich der DirectAccess-Client hinter einem NAT-Gerät befindet und eine private IPv4-Adresse zugeordnet wurde, wird Teredo als IPv6-Übergangstechnologie bevorzugt. In der Ausgabe des Befehls "ipconfig" sollten ein Abschnitt für Tunneladapter Teredo Tunneling Pseudo-Interface und die Beschreibung Microsoft-Teredo-Tunneling-Adapter mit einer IP-Adresse angezeigt werden, die entsprechend einer Teredo-Adresse mit "2001:" beginnt. Wenn der Teredo-Abschnitt nicht angezeigt wird, aktivieren Sie Teredo mit dem Befehl **netsh interface Teredo set state enterpriseclient**, und wiederholen Sie anschließend den Befehl "ipconfig". Für den Teredo-Tunneladapter wird kein Standardgateway aufgeführt.

3. Geben Sie im Windows PowerShell-Fenster **ipconfig/flushdns** ein, und drücken Sie die EINGABETASTE.

Dadurch werden Namensauflösungseinträge geleert, die eventuell noch im Client-DNS-Cache vorhanden sind, seitdem der Clientcomputer mit dem Internet verbunden wurde.

4. Geben Sie im Windows PowerShell-Fenster **Get-dnsclientnrptpolicy** ein, und drücken Sie die EINGABETASTE.

In der Ausgabe werden die aktuellen Einstellungen der Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) angezeigt. Diese Einstellungen weisen darauf hin, dass alle Verbindungen zu .corp.contoso.com vom Remote-Access-DNS-Server mit der IPv6-Adresse "2001:db8:1::2" aufgelöst werden sollen. Beachten Sie außerdem den NRPT-Eintrag, dass eine Ausnahme für den Namen "nls.corp.contoso.com" vorhanden ist; Namen in der Ausnahmeliste werden vom Remote-Access-DNS-Server nicht beantwortet. Sie können einen Ping-Befehl an die IP-Adresse des Remote-Access-DNS-Servers senden, um die Konnektivität zum RAS-Server zu bestätigen. In diesem Beispiel können Sie einen Ping-Befehl an "2001:db8:1::2" senden.

5. Geben Sie im Windows PowerShell-Fenster **Ping App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse von APP1 "2001:db8:1::3" angezeigt werden.
6. Geben Sie im Windows PowerShell-Fenster **Ping App2** ein, und drücken Sie die EINGABETASTE. Sie sollten Antworten von der NAT64-Adresse erhalten, die von EDGE1 zu APP2 zugeordnet wurde (in diesem Fall "fdc9:9f4e:eb1b:7777::a00:4").
7. Lassen Sie das Windows PowerShell-Fenster für das nächste Verfahren geöffnet.
8. Öffnen Sie Internet Explorer, geben Sie in der Internet Explorer-Adressleiste <https://app1/> ein, und drücken Sie die EINGABETASTE. Die Standard-IIS-Website auf APP1 wird angezeigt.
9. Geben Sie in der Internet Explorer-Adressleiste <https://app2/> ein, und drücken Sie die EINGABETASTE. Die Standardwebsite auf APP2 wird angezeigt.
10. Geben Sie auf dem **Start Bildschirm\\app2\\file** ein, und drücken Sie dann die EINGABETASTE. Doppelklicken Sie auf die neue Textdokumentdatei. Dadurch wird bewiesen, dass Sie eine Verbindung zu einem reinen IPv4-Server herstellen konnten, indem Sie mit SMB eine Ressource auf einem reinen IPv4-Host abgerufen haben.

## IP-HTTPS-Konnektivität testen

1. Öffnen Sie ein Windows PowerShell-Fenster mit erhöhten Rechten, geben Sie **Netsh Interface Teredo Set State deaktiviert** ein, und drücken Sie EINGABETASTE. Dadurch wird Teredo auf dem Clientcomputer deaktiviert. Der Clientcomputer kann sich nun selbst für IP-HTTPS konfigurieren. Nach Ausführung des Befehls wird die Antwort **OK** angezeigt.
2. Geben Sie im Windows PowerShell-Fenster **ipconfig/all** ein, und drücken Sie die EINGABETASTE.
3. Prüfen Sie die Ausgabe des Befehls "ipconfig". Dieser Computer ist jetzt hinter einem NAT-Gerät mit dem Internet verbunden und hat eine private IPv4-Adresse erhalten. Teredo ist deaktiviert, und der DirectAccess-Client fällt auf IP-HTTPS zurück. In der Ausgabe des Befehls "ipconfig" wird der Abschnitt Tunneladapter

iphttpsinterface mit einer IP-Adresse angezeigt, die entsprechend einer IP-HTTPS-Adresse mit "2001:db8:1:100" beginnt. Grundlage hierfür ist das Präfix, das beim Einrichten von DirectAccess konfiguriert wurde. Für den IP-HTTPS-Tunneladapter wird kein Standardgateway aufgeführt.

4. Geben Sie im Windows PowerShell-Fenster **ipconfig/flushdns** ein, und drücken Sie die EINGABETASTE. Dadurch werden Namensauflösungseinträge geleert, die eventuell noch im Client-DNS-Cache vorhanden sind, seitdem der Clientcomputer mit dem Unternehmensnetzwerk verbunden war.
5. Geben Sie im Windows PowerShell-Fenster **Ping App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse von APP1 "2001:db8:1::3" angezeigt werden.
6. Geben Sie im Windows PowerShell-Fenster **Ping App2** ein, und drücken Sie die EINGABETASTE. Sie sollten Antworten von der NAT64-Adresse erhalten, die von EDGE1 zu APP2 zugeordnet wurde (in diesem Fall "fdc9:9f4e:eb1b:7777::a00:4").
7. Öffnen Sie Internet Explorer, geben Sie in der Internet Explorer-Adressleiste **https://app1/** ein, und drücken Sie die EINGABETASTE. Die Standard-IIS-Site auf APP1 wird angezeigt.
8. Geben Sie in der Internet Explorer-Adressleiste **https://app2/** ein, und drücken Sie die EINGABETASTE. Die Standardwebsite auf APP2 wird angezeigt.
9. Geben Sie auf dem **Start** Bildschirm\\app2\\file ein, und drücken Sie dann die EINGABETASTE. Doppelklicken Sie auf die neue Textdokumentdatei. Dadurch wird bewiesen, dass Sie eine Verbindung zu einem reinen IPv4-Server herstellen konnten, indem Sie mit SMB eine Ressource auf einem reinen IPv4-Host abgerufen haben.

# Schritt 7 Testen der Konnektivität bei der Rückkehr zum Unternehmensnetzwerk

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Viele Ihrer Benutzer wechseln zwischen Remote Standorten und dem Unternehmensnetzwerk. Daher ist es wichtig, wenn Sie zum Unternehmensnetzwerk zurückkehren, dass Sie auf Ressourcen zugreifen können, ohne Änderungen an der Konfiguration vornehmen zu müssen. Der Remote Zugriff ermöglicht dies, weil der DirectAccess-Client beim zurückkehren zum Corpnet eine Verbindung mit dem Netzwerkadressen Server herstellen kann. Nachdem die HTTPS-Verbindung erfolgreich mit dem Netzwerkadressen Server hergestellt wurde, deaktiviert der DirectAccess-Client die DirectAccess-Client Konfiguration und verwendet eine direkte Verbindung mit Corpnet.

## Testen der Konnektivität auf CLIENT1

1. Beenden Sie CLIENT1, und entfernen Sie dann CLIENT1 aus dem Subnetz homenet oder dem virtuellen Switch, und verbinden Sie es mit dem Subnetz "Corpnet" oder dem virtuellen Switch. Aktivieren Sie CLIENT1, und melden Sie sich als corp\user1 an.
2. Öffnen Sie ein Windows PowerShell-Fenster mit erhöhten Rechten, geben Sie **ipconfig/allein**, und drücken Sie EINGABETASTE Die Ausgabe zeigt an, dass CLIENT1 über eine lokale IP-Adresse verfügt und dass kein aktiver IPv6-zu-IPv4-, Teredo-oder IP-HTTPS-Tunnel vorhanden ist.
3. Testen Sie die Konnektivität mit der Netzwerkf freigabe auf APP2. Geben Sie auf dem **Start** Bildschirm\\app2\\file ein, und drücken Sie dann die EINGABETASTE. Sie können die Datei in diesem Ordner öffnen.

# Schritt 8: Momentaufnahme des DirectAccess-Clusters (NLB-Konfiguration)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dadurch wird die DirectAccess-Testumgebung abgeschlossen. Um diese Konfiguration zu speichern, sodass Sie schnell zu einer funktionierenden DirectAccess-Konfiguration mit NLB-Cluster Konfiguration zurückkehren können, mit der Sie andere Test Umgebungs Anleitungen für DirectAccess und Test Umgebungs Anleitungen testen können, oder für Ihr eigenes Experimentieren und lernen, führen Sie die folgenden Schritte aus: folgenden

1. Schließen Sie alle Fenster auf allen physischen oder virtuellen Computern in der Testumgebung, und fahren Sie die Computer dann normal herunter.
2. Wenn Ihre Testumgebung auf virtuellen Computern basiert, speichern Sie eine Momentaufnahme der einzelnen virtuellen Computer, und benennen Sie die Momentaufnahmen DirectAccess-Cluster und NLB. Wenn Ihr Lab physische Computer verwendet, erstellen Sie Datenträger Images, um die Konfiguration der DirectAccess-Testumgebung zu speichern.

# Testumgebungsanleitung: Vorführung einer DirectAccess-Bereitstellung für mehrere Standorte

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der Remote Zugriff ist eine Server Rolle in den Betriebssystemen Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012, die Remote Benutzern den sicheren Zugriff auf interne Netzwerkressourcen über DirectAccess oder RRAS-VPN ermöglicht. Diese Anleitung enthält Schritt-für-Schritt-Anweisungen zum Erweitern der [Test Umgebungs Anleitung: veranschaulichen der Einrichtung von DirectAccess Single Server mit gemischemtem IPv4 und IPv6](#), um den Remote Zugriff in einem Szenario mit mehreren Standorten zu veranschaulichen.

Beim Bereitstellen des Remote Zugriffs in einem Szenario mit mehreren Standorten können Sie RAS-Server an geografisch unterschiedlichen Standorten konfigurieren. Früher mussten Remote Benutzer stets eine Verbindung mit dem Unternehmensnetzwerk über einen bestimmten DirectAccess-Server herstellen. Mit Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 und Windows 10 oder Windows 8 können Sie Einstiegspunkte für jeden geografischen Standort in Ihrer Bereitstellung konfigurieren. Jeder Einstiegspunkt kann ein einzelner RAS-Server oder ein Cluster von Remote Zugriffs Servern sein. Remote Benutzer haben die Möglichkeit, eine Verbindung mit einem der RAS-Einstiegspunkte der Organisation herzustellen. Wenn ein Remote Benutzer z. b. in der Regel eine Verbindung mit dem RAS-Einstiegspunkt in Asien herstellt, aber dann einen geschäftlichen Trip zu Europa durchführt, stellt der Client Computer automatisch eine Verbindung mit dem nächstgelegenen RAS-Einstiegspunkt her.

## Informationen zur Anleitung

Dieses Handbuch enthält Anweisungen zum Konfigurieren und veranschaulichen des Remote Zugriffs mithilfe von neun Servern und drei Client Computern. Die abgeschlossene Remote Zugriffs-Testumgebung für mehrere Standorte simuliert ein Intranet, das Internet und ein Heimnetzwerk und veranschaulicht die Remote Zugriffs Funktionalität in verschiedenen Internetverbindungs Szenarien.

### IMPORTANT

Diese Testumgebung ist eine Machbarkeitsstudie mit der minimalen Anzahl an Computern. Die in dieser Anleitung beschriebene Konfiguration ist nur für Testzwecke geeignet und sollte nicht in einer Produktionsumgebung verwendet werden.

# Übersicht über das Testumgebungsszenario

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der Remote Zugriff ist eine Server Rolle in den Betriebssystemen Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012, die Remote Benutzern den sicheren Zugriff auf interne Netzwerkressourcen über DirectAccess oder virtuelle private Netzwerke (Virtual Private Networks, VPNs) mit dem RRAS (Routing and Remote Access Service). Diese Anleitung enthält Schritt-für-Schritt-Anweisungen zum Erweitern der [Test Umgebungs Anleitung: veranschaulichen der Einrichtung von DirectAccess Single Server mit gemischemtem IPv4 und IPv6](#), um eine Konfiguration des einmaligen Zugriffs per Remote Zugriff zu veranschaulichen.

## **WARNING**

Der Entwurf dieser Test Umgebungs Anleitung umfasst Infrastruktur Server, z. b. einen Domänen Controller und eine Zertifizierungsstelle (Certification Authority, ca), auf denen entweder Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird. Die Verwendung dieser Test Umgebungs Anleitung zum Konfigurieren von Infrastruktur Servern, auf denen andere Betriebssysteme ausgeführt werden, wurde nicht getestet, und Anweisungen zum Konfigurieren anderer Betriebssysteme sind in diesem Handbuch nicht enthalten.

## Informationen zur Anleitung

Der Remote Zugriff in Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 bietet Unterstützung für die Client Authentifizierung mit OTP. Im Rahmen dieser Testumgebung wird nur RSA SecurID verwendet, um die OTP-Funktionalität mit Remote Zugriff zu veranschaulichen. Andere auf RADIUS basierende OTP-Lösungen werden ebenfalls unterstützt, sind jedoch außerhalb des Umfangs dieses Testlabors. Diese Anleitung enthält Anweisungen zum Konfigurieren und Veranschaulichen des Remotezugriffs mit sechs Servern und zwei Clientcomputern. Der abgeschlossene Remote Zugriff mit OTP-Test Labor simuliert ein Intranet, das Internet und ein Heimnetzwerk und veranschaulicht die Remote Zugriffs Funktionalität in verschiedenen Internetverbindungs Szenarien.

## **IMPORTANT**

Diese Testumgebung ist eine Machbarkeitsstudie mit der minimalen Anzahl an Computern. Die in dieser Anleitung beschriebene Konfiguration ist nur für Testzwecke geeignet und sollte nicht in einer Produktionsumgebung verwendet werden.

# Konfigurationsanforderungen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die folgenden Komponenten sind erforderlich, um den Remote Zugriff im Testlabor zu konfigurieren:

- Die Produkt-CD oder-Dateien für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.
- Neun Computer oder virtuelle Computer, die die Mindesthardwareanforderungen für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 erfüllen auf drei dieser Computer sind zwei Netzwerkadapter installiert.
- Die Produkt-CD oder-Dateien für Windows 10® oder Windows® 8.
- Die Produkt-CD oder-Dateien für Windows 7 Ultimate.
- Drei Computer oder virtuelle Computer, die die Mindesthardwareanforderungen für Windows 10®, Windows 8 oder Windows 7 erfüllen auf einem dieser Computer sind zwei Netzwerkadapter installiert.

# Schritte zum Konfigurieren der Testumgebung

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In den folgenden Schritten wird beschrieben, wie Sie die Remote Zugriffs Infrastruktur konfigurieren, die RAS-Server und-Clients konfigurieren und die DirectAccess-Konnektivität aus den Subnetzen Internet und homenet testen.

In dieser Test Umgebungs Anleitung erstellen Sie eine Remote Zugriffs Bereitstellung für mehrere Standorte, indem Sie die folgenden Schritte ausführen:

- [Schritt 1: vervollständigen der Basiskonfiguration.](#) Führen Sie alle Schritte in der [Test Umgebungs Anleitung zum Veranschaulichen der Einrichtung von DirectAccess Single Server mit gemischemtem IPv4 und IPv6](#) aus.
- [Schritt 2: Installieren und Konfigurieren von ROUTER1.](#) ROUTER1 bietet Routing-und Weiterleitungs Funktionen zwischen den Subnetzen Corpnet und 2-Corpnet.
- [Schritt 3: Installieren und Konfigurieren von CLIENT2.](#) CLIENT2 ist ein Windows 7-Client Computer, der verwendet wird, um die Abwärtskompatibilität einer Windows Server 2016-, Windows Server 2012 R2-oder Windows Server 2012-Remote Zugriffs Bereitstellung zu veranschaulichen.
- [Schritt 4: Konfigurieren von App1.](#) Konfigurieren Sie App1 mit ROUTER1 als Standard Gateway und 2 DC1 als alternativen DNS-Server.
- [Schritt 5: Konfigurieren von DC1.](#) Konfigurieren Sie DC1 mit einer zusätzlichen Active Directory Site und zusätzlichen Sicherheitsgruppen für Windows 7-Client Computer.
- [Schritt 6: Installieren und Konfigurieren von 2-DC1](#) Bei einer Bereitstellung mit mehreren Standorten verfügen Sie über zwei oder mehr Domänen und Standorte. 2 DC1 stellt Domänen Controller und DNS-Dienste für die corp2.Corp.contoso.com-Domäne bereit.
- [Schritt 7: Installieren und Konfigurieren von 2-App1](#) 2 App1 ein Web-und Dateiserver im Netzwerk "2-Corpnet".
- [Schritt 8: Konfigurieren von INET1.](#) INET1 simuliert das Internet in dieser Test Umgebungs Anleitung. Sie müssen einen DNS-Eintrag konfigurieren, der in die öffentliche IP-Adresse von 2-Edge1 aufgelöst wird.
- [Schritt 9: Konfigurieren von Edge1.](#) Konfigurieren Sie den DNS-Server 2-Corpnet und das Routing auf Edge1.
- [Schritt 10: Installieren und Konfigurieren von 2-Edge1](#) Bei einer Bereitstellung mit mehreren Standorten sind zwei Remote Zugriffs Server erforderlich. 2 Edge1 bietet Remote Zugriffs Dienste für die zweite Domäne.
- [Schritt 11: Konfigurieren der Bereitstellung für mehrere Standorte.](#) Nach dem Konfigurieren von Remote Zugriffs Servern können Sie die Bereitstellung für mehrere Standorte konfigurieren.
- [Schritt 12: Testen der DirectAccess-Konnektivität.](#) Testen Sie die DirectAccess-Konnektivität von beiden Client Computern aus dem Subnetz Internet über Edge1 und 2-Edge1.
- [Schritt 13: Testen der DirectAccess-Konnektivität hinter einem NAT-Gerät.](#) Testen Sie die DirectAccess-Konnektivität hinter einem NAT-Gerät.
- [Schritt 14: Erstellen einer Momentaufnahme der Konfiguration](#) Nachdem Sie die Testumgebung abgeschlossen haben, erstellen Sie eine Momentaufnahme der funktionierenden Remote Zugriffs Bereitstellung für mehrere Standorte, damit Sie sie später wieder aufrufen können, um weitere Szenarios zu

testen.

# Schritt 1 vervollständigen der DirectAccess-Konfiguration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt besteht darin, alle Schritte in der [Test Umgebungs Anleitung zum Veranschaulichen der Einrichtung eines einzelnen Servers mit gemischemtem IPv4 und IPv6](#) auszuführen. Wenn Sie die Schritte in dieser Test Umgebungs Anleitung bereits ausgeführt und eine Momentaufnahme oder ein Datenträger Image der Testumgebung gespeichert haben, können Sie die Momentaufnahme oder das Image wiederherstellen und mit dem nächsten Schritt beginnen.

# Schritt 2 ROUTER1 installieren und Konfigurieren von

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In dieser Test Umgebungs Anleitung für mehrere Standorte stellt der Routercomputer eine IPv4-und IPv6-Brücke zwischen den Subnetzen "Corpnet" und "2-Corpnet" bereit und fungiert als Router für den IP-HTTPS-und Teredo-Datenverkehr.

- Installieren des Betriebssystems auf ROUTER1
- Konfigurieren von TCP/IP-Eigenschaften und Umbenennen des Computers
- Deaktivieren der Firewall
- Konfigurieren von Routing und Weiterleitung

## Installieren des Betriebssystems auf ROUTER1

Installieren Sie zunächst Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.

### So installieren Sie das Betriebssystem auf ROUTER1

1. Starten Sie die Installation von Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 (vollständige Installation).
2. Folgen Sie den Installationsanweisungen, und legen Sie ein sicheres Kennwort für das lokale Administratorkonto fest. Melden Sie sich mit dem lokalen Administratorkonto an.
3. Verbinden Sie ROUTER1 mit einem Netzwerk, das über Internet Zugriff verfügt, und führen Sie Windows Update aus, um die neuesten Updates für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 zu installieren, und trennen Sie dann die Verbindung mit dem Internet.
4. Verbinden Sie ROUTER1 mit den Subnetzen Corpnet und 2-Corpnet.

## Konfigurieren von TCP/IP-Eigenschaften und Umbenennen des Computers

Konfigurieren Sie die TCP/IP-Einstellungen auf dem Router, und benennen Sie den Computer in ROUTER1 um.

### So konfigurieren Sie TCP/IP-Eigenschaften und benennen den Computer um

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **verkabelte Ethernet-Verbindung** auf den Link.
2. Klicken Sie im Fenster **Netzwerkverbindungen** mit der rechten Maustaste auf den mit Corpnet verbundenen Netzwerkadapter, klicken Sie auf **Umbenennen**, geben Sie **Corpnet** ein, und drücken Sie die EINGABETASTE.
3. Klicken Sie mit der rechten Maustaste auf **Corpnet**, und klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)**, und klicken Sie dann auf **Eigenschaften**.
5. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie unter **IP-Adresse** den Namen **10.0.0.254** ein. Geben Sie **255.255.255.0** in **Subnetzmase** ein, und klicken Sie dann auf **OK**.

6. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)**, und klicken Sie dann auf **Eigenschaften**.
7. Klicken Sie auf **folgende IPv6-Adresse verwenden**. Geben Sie in der **IPv6-Adresse 2001: db8:1:: FE ein**. Geben Sie unter **Subnetzpräfix-Länge 64** ein, und klicken Sie dann auf **OK**.
8. Klicken Sie im Dialogfeld **Corpnet-Eigenschaften** auf **Schließen**.
9. Klicken Sie im Fenster **Netzwerkverbindungen** mit der rechten Maustaste auf den Netzwerkadapter, der mit 2-Corpnet verbunden ist, klicken Sie auf **Umbenennen**, geben Sie **2-Corpnet** ein, und drücken Sie die **EINGABETASTE**.
10. Klicken Sie mit der rechten Maustaste auf **2-Corpnet**, und klicken Sie dann auf **Eigenschaften**.
11. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)**, und klicken Sie dann auf **Eigenschaften**.
12. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie unter **IP-Adressen** den Namen **10.2.0.254** ein. Geben Sie **255.255.255.0** in **Subnetzmaseke** ein, und klicken Sie dann auf **OK**.
13. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)**, und klicken Sie dann auf **Eigenschaften**.
14. Klicken Sie auf **folgende IPv6-Adresse verwenden**. Geben Sie in **IPv6-Adresse 2001: db8:2:: FEEin**. Geben Sie unter **Subnetzpräfix-Länge 64** ein, und klicken Sie dann auf **OK**.
15. Klicken Sie im Dialogfeld **Eigenschaften von 2 Corpnet** auf **Schließen**.
16. Schließen Sie das Fenster **Netzwerkverbindungen**.
17. Klicken Sie in der Server-Manager Konsole unter **lokaler Server** im Bereich **Eigenschaften** neben **Computer Name** auf den Link.
18. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
19. Geben Sie im Dialogfeld **Computername/Domänen Änderungen** unter **Computername** den Namen **ROUTER1** ein, und klicken Sie dann auf **OK**.
20. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
21. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
22. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.
23. Nachdem der Computer neu gestartet wurde, melden Sie sich mit dem lokalen Administrator Konto an.

## Deaktivieren der Firewall

Dieser Computer ist nur für die Bereitstellung des Routings zwischen den Subnetzen "Corpnet" und "2-Corpnet" konfiguriert. Daher muss die Firewall ausgeschaltet werden.

### So schalten Sie die Firewall aus

1. Geben Sie auf dem **Start** Bildschirm **WF. mscein**, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie in Windows-Firewall mit erweiterter Sicherheit im **Aktions** Bereich auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Windows-Firewall mit erweiterter Sicherheit** auf der Registerkarte **Domänen Profil** unter **Firewallstatus** auf **aus. Firewall state**.
4. Klicken Sie im Dialogfeld **Windows-Firewall mit erweiterter Sicherheit** auf der Registerkarte **privates Profil** unter **Firewallstatus** auf **Firewall state aus**.
5. Klicken Sie im Dialogfeld **Windows-Firewall mit erweiterter Sicherheit** auf der Registerkarte **Öffentliches Profil** unter **Firewallstatus** auf **Firewall state aus**, und klicken Sie dann auf **OK**.

6. Schließen Sie Windows-Firewall mit erweiterter Sicherheit.

## Konfigurieren von Routing und Weiterleitung

Um Routing-und Weiterleitungs Dienste zwischen den Subnetzen Corpnet und 2-Corpnet bereitzustellen, müssen Sie die Weiterleitung auf den Netzwerkschnittstellen aktivieren und statische Routen zwischen den Subnetzen konfigurieren.

### So konfigurieren Sie statische Routen

1. Geben Sie auf dem **Start** Bildschirmcmd. exeein, und drücken Sie dann die EINGABETASTE.
2. Aktivieren Sie die Weiterleitung an IPv4-und IPv6-Schnittstellen beider Netzwerkadapter mithilfe der folgenden Befehle. Drücken Sie nach dem Eingeben der einzelnen Befehle die EINGABETASTE.

```
netsh interface IPv4 set interface Corpnet forwarding=enabled  
netsh interface IPv4 set interface 2-Corpnet forwarding=enabled  
netsh interface IPv6 set interface Corpnet forwarding=enabled  
netsh interface IPv6 set interface 2-Corpnet forwarding=enabled
```

3. Aktivieren Sie das IP-HTTPS-Routing zwischen den Subnetzen "Corpnet" und "2-Corpnet".

```
netsh interface IPv6 add route 2001:db8:1:1000::/59 Corpnet 2001:db8:1::2  
netsh interface IPv6 add route 2001:db8:2:2000::/59 2-Corpnet 2001:db8:2::20
```

4. Aktivieren Sie das Teredo-Routing zwischen den Subnetzen "Corpnet" und "2-Corpnet".

```
netsh interface IPv6 add route 2001:0:836b:2::/64 Corpnet 2001:db8:1::2  
netsh interface IPv6 add route 2001:0:836b:14::/64 2-Corpnet 2001:db8:2::20
```

5. Schließen Sie das Eingabeaufforderungsfenster.

# Schritt 3 installieren und Konfigurieren von client2

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

CLIENT2 ist ein Windows 7-® Computer, der verwendet wird, um die Abwärtskompatibilität des Remote Zugriffs zu veranschaulichen, der auf Windows Server 2016-Servern ausgeführt wird.

1. So installieren Sie das Betriebssystem auf CLIENT2 Installieren Sie Windows® 7 Enterprise oder Windows® 7 Ultimate auf client2.
2. Um CLIENT2 der Corp-Domäne beizutreten. Fügen Sie CLIENT2 der Corp.contoso.com-Domäne hinzu.

## So installieren Sie das Betriebssystem auf CLIENT2

1. Starten Sie die Installation von Windows 7.
2. Wenn Sie zur Eingabe eines Benutzernamens aufgefordert werden, geben Sie **User1**ein. Wenn Sie zur Eingabe eines Computer namens aufgefordert werden, geben Sie **client2**ein.
3. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie ein sicheres Kennwort zweimal ein.
4. Wenn Sie zur Eingabe der Schutzeinstellungen aufgefordert werden, klicken Sie auf **Empfohlene Einstellungen verwenden**.
5. Wenn Sie zur Eingabe des aktuellen Speicher Orts Ihres Computers aufgefordert werden, klicken Sie auf **Work Network**.
6. Verbinden Sie CLIENT2 mit einem Netzwerk, das über Internet Zugriff verfügt, und führen Sie Windows Update aus, um die neuesten Updates für Windows 7 zu installieren, und trennen Sie die Verbindung mit dem Internet.
7. Verbinden Sie CLIENT2 mit dem Corpnet-Subnetz.

## Benutzerkontensteuerung

Wenn Sie das Betriebssystem Windows 7 konfigurieren, müssen Sie im Dialogfeld **Benutzerkontensteuerung** (**User Account Control** , UAC) für einige Aufgaben auf **weiter** klicken. Einige der Konfigurationsaufgaben erfordern eine UAC-Genehmigung. Wenn Sie dazu aufgefordert werden, klicken Sie immer auf **weiter** , um diese Änderungen zu autorisieren.

## So fügen Sie CLIENT2 der Corp-Domäne hinzu

1. Klicken Sie auf **Start**und mit der rechten Maustaste auf **Computer**und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Seite **System** im Bereich **Computer Name, Domäne und Arbeitsgruppen Einstellungen** auf **Einstellungen ändern**.
3. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
4. Klicken Sie im Dialogfeld **Computer Name/Domänen Änderungen** auf **Domäne**, geben Sie **Corp.contoso.com**ein, und klicken Sie dann auf **OK**.
5. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den

Benutzernamen und das Kennwort für das user1-Domänen Konto ein, und klicken Sie dann auf **OK**.

6. Klicken Sie, wenn das Begrüßungsdialogfeld für die Domäne %amp;quot;corp.contoso.com%amp;quot; angezeigt wird, auf **OK**.
7. Wenn Sie ein Dialogfeld sehen, in dem Sie aufgefordert werden, den Computer neu zu starten, klicken Sie auf **OK**.
8. Klicken Sie im Dialogfeld **System Eigenschaften** auf **Schließen**, und wenn ein Dialogfeld angezeigt wird, in dem Sie aufgefordert werden, den Computer neu zu starten, klicken Sie auf **jetzt neu starten**.
9. Melden Sie sich nach dem Neustart des Computers als corp\user1 an.

# Schritt 4 App1 konfigurieren

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Konfigurieren Sie die statische IPv6-Adressierung und die Gateweyeinstellungen, um App1 den Zugriff auf das Subnetz 2-Corpnet zu aktivieren

- So konfigurieren Sie das Standard Gateway und den DNS-Server Bei der Konfiguration für mehrere Standorte wird der Computer ROUTER1 als Standard Gateway verwendet. Konfigurieren Sie das Standard Gateway auf App1.

## So konfigurieren Sie das Standard Gateway und den DNS-Server

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **verkabelte Ethernet-Verbindung** auf den Link.
2. Klicken Sie im Fenster **Netzwerkverbindungen** mit der rechten Maustaste auf **verkabelte Ethernet-Verbindung**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften für verkabelte Ethernet-Verbindung** auf **Internet Protokoll Version 4 (TCP/IPv4)** , und klicken Sie dann auf **Eigenschaften**.
4. Geben Sie im **Standard Gateway** 10.0.0.254 ein, und geben Sie in **Alternativer DNS-Server** 10.2.0.1 bisein, und klicken Sie dann auf **OK**.
5. Klicken Sie im Dialogfeld **Eigenschaften für verkabelte Ethernet-Verbindung** auf **Internet Protokoll Version 6 (TCP/IPv6)** , und klicken Sie dann auf **Eigenschaften**.
6. Geben Sie unter **Standard Gateway** den Wert 2001: db8:1:: FE ein. Geben Sie im alternativen **DNS-Server** 2001: db8:2:: 1 ein, und klicken Sie dann auf **OK**.
7. Klicken Sie im Dialogfeld **Eigenschaften für verkabelte Ethernet-Verbindung** auf **Schließen**, und schließen Sie dann das Fenster **Netzwerkverbindungen** .

# Schritt 5 DC1 konfigurieren

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

DC1 fungiert als Domänen Controller, DNS-Server und DHCP-Server für die Corp.contoso.com-Domäne.

Um den Remote Zugriff für die Verwendung einer Topologie mit mehreren Standorten zu konfigurieren, müssen Sie einen zusätzlichen Active Directory Domain Services (AD DS)-Standort für den zweiten Domänen Controller 2 DC1 hinzufügen und das Routing zwischen den Subnetzen konfigurieren.

1. Zum Konfigurieren des Standard Gateways auf dem Domänen Controller. Konfigurieren Sie das Standard Gateway auf DC1.
2. Erstellen Sie Sicherheitsgruppen für DirectAccess-Clients unter Windows 7 auf DC1. Wenn DirectAccess konfiguriert ist, werden automatisch Gruppenrichtlinie Objekte (GPOs) und GPO-Einstellungen erstellt, die auf DirectAccess-Clients und-Server angewendet werden. Das DirectAccess-Client-GPO wird auf bestimmte Active Directory Sicherheitsgruppen angewendet.
3. Zum Hinzufügen einer neuen AD DS Website. Erstellen Sie eine zweite AD DS Website.

## So konfigurieren Sie das Standard Gateway auf dem Domänen Controller

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **verkabelte Ethernet-Verbindung** auf den Link.
2. Klicken Sie im Fenster Netzwerkverbindungen mit der rechten Maustaste auf **verkabelte Ethernet-Verbindung**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)**, und klicken Sie dann auf **Eigenschaften**.
4. Geben Sie im **Standard Gateway** 10.0.0.254 ein, und geben Sie in **Alternativer DNS-Server** 10.2.0.1 **bis** ein, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)**, und klicken Sie dann auf **Eigenschaften**.
6. Geben Sie im **Standard Gateway** 2001: db8:1:: FE ein, und geben Sie auf dem **alternativen DNS-Server** 2001: db8:2:: 1 ein, und klicken Sie dann auf **OK**.
7. Klicken Sie im Dialogfeld **Eigenschaften für verkabelte Ethernet-Verbindung** auf **Schließen**.
8. Schließen Sie das Fenster **Netzwerkverbindungen**.

## Erstellen von Sicherheitsgruppen für Windows 7-DirectAccess-Clients auf DC1

Erstellen Sie die DirectAccess-Sicherheitsgruppen für Windows 7 mit dem folgenden Verfahren.

Windows 7-Client Computer müssen Mitglieder von separaten Sicherheitsgruppen sein, da Sie nur über einen einzigen Einstiegspunkt eine Verbindung mit internen Ressourcen herstellen können. Wenn beim Aktivieren der Unterstützung für mehrere Standorte oder beim Hinzufügen von Einstiegspunkten eine Windows 7-Unterstützung angefordert wird, wird von DirectAccess für Windows 7-Clients für jeden Einstiegspunkt automatisch ein separates

GPO erstellt.

### **Erstellen von Sicherheitsgruppen**

1. Geben Sie auf dem **Start BildschirmDSA**. mscein, und drücken Sie dann die EINGABETASTE.
2. Erweitern Sie im linken Bereich **Corp.contoso.com**, klicken Sie auf **Benutzer**, klicken Sie dann mit der rechten Maustaste auf **Benutzer**, zeigen Sie auf **neu**, und klicken Sie dann auf **Gruppe**.
3. Geben Sie im Dialogfeld **Neues Objekt-Gruppe** unter **Gruppenname** den Namen **Win7\_Clients\_Site1** ein.
4. Klicken Sie unter **Gruppenbereich** auf **Global**, unter **Gruppentyp** auf **Sicherheit** und anschließend auf **OK**.
5. Doppelklicken Sie auf die **Win7\_Clients\_Site1** Sicherheitsgruppe, und klicken Sie im Dialogfeld **Win7\_Clients\_Site1 Eigenschaften** auf die Registerkarte **Mitglieder**.
6. Auf der Registerkarte **Mitglieder** klicken Sie auf **Hinzufügen**.
7. Klicken Sie im Dialogfeld **Benutzer, Kontakte, Computer oder Dienst Konten auswählen** auf **Objekttypen**. Wählen Sie im Dialogfeld **Objekttypen** die Option **Computer** aus, und klicken Sie dann auf **OK**.
8. Geben Sie im Feld **Geben Sie die zu ausgewählenden Objektnamen ein** den Namen **client2ein**, klicken Sie dann auf **OK**, und klicken Sie dann im Dialogfeld **Win7\_Clients\_Site1 Eigenschaften** auf **OK**.
9. Klicken Sie in der Konsole **Active Directory Benutzer und Computer** im linken Bereich mit der rechten Maustaste auf **Benutzer**, zeigen Sie auf **neu**, und klicken Sie dann auf **Gruppe**.
10. Geben Sie im Dialogfeld **Neues Objekt-Gruppe** unter **Gruppenname** den Namen **Win7\_Clients\_Site2** ein.
11. Klicken Sie unter **Gruppenbereich** auf **Global**, unter **Gruppentyp** auf **Sicherheit** und anschließend auf **OK**.
12. Schließen Sie die Konsole **Active Directory-Benutzer und -Computer**.

### **So fügen Sie eine neue AD DS Site hinzu**

1. Geben Sie auf dem **Start Bildschirmdssite**. mscein, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie in der Konsole Active Directory Standorte und Dienste in der Konsolen Struktur mit der rechten Maustaste auf **Standorte**, und klicken Sie dann auf **neuer Standort**.
3. Geben Sie im Dialogfeld **Neues Objekt-Standort** im Feld **Name** den Namen **Second-Site** ein.
4. Klicken Sie im Listenfeld auf **DEFAULTIPSITELINK**, und klicken Sie dann zweimal auf **OK**.
5. Erweitern Sie in der Konsolen Struktur **Standorte**, klicken Sie mit der rechten Maustaste auf **Subnetze**, und klicken Sie dann auf **Neues Subnetz**.
6. Geben Sie im Dialogfeld **Neues Objekt-Subnetz** unter **Präfix** **10.0.0.0/24** ein, klicken Sie in der Liste **Wählen Sie ein Standort Objekt für dieses Präfix aus** auf **Default-First-Site-Name**, und klicken Sie dann auf **OK**.
7. Klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf **Subnetze**, und klicken Sie dann auf **Neues Subnetz**.
8. Geben Sie im Dialogfeld **Neues Objekt-Subnetz** unter **Präfix** Folgendes ein: **2001: db8:1::/64**, klicken Sie in der Liste **Wählen Sie ein Standort Objekt für dieses Präfix aus** auf **Default-First-Site-Name**, und

klicken Sie dann auf **OK**.

9. Klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf **Subnetze**, und klicken Sie dann auf **Neues Subnetz**.
10. Geben Sie im Dialogfeld **Neues Objekt-Subnetz** unter **Präfix** **10.2.0.0/24** ein, klicken Sie in der Liste **Wählen Sie ein Standort Objekt für dieses Präfix aus** auf **zweiter Standort**, und klicken Sie dann auf **OK**.
11. Klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf **Subnetze**, und klicken Sie dann auf **Neues Subnetz**.
12. Geben Sie im Dialogfeld **Neues Objekt-Subnetz** unter **Präfix** Folgendes ein: **2001: db8:2::/64**, klicken Sie in der Liste **Wählen Sie ein Standort Objekt für dieses Präfix aus** auf **zweiter Standort**, und klicken Sie dann auf **OK**.
13. Schließen Sie Active Directory Websites und Dienste.

# Schritt 6: Installieren und Konfigurieren von 2-DC1

09.04.2020 • 14 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

2 DC1 stellt die folgenden Dienste bereit:

- Ein Domänen Controller für die Domäne corp2.Corp.contoso.com Active Directory Domain Services (AD DS).
- Einen DNS-Server für die DNS-Domäne corp2.Corp.contoso.com.

2: die DC1-Konfiguration besteht aus folgendem:

- Installieren des Betriebssystems auf 2-DC1
- Konfigurieren von TCP/IP-Eigenschaften
- Konfigurieren von 2 DC1 als Domänen Controller und DNS-Server
- Geben Sie Gruppenrichtlinie Berechtigungen für corp\user1 an.
- CORP2 Computern das Abrufen von Computer Zertifikaten gestatten
- Erzwingen der Replikation zwischen DC1 und 2-DC1

## Installieren des Betriebssystems auf 2-DC1

Installieren Sie zunächst Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.

### So installieren Sie das Betriebssystem auf 2-DC1

1. Starten Sie die Installation von Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.
2. Befolgen Sie die Anweisungen, um die Installation abzuschließen, indem Sie Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 (vollständige Installation) und ein sicheres Kennwort für das lokale Administrator Konto angeben. Melden Sie sich mit dem lokalen Administratorkonto an.
3. Verbinden Sie 2 DC1 mit einem Netzwerk, das über Internet Zugriff verfügt, und führen Sie Windows Update aus, um die neuesten Updates für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 zu installieren, und trennen Sie dann die Verbindung mit dem Internet.
4. Verbinden Sie 2 DC1 mit dem Subnetz 2-Corpnet.

## Konfigurieren von TCP/IP-Eigenschaften

Konfigurieren Sie das TCP/IP-Protokoll mit statischen IP-Adressen.

### So konfigurieren Sie TCP/IP auf 2 DC1

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **verkabelte Ethernet-Verbindung** auf den Link.
2. Klicken Sie unter **Netzwerkverbindungen** mit der rechten Maustaste auf **Verkabelte Ethernetverbindung**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie unter **IP-Adressen** den Namen **10.2.0.1**

bisein. Geben Sie im Feld **Subnetzmaske** den Wert 255.255.255.0 ein. Geben Sie unter **Standard Gateway** den Namen 10.2.0.254 ein. Klicken Sie auf **folgende DNS-Serveradressen verwenden**, geben Sie unter **Bevorzugter DNS-Server** den Namen 10.2.0.1 bisein, und geben Sie in **Alternativer DNS-Server** 10.0.0.1 ein.

5. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
6. Geben Sie unter **DNS-Suffix für diese Verbindung** corp2.Corp.contoso.com ein, und klicken Sie dann zweimal auf **OK**.
7. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)**, und klicken Sie dann auf **Eigenschaften**.
8. Klicken Sie auf **folgende IPv6-Adresse verwenden**. Geben Sie in der **IPv6-Adresse** 2001: db8:2:: 1 ein. Geben Sie unter **Subnetzpräfix-Länge** den Wert 64 ein. Geben Sie unter **Standard Gateway** den Wert 2001: db8:2:: FE ein. Klicken Sie auf **folgende DNS-Serveradressen verwenden**, geben Sie unter **Bevorzugter DNS-Server** den Namen 2001: db8:2:: 1 ein, und geben Sie im **alternativen DNS-Server** 2001: db8:1:: 1 ein.
9. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
10. Geben Sie unter **DNS-Suffix für diese Verbindung** corp2.Corp.contoso.com ein, und klicken Sie dann zweimal auf **OK**.
11. Klicken Sie im Dialogfeld **Eigenschaften für verkabelte Ethernet-Verbindung** auf **Schließen**.
12. Schließen Sie das Fenster **Netzwerkverbindungen**.
13. Klicken Sie in der Server-Manager Konsole unter **lokaler Server** im Bereich **Eigenschaften** neben **Computer Name** auf den Link.
14. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
15. Geben Sie im Dialogfeld **Computername/Domänen Änderungen** unter **Computername** den Namen 2-DC1 ein, und klicken Sie dann auf **OK**.
16. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
17. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
18. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.
19. Melden Sie sich nach dem Neustart mit dem lokalen Administrator Konto an.

## Konfigurieren von 2 DC1 als Domänen Controller und DNS-Server

Konfigurieren Sie 2 DC1 als Domänen Controller für die corp2.Corp.contoso.com-Domäne und als DNS-Server für die corp2.Corp.contoso.com DNS-Domäne.

### So konfigurieren Sie 2 DC1 als Domänen Controller und DNS-Server

1. Klicken Sie in der Server-Manager-Konsole auf dem **Dashboard** auf **Rollen und Features hinzufügen**.
2. Klicken Sie dreimal auf **weiter**, um zum Bildschirm für die Server Rollenauswahl zu gelangen.
3. Wählen Sie auf der Seite **Server Rollen auswählen** die Option **Active Directory Domain Services** aus. Klicken Sie bei entsprechender Aufforderung auf **Features hinzufügen**, und klicken Sie dann dreimal auf **weiter**.
4. Klicken Sie auf der Seite **Installationsauswahl bestätigen** auf **Installieren**.
5. Wenn die Installation erfolgreich abgeschlossen wurde, klicken Sie auf **Server zu einem Domänen Controller** herauf Stufen.

6. Klicken Sie im Konfigurations-Assistenten für Active Directory Domain Services auf der Seite **Bereitstellungs Konfiguration** auf **neue Domäne einer vorhandenen Gesamtstruktur hinzufügen**.
7. Geben Sie unter Name der über **geordneten Domäne Corp.contoso.com** ein, geben Sie unter **neuer Domänen Name** den Namen **corp2** ein.
8. Klicken Sie unter Geben Sie die **Anmelde Informationen an, um diesen Vorgang auszuführen**, auf **ändern**. Geben Sie im Dialogfeld **Windows-Sicherheit** unter **Benutzername** den Namen **Corp Configuration**. com\administrator ein, und geben Sie im Feld **Kennwort** das Kennwort **corp\administrator** ein, klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.
9. Vergewissern Sie sich auf der Seite **Domänen Controller Optionen**, dass der **Name des Standorts** auf der **zweiten Seite** liegt. Geben Sie unter **Kennwort** und **Kennwort bestätigen** ein Kennwort für den **Verzeichnisdienst-Wiederherstellungs Modus (DSRM-Kennwort)** ein, und klicken Sie dann zweimal auf **weiter**.
10. Klicken Sie nach der Überprüfung der Voraussetzungen auf der Seite **Voraussetzungen Prüfung** auf **Installieren**.
11. Warten Sie, bis der Assistent die Konfiguration von Active Directory und DNS-Diensten abgeschlossen hat, und klicken Sie dann auf **Schließen**.
12. Nachdem der Computer neu gestartet wurde, melden Sie sich mit dem Administrator Konto bei der CORP2-Domäne an.

## Geben Sie Gruppenrichtlinie Berechtigungen für corp\user1 an.

Verwenden Sie dieses Verfahren, um den Benutzer "corp\user1" mit vollen Berechtigungen zum Erstellen und Ändern von corp2-Gruppenrichtlinie Objekten bereitzustellen.

### So geben Sie Gruppenrichtlinie Berechtigungen an

1. Geben Sie auf dem **Start Bildschirm GPMC**. mscein, und drücken Sie dann die **EINGABETASTE**.
2. Öffnen Sie in der Gruppenrichtlinie-Verwaltungskonsole die Struktur "**Forest: Corp.contoso.com/Domains/corp2.Corp.contoso.com**".
3. Klicken Sie im Detailbereich auf die Registerkarte **Delegierung**. Klicken Sie in der Dropdown Liste **Berechtigung** auf Gruppenrichtlinien Objekte **Verknüpfen**.
4. Klicken Sie auf **Hinzufügen**, und klicken Sie im Dialogfeld **Neuer Benutzer, Computer oder Gruppe auswählen** auf **Speicher Orte**.
5. Klicken Sie im Dialogfeld **Speicher Orte** in der Struktur **Speicherort** auf **Corp.contoso.com**, und klicken Sie dann auf **OK**.
6. Klicken Sie im Feld **Geben Sie den Namen des zu ausgewählenden Objekts** ein **User1** auf **OK**, und klicken Sie im Dialogfeld **Gruppe oder Benutzer hinzufügen** auf **OK**.
7. Klicken Sie in der Gruppenrichtlinie-Verwaltungskonsole in der Struktur auf **Objekte Gruppenrichtlinie**, und klicken Sie im Detailbereich auf die Registerkarte **Delegierung**.
8. Klicken Sie auf **Hinzufügen**, und klicken Sie im Dialogfeld **Neuer Benutzer, Computer oder Gruppe auswählen** auf **Speicher Orte**.
9. Klicken Sie im Dialogfeld **Speicher Orte** in der Struktur **Speicherort** auf **Corp.contoso.com**, und klicken Sie dann auf **OK**.
10. Klicken Sie in **Geben Sie den Namen des zu ausgewählten Objekts** ein **User1** auf **OK**.

11. Klicken Sie in der Gruppenrichtlinie-Verwaltungskonsole in der Struktur auf **WMI-Filter**, und klicken Sie im Detailbereich auf die Registerkarte **Delegierung**.
12. Klicken Sie auf **Hinzufügen**, und klicken Sie im Dialogfeld **Neuer Benutzer, Computer oder Gruppe auswählen** auf Speicher Orte.
13. Klicken Sie im Dialogfeld **Speicher Orte** in der Struktur **Speicherort** auf **Corp.contoso.com**, und klicken Sie dann auf **OK**.
14. Klicken Sie in **Geben Sie den Namen des zu ausgewählten Objekts** ein **User1** auf **OK**. Vergewissern Sie sich, dass im Dialogfeld **Gruppe oder Benutzer hinzufügen** die Berechtigungen auf **vollZugriff** festgelegt sind, und klicken Sie dann auf **OK**.
15. Schließen Sie die Gruppenrichtlinien-Verwaltungskonsole.

## CORP2 Computern das Abrufen von Computer Zertifikaten gestatten

Computer in der CORP2-Domäne müssen Computer Zertifikate von der Zertifizierungsstelle auf App1 abrufen. Führen Sie dieses Verfahren auf App1 aus.

### **So ermöglichen Sie CORP2-Computern das automatische Abrufen von Computer Zertifikaten**

1. Klicken Sie auf App1 auf **Start**, geben Sie **certtmpl. mscein**, und drücken Sie dann die EINGABETASTE.
2. Doppelklicken Sie in der **Zertifikat Vorlagen Konsole** im mittleren Bereich auf **Client-Server-Authentifizierung**.
3. Klicken Sie im Dialogfeld **Eigenschaften von Client-Server-Authentifizierung** auf die Registerkarte **Sicherheit**.
4. Klicken Sie auf **Hinzufügen**, und klicken Sie im Dialogfeld **Benutzer, Computer, Dienst Konten oder Gruppen auswählen** auf Speicher Orte.
5. Erweitern Sie im Dialogfeld **Speicher Orte** unter **Speicherort** die Option **Corp.contoso.com**, klicken Sie auf **corp2.Corp.contoso.com**, und klicken Sie dann auf **OK**.
6. Geben Sie unter **Geben Sie die zuentwerfbaren Objektnamen ein** die Zeichen **Domäne Admins Domänen Computer**, und klicken Sie dann auf **OK**.
7. Klicken Sie im Dialogfeld **Eigenschaften von Client-Server-Authentifizierung** unter **Gruppen-oder Benutzernamenauf Domänen-Admins (CORP2\Domain Admins)**, und wählen Sie in **Berechtigungen für Domänen Administratoren** in der Spalte **zulassen** die Option **Schreiben** und **Anmelden** aus.
8. Klicken Sie unter **Gruppen-oder Benutzernamenauf Domänen Computer (CORP2\Domain-Computer)**, und wählen Sie unter **Berechtigungen für Domänen Computer** in der Spalte **zulassen** die Option **registrieren und automatisch registrieren** aus, und klicken Sie dann auf **OK**.
9. Schließen Sie die Zertifikatvorlagenkonsole.

## Erzwingen der Replikation zwischen DC1 und 2-DC1

Bevor Sie sich für Zertifikate bei 2 Edge1 registrieren können, müssen Sie die Replikation von Einstellungen von DC1 zu 2-DC1 erzwingen. Dieser Vorgang sollte auf DC1 ausgeführt werden.

### **Erzwingen der Replikation**

1. Klicken Sie auf DC1 auf **Start**, und klicken Sie dann auf **Active Directory Websites und Dienste**.
2. Erweitern Sie in der Konsole **Active Directory Standorte und Dienste** in der Struktur **standortübergreifende Transporte**, und klicken Sie dann auf **IP**.

3. Doppelklicken Sie im Detailbereich auf **DEFAULTIPSITELINK**.
4. Geben Sie im Dialogfeld **DEFAULTIPSITELINK-Eigenschaften** unter **Kosten** den Text **1** ein, geben Sie in **Replizieren** alle den Typ **15** ein, und klicken Sie dann auf **OK**. Warten Sie 15 Minuten, bis die Replikation abgeschlossen ist.
5. Um die Replikation jetzt in der Konsolen Struktur zu erzwingen, erweitern Sie **Sites\Default-First-Site-name\servers\dc1\ntds Settings**, klicken Sie im Detailbereich mit der rechten Maustaste auf , klicken Sie auf **Jetzt replizieren**, und klicken Sie dann im Dialogfeld **Jetzt replizieren** auf **OK**.
6. Gehen Sie folgendermaßen vor, um eine erfolgreiche Replikation sicherzustellen:
  - a. Geben Sie auf dem **Start** Bildschirm **cmd. exe** ein, und drücken Sie dann die EINGABETASTE.
  - b. Geben Sie den folgenden Befehl ein, und drücken Sie dann die EINGABETASTE.

```
repadmin /syncall /e /A /P /d /q
```

- c. Stellen Sie sicher, dass alle Partitionen ohne Fehler synchronisiert werden. Wenn nicht, führen Sie den Befehl erneut aus, bis keine Fehler gemeldet werden, bevor Sie den Vorgang fortsetzen.
7. Schließen Sie das Eingabeaufforderungsfenster.

# Schritt 7: Installieren und Konfigurieren von 2-App1

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

2 App1 stellt Web-und Dateifreigabe Dienste bereit. 2: die App1-Konfiguration besteht aus folgendem:

- Installieren des Betriebssystems auf 2-App1
- Konfigurieren von TCP/IP-Eigenschaften
- Join 2 App1 zur CORP2-Domäne
- Installieren Sie die Rolle "Webserver (IIS)" auf 2 App1
- Erstellen eines freigegebenen Ordners auf 2-App1

## Installieren des Betriebssystems auf 2-App1

Installieren Sie zunächst Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.

### So installieren Sie das Betriebssystem auf 2-App1

1. Starten Sie die Installation von Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 (vollständige Installation).
2. Folgen Sie den Installationsanweisungen, und legen Sie ein sicheres Kennwort für das lokale Administratorkonto fest. Melden Sie sich mit dem lokalen Administratorkonto an.
3. Verbinden Sie 2 App1 mit einem Netzwerk, das über Internet Zugriff verfügt, und führen Sie Windows Update aus, um die neuesten Updates für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 zu installieren, und trennen Sie dann die Verbindung mit dem Internet.
4. Verbinden Sie 2 App1 mit dem Subnetz 2-Corpnet.

## Konfigurieren von TCP/IP-Eigenschaften

Konfigurieren Sie die TCP/IP-Eigenschaften für 2 App1.

### So konfigurieren Sie die TCP/IP-Eigenschaften

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **verkabelte Ethernet-Verbindung** auf den Link.
2. Klicken Sie im Fenster **Netzwerkverbindungen** mit der rechten Maustaste auf **verkabelte Ethernet-Verbindung**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie unter **IP-Adresse** den Namen **10.2.0.3** ein. Geben Sie im Feld **Subnetzmaske** den Wert **255.255.255.0** ein. Geben Sie unter **Standard Gateway** den Namen **10.2.0.254** ein.
5. Klicken Sie auf **Folgende DNS-Serveradressen verwenden**. Geben Sie unter **Bevorzugter DNS-Server** **10.2.0.1** ein.
6. Klicken Sie auf **erweitert**, und klicken Sie dann auf die Registerkarte **DNS**. Geben Sie unter **DNS-Suffix**

für diese Verbindung corp2.Corp.contoso.com ein, und klicken Sie zweimal auf OK .

7. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)** , und klicken Sie dann auf **Eigenschaften**.
8. Klicken Sie auf **folgende IPv6-Adresse verwenden**. Geben Sie in der **IPv6-Adresse** 2001: db8:2:: 3 ein. Geben Sie unter **Subnetzpräfix-Länge** den Wert 64 ein. Geben Sie unter **Standard Gateway** den Wert 2001: db8:2:: FEEin. Klicken Sie auf **folgende DNS-Serveradressen verwenden**, und geben Sie unter **Bevorzugter DNS-Server** 2001: db8:2:: 1 ein.
9. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
10. Geben Sie unter **DNS-Suffix für diese Verbindung** corp2.Corp.contoso.com ein, und klicken Sie dann zweimal auf OK .
11. Klicken Sie im Dialogfeld **Eigenschaften für verkabelte Ethernet-Verbindung** auf **Schließen**.
12. Schließen Sie das Fenster **Netzwerkverbindungen**.

## Join 2 App1 zur CORP2-Domäne

Join 2 App1 zur corp2.Corp.contoso.com-Domäne.

### **So verknüpfen Sie 2 App1 mit der CORP2-Domäne**

1. Klicken Sie in der Server-Manager Konsole unter **lokaler Server** im Bereich **Eigenschaften** neben **Computer Name** auf den Link.
2. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
3. Geben Sie unter **Computer Name** den Namen 2-App1 ein. Klicken Sie unter **Mitglied von** auf **Domäne**, geben Sie corp2.Corp.contoso.com ein, und klicken Sie dann auf **OK**.
4. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie **Administrator** und Kennwort ein, und klicken Sie dann auf **OK**.
5. Wenn ein Dialogfeld angezeigt wird, in dem Sie zur Domäne corp2.Corp.contoso.com Willkommen werden, klicken Sie auf **OK**.
6. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
7. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
8. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.
9. Klicken Sie nach dem Neustart des Computers auf **Benutzer wechseln** und dann auf **anderer Benutzer** , und melden Sie sich bei der Domäne CORP2 mit dem Administrator Konto an.

## Installieren Sie die Rolle "Webserver (IIS)" auf 2 App1

Installieren Sie die Rolle "Webserver (IIS)", um "2 App1 a Web Server" zu erstellen.

### **So installieren Sie die Rolle "Webserver (IIS)"**

1. Klicken Sie in der Server-Manager-Konsole auf dem **Dashboard** auf **Rollen und Features hinzufügen**.
2. Klicken Sie dreimal auf **weiter** , um zum Bildschirm für die Server Rollenauswahl zu gelangen.
3. Wählen Sie auf der Seite **Server Rollen auswählen** die Option **Webserver (IIS)** aus, und klicken Sie dann vier Mal auf **weiter** .
4. Klicken Sie auf der Seite **Installationsauswahl bestätigen** auf **Installieren**.
5. Überprüfen Sie, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.

# Erstellen eines freigegebenen Ordners auf 2-App1

Erstellen Sie einen freigegebenen Ordner und eine Textdatei im Ordner auf 2 App1.

## So erstellen Sie einen freigegebenen Ordner

1. Geben Sie auf dem **Start BildschirmExplorer**. exeein, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie auf **Computer**, und doppelklicken Sie dann auf lokaler Datenträger (C:) .
3. Klicken Sie auf **neuer Ordner**, geben Sie Dateienein, und drücken Sie die EINGABETASTE. Lassen Sie das Fenster **lokaler Datenträger** geöffnet.
4. Geben Sie im **Start BildschirmNotepad**. exeein, klicken Sie mit der rechten Maustaste auf **Notepad**, klicken Sie auf **erweitert**, und klicken Sie dann auf **als Administrator ausführen**.
5. Geben Sie im Fenster " **unbenanntes Notepad** " eine freigegebene Datei in "2-App1" ein.
6. Klicken Sie auf **Datei**, klicken Sie auf **Speichern**, klicken Sie auf **Computer**, doppelklicken Sie auf lokaler Datenträger (C:) , und doppelklicken Sie dann auf den Ordner **Dateien** .
7. Geben Sie unter **Dateiname die Bezeichnung example. txtein**, und klicken Sie dann auf **Speichern**. Schließen Sie Editor.
8. Klicken Sie im Fenster **lokaler Datenträger** mit der rechten Maustaste auf den Ordner **Dateien** , zeigen Sie auf **Freigabenfür**, und klicken Sie dann auf **bestimmte Personen**.
9. Klicken Sie im Dialogfeld **Dateifreigabe** in der Dropdown Liste auf **alle**, und klicken Sie dann auf **Hinzufügen**. Klicken Sie in **Berechtigungsstufe** für alle auf **Lesen/Schreiben**.
10. Klicken Sie auf **Freigeben** und dann auf **done**.
11. Schließen Sie das Fenster **lokaler Datenträger**.

# SCHRITT 8: Konfigurieren von INET1

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Damit Client Computer eine Verbindung mit RAS-Servern über das Internet herstellen können, müssen Sie einen DNS-Eintrag für 2-Edge1 auf INET1 konfigurieren.

## So erstellen Sie den 2 Edge1-DNS-Eintrag

1. Geben Sie auf der Start Seite **dnsmgmt.msc**, und drücken Sie dann die EINGABETASTE.
2. Öffnen Sie in der Konsolen Struktur **Forward-Lookupzonen**, klicken Sie auf **contoso.com**, klicken Sie mit der rechten Maustaste auf **contoso.com**, und klicken Sie dann auf **neuer Host (A oder AAAA)**.
3. Geben Sie unter **Name** den Namen **2-Edge1** ein. Geben Sie unter **IP-Adresse** den Namen **131.107.0.20** ein. Klicken Sie auf **Host hinzufügen**, klicken Sie auf **OK**, und klicken Sie dann auf **Fertig**.

# Schritt 9 Edge1 konfigurieren

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die folgenden Prozeduren werden auf dem Edge1-Server ausgeführt:

1. Konfigurieren Sie die DNS-Server auf Edge1. Es ist erforderlich, den DNS-Server in der corp2.Corp.contoso.com-Domäne auf Edge1 zu konfigurieren.
2. Konfigurieren Sie das Routing zwischen Subnetzen. Konfigurieren Sie das Routing auf Edge1, um die Kommunikation zwischen den Subnetzen Corpnet und 2-Corpnet zu ermöglichen.

## Konfigurieren der DNS-Server auf Edge1

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **Corpnet** auf den Link.
2. Klicken Sie im Fenster Netzwerkverbindungen mit der rechten Maustaste auf **Corpnet**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)**, und klicken Sie dann auf **Eigenschaften**.
4. Geben Sie im **alternativen DNS-Server** 10.2.0.1 **bis ein**, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)**, und klicken Sie dann auf **Eigenschaften**.
6. Geben Sie im **alternativen DNS-Server** 2001: db8:2:: 1 **ein**, und klicken Sie dann auf **OK**.
7. Klicken Sie im Dialogfeld **Corpnet-Eigenschaften** auf **Schließen**.
8. Schließen Sie das Fenster **Netzwerkverbindungen**.

## Konfigurieren des Routings zwischen Subnetzen

1. Geben Sie im **Start Bildschirmcmd. exeein**, klicken Sie mit der rechten Maustaste auf **cmd**, klicken Sie auf **erweitert**, und klicken Sie dann auf **als Administrator ausführen**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Geben Sie im Eingabe Aufforderungs Fenster die folgenden Befehle ein. Drücken Sie nach dem Eingeben der einzelnen Befehle die **EINGABETASTE**.

```
netsh interface IPv4 add route 10.2.0.0/24 Corpnet 10.0.0.254  
netsh interface IPv6 add route 2001:db8:2::/64 Corpnet 2001:db8:1::fe
```

3. Schließen Sie das Eingabeaufforderungsfenster.

# Schritt 10: Installieren und Konfigurieren von 2-Edge1

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

2: die Edge1-Konfiguration besteht aus folgendem:

- Installieren Sie das Betriebssystem auf 2 Edge1. Installieren Sie Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 auf 2 Edge1.
- Konfigurieren von TCP/IP-Eigenschaften Konfigurieren Sie 2 Edge1 mit statischen Adressen an beiden Netzwerkschnittstellen.
- Konfigurieren Sie das Routing zwischen Subnetzen. Um die Kommunikation zwischen den Subnetzen Corpnet und 2-Corpnet zu aktivieren, müssen Sie das Routing konfigurieren.
- Join 2 Edge1 zur CORP2-Domäne. Join 2 Edge1 zur corp2.Corp.contoso.com-Domäne.
- Beziehen Sie Zertifikate auf 2 Edge1. Zertifikate sind für die IPSec-Verbindung zwischen DirectAccess-Clients und dem RAS-Server erforderlich und zum Authentifizieren des IP-HTTPS-Listener, wenn Clients eine Verbindung über HTTPS herstellen.
- Gewähren des Zugriffs auf corp\user1. Der Benutzer corp\user1 ist der Remote Zugriffs Administrator. Damit dieser Benutzer Änderungen an 2 Edge1 von Edge1 aus vornehmen kann, müssen Sie dem Benutzer Zugriff erteilen.
- Installieren Sie die Remote Zugriffs Rolle auf 2 Edge1. Um eine Bereitstellung für mehrere Standorte zu aktivieren, müssen Sie die Remote Zugriffs Rolle auf 2 Edge1 installieren.

2 Edge1 es müssen zwei Netzwerkadapter installiert sein.

## Installieren des Betriebssystems auf 2-Edge1

1. Starten Sie die Installation von Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.
2. Befolgen Sie die Anweisungen, um die Installation abzuschließen, indem Sie Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 (vollständige Installation) und ein sicheres Kennwort für das lokale Administrator Konto angeben. Melden Sie sich mit dem lokalen Administratorkonto an.
3. Verbinden Sie 2 Edge1 mit einem Netzwerk, das über Internet Zugriff verfügt, und führen Sie Windows Update aus, um die neuesten Updates für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 zu installieren, und trennen Sie dann die Verbindung mit dem Internet.
4. Verbinden Sie einen Netzwerkadapter mit dem Subnetz 2-Corpnet und dem anderen mit dem simulierten Internet.

## Konfigurieren von TCP/IP-Eigenschaften

1. Klicken Sie in der Server-Manager Konsole auf **lokaler Server**, und klicken Sie dann im Bereich **Eigenschaften** neben **verkabelte Ethernet-Verbindung** auf den Link.
2. Klicken Sie unter **Netzwerkverbindungen** mit der rechten Maustaste auf die Netzwerkverbindung, die mit dem Subnetz 2-Corpnet verbunden ist, klicken Sie auf **Umbenennen**, geben Sie **2-Corpnet** ein, und drücken Sie die EINGABETASTE.

3. Klicken Sie mit der rechten Maustaste auf **2-Corpnet**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)** , und klicken Sie dann auf **Eigenschaften**.
5. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie in **IP-Adresse** 10.2.0.20 ein, geben Sie in **Subnetzmaske** 255.255.255.0 ein.
6. Klicken Sie auf **Folgende DNS-Serveradressen verwenden**. Geben Sie unter **Bevorzugter DNS-Server** 10.2.0.1 ein, und geben Sie in **Alternativer DNS-Server** 10.0.0.1 ein.
7. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
8. Geben Sie unter **DNS-Suffix für diese Verbindung** corp2.Corp.contoso.com ein, und klicken Sie dann zweimal auf **OK** .
9. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)** , und klicken Sie dann auf **Eigenschaften**.
10. Klicken Sie auf **folgende IPv6-Adresse verwenden**. Geben Sie in **IPv6-Adresse** 2001: db8:2:: 20, in **Subnetzpräfix-Längeden Wert** 64 ein. Klicken Sie auf **folgende DNS-Serveradressen verwenden**, und geben Sie unter **Bevorzugter DNS-Server** 2001: db8:2:: 1, auf dem **alternativen DNS-Server** den Namen 2001: db8:1:: 1 ein.
11. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
12. Geben Sie unter **DNS-Suffix für diese Verbindung** corp2.Corp.contoso.com ein, und klicken Sie dann zweimal auf **OK** .
13. Klicken Sie im Dialogfeld **Eigenschaften von 2 Corpnet** auf **Schließen**.
14. Klicken Sie im Fenster **Netzwerkverbindungen** mit der rechten Maustaste auf die Netzwerkverbindung, die mit dem Subnetz Internet verbunden ist, klicken Sie auf **Umbenennen**, geben Sie **Internetein**, und drücken Sie dann die EINGABETASTE.
15. Klicken Sie mit der rechten Maustaste auf **Internet**, und klicken Sie dann auf **Eigenschaften**.
16. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)** , und klicken Sie dann auf **Eigenschaften**.
17. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie unter **IP-Adresseden Namen** 131.107.0.20 ein. Geben Sie im Feld **Subnetzmaske** den Wert 255.255.255.0 ein.
18. Klicken Sie auf **Erweitert**. Klicken Sie auf der Registerkarte **IP-Einstellungen** im Bereich **IP-Adressen** auf **Hinzufügen**. Geben Sie im Dialogfeld **TCP/IP-Adresse** unter **IP-Adressentyp** 131.107.0.21 unter **Subnetzmaske** den Wert 255.255.255.0 ein, und klicken Sie dann auf **Hinzufügen**.
19. Klicken Sie auf die Registerkarte **DNS**.
20. Geben Sie unter **DNS-Suffix für diese Verbindung** ISP.example.com ein, klicken Sie zweimal auf **OK** , und klicken Sie dann auf **Schließen**.
21. Schließen Sie das Fenster **Netzwerkverbindungen**.

## Konfigurieren des Routings zwischen Subnetzen

1. Geben Sie auf dem **Start** Bildschirmcmd. exe ein, und drücken Sie dann die EINGABETASTE.
2. Geben Sie im Eingabe Aufforderungs Fenster die folgenden Befehle ein. Drücken Sie nach dem Eingeben der einzelnen Befehle die EINGABETASTE.

```
netsh interface IPv4 add route 10.0.0.0/24 2-Corpnet 10.2.0.254  
netsh interface IPv6 add route 2001:db8:1::/64 2-Corpnet 2001:db8:2::fe
```

3. Geben Sie **ping dc1.Corp.contoso.com** ein, um die Netzwerkkommunikation zwischen 2 Edge1 und DC1 zu überprüfen.
4. Stellen Sie sicher, dass vier Antworten von der IPv4-Adresse, 10.0.0.1 oder der IPv6-Adresse "2001: db8:1:: 1" vorhanden sind.
5. Schließen Sie das Eingabeaufforderungsfenster.

## Join 2 Edge1 zur CORP2-Domäne

1. Klicken Sie in der Server-Manager Konsole unter **lokaler Server** im Bereich **Eigenschaften** neben **Computer Name** auf den Link.
2. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
3. Geben Sie im Dialogfeld **Computername/Domänen Änderungen** unter **Computername** den Namen **2-Edge1** ein. Klicken Sie unter **Mitglied von** auf **Domäne**, geben Sie **corp2.Corp.contoso.com** ein, und klicken Sie dann auf **OK**.
4. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie **Administrator** und Kennwort ein, und klicken Sie dann auf **OK**.
5. Wenn ein Dialogfeld angezeigt wird, in dem Sie zur Domäne corp2.Corp.contoso.com Willkommen werden, klicken Sie auf **OK**.
6. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
7. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
8. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.
9. Klicken Sie nach dem Neustart des Computers auf **Benutzer wechseln** und dann auf **anderer Benutzer**, und melden Sie sich bei der Domäne CORP2 mit dem Administrator Konto an.

## Abrufen von Zertifikaten auf 2-Edge1

1. Geben Sie auf dem **Start** Bildschirm **MMC. exeein**, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-ins hinzufügen oder entfernen** auf **Zertifikate, Hinzufügen**, **Computerkonto, Weiter**, **Lokaler Computer, Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolen Struktur des Zertifikate-Snap-Ins den Bereich **Zertifikate (lokaler Computer) \persönlich**.
5. Klicken Sie mit der rechten Maustaste auf **persönlich**, zeigen Sie auf **alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
6. Klicken Sie zweimal auf **Weiter**.
7. Wählen Sie auf der Seite **Zertifikate anfordern** die Kontrollkästchen **Client-Server-Authentifizierung** und **Webserver** aus, und klicken Sie dann auf **Weitere Informationen sind erforderlich, um dieses Zertifikat zu registrieren**.
8. Wählen Sie im Dialogfeld **Zertifikat Eigenschaften** auf der **Registerkarte Antragsteller** im Bereich **Antragsteller Name** unter **Typ** den **Namen allgemeiner Name** aus.
9. Geben Sie **2-Edge1.contoso.com** in **value** ein, und klicken Sie dann auf **Hinzufügen**.
10. Wählen Sie unter **Alternativer Name** für **Typ** die Option **DNS** aus.

11. Geben Sie 2-Edge1.contoso.com in **value** ein, und klicken Sie dann auf **Hinzufügen**.
12. Geben Sie auf der Registerkarte **Allgemein** unter Anzeige **Name** den Namen **IP-HTTPS-Zertifikate** ein.
13. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
14. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, ob ein neues Zertifikat mit dem Namen 2-Edge1.contoso.com mit dem beabsichtigten Zweck der Server Authentifizierung registriert wurde und ein neues Zertifikat mit dem Namen 2-Edge1.corp2.Corp.contoso.com bei registriert wurde. Beabsichtigte Zwecke der Client Authentifizierung und Server Authentifizierung.
15. Schließen Sie das Konsolenfenster. Wenn Sie zum Speichern der Einstellungen aufgefordert werden, klicken Sie auf **Nein**.

## Gewähren des Zugriffs auf "corp\user1"

1. Geben Sie auf dem **Start** Bildschirm compmgmt. mscein, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie im linken Bereich auf **lokale Benutzer und Gruppen**.
3. Doppelklicken Sie auf **Gruppen**, und doppelklicken Sie dann auf **Administratoren**.
4. Klicken Sie im Dialogfeld **Administrator Eigenschaften** auf **Hinzufügen**, und klicken Sie im Dialogfeld **Benutzer, Computer, Dienst Konten oder Gruppen auswählen** auf **Speicher Orte**.
5. Klicken Sie im Dialogfeld **Speicher Orte** in der Struktur **Speicherort** auf **Corp.contoso.com**, und klicken Sie dann auf **OK**.
6. Geben Sie unter **Geben Sie die zu entwernenden Objektnamen** ein **User1** ein, und klicken Sie dann auf **OK**.
7. Klicken Sie im Dialogfeld **Administrator Eigenschaften** auf **OK**.
8. Schließen Sie das Fenster Computerverwaltung.

## Installieren der Remote Zugriffs Rolle auf 2 Edge1

1. Klicken Sie in der Server-Manager-Konsole im **Dashboard** auf **Rollen und Features hinzufügen**.
2. Klicken Sie dreimal auf **Weiter**, um zur Anzeige für die Serverrollenauswahl zu gelangen.
3. Auf der **Serverrollen auswählen** die Option **RAS** klicken Sie auf **Features hinzufügen** und klicken Sie dann auf **Weiter**.
4. Klicken Sie fünfmal auf **Weiter**.
5. Klicken Sie im Dialogfeld **Installationsauswahl bestätigen** auf **Installieren**.
6. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.

# Schritt 11 Konfigurieren der Bereitstellung für mehrere Standorte

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Um eine Bereitstellung für mehrere Standorte zu konfigurieren, nehmen Sie Änderungen am Assistenten für die Remote Zugriffs Konfiguration auf Edge1 vor, aktivieren Sie die Funktion für mehrere Standorte, und fügen Sie dann 2-Edge1 als zweiten Einstiegspunkt hinzu.

- Konfigurieren des Remote Zugriffs auf Edge1
- Aktivieren der Konfiguration für mehrere Standorte auf Edge1
- 2-Edge1 als zweiten Einstiegspunkt hinzufügen

## Konfigurieren des Remote Zugriffs auf Edge1

1. Geben Sie auf dem **Start Bildschirmramgmtui. exeein**, und drücken Sie dann die **EINGABETASTE**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remotezugriffs-Verwaltungskonsole auf **Konfiguration**.
3. Klicken Sie im mittleren Bereich der Konsole im Bereich **Schritt 2 RAS-Server** auf **Bearbeiten**.
4. Klicken Sie auf **Präfix Konfiguration**. Geben Sie auf der Seite **Präfix Konfiguration in interne Netzwerk-IPv6-Präfixe 2001: db8:1::/64; 2001: db8:2::/64ein**. Geben Sie im **IPv6-Präfix, das DirectAccess-Client Computern zugewiesen ist**, **2001: db8:1: 1000::/64ein**, klicken Sie auf **weiter** und dann auf **Fertigstellen**.
5. Klicken Sie im mittleren Bereich der Konsole im Bereich **Schritt 3 Infrastruktur Server** auf **Bearbeiten**.
6. Klicken Sie auf **DNS-Suffixsuchliste**. Vergewissern Sie sich, dass auf der Seite **DNS-Suffixsuchliste** das Kontrollkästchen **DirectAccess-Clients mit DNS-clientsuffixsuchliste konfigurieren** aktiviert ist und dass die Domänen **Suffixe Corp.contoso.com und corp2.Corp.contoso.com** in der Liste **zu verwendende Domänen Suffixe** angezeigt werden. Klicken Sie auf **weiter** und dann auf **Fertigstellen**.
7. Klicken Sie im mittleren Bereich der Konsole auf **Fertigstellen**.
8. Überprüfen Sie im Dialogfeld **Remote Zugriffs Überprüfung** die Konfigurationseinstellungen, und klicken Sie dann auf **übernehmen**. Klicken Sie im Dialogfeld **Anwenden der Einstellungen zum Einrichten des Remotezugriffs auf Schließen**.
9. Klicken Sie im Bereich **Tasks** auf **Verwaltungs Server aktualisieren**, und klicken Sie dann auf **Schließen**, wenn Sie fertig sind.

## Aktivieren der Konfiguration für mehrere Standorte auf Edge1

1. Klicken Sie in der Remote Zugriffs-Verwaltungskonsole im Bereich **Tasks** auf **Multisite aktivieren**.
2. Klicken Sie im Assistenten zum Aktivieren der Bereitstellung für mehrere Standorte auf der Seite **Vorbemerkungen** auf **weiter**.

3. Geben Sie auf der Seite **Bereitstellungs Name** unter **Name der Bereitstellung für mehrere Standorte** den Wert " Edge1-Site" ein, und klicken Sie dann auf **weiter**.
4. Klicken Sie auf der Seite **Einstiegspunkt Auswahl** auf **Einstiegspunkte automatisch zuweisen**, und aktivieren Sie die Option **Clients manuell auswählen**, und klicken Sie dann auf **weiter**.
5. Klicken Sie auf der Seite **Globaler Lastenausgleich** auf **Nein, verwenden Sie keinen globalen Lastenausgleich**, und klicken Sie dann auf **weiter**.
6. Klicken Sie auf der Seite **Client Unterstützung** auf **Client Computern, auf denen Windows 7 ausgeführt wird, auf diesen Einstiegspunkt zugreifen**, und klicken Sie auf **Hinzufügen**.
7. Geben Sie im Dialogfeld **Gruppen auswählen** unter **Geben Sie die zu ausgewählenden Objektnamenein** **Win7\_Clients\_Site1** ein, klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.
8. Klicken Sie auf der Seite **Einstellungen des Client -Gruppenrichtlinien Objekts** auf **weiter**.
9. Klicken Sie auf der Seite **Zusammenfassung** auf **Commit**.
10. Klicken Sie im Dialogfeld **Bereitstellung für mehrere Standorte** aktivieren auf **Schließen**, und klicken Sie dann im Assistenten zum Aktivieren der Bereitstellung für mehrere Standorte auf **Schließen**.

## 2-Edge1 als zweiten Einstiegspunkt hinzufügen

1. Klicken Sie in der Remote Zugriffs-Verwaltungskonsole im Bereich **Tasks** auf **Einstiegspunkt hinzufügen**.
2. Geben Sie im Assistenten zum Hinzufügen von Einstiegspunkten auf der Seite **Details zum Einstiegspunkt** unter **RAS- Server** den Namen **2-Edge1.corp2.Corp.contoso.com** ein, geben Sie unter **Einstiegspunkt Name** den Namen **2-Edge1-Site** ein, und klicken Sie dann auf **weiter**.
3. Klicken Sie auf der Seite **Netzwerktopologie** auf **Edge** und dann auf **weiter**.
4. Geben Sie auf der Seite **Netzwerkname oder IP-Adresse** unter **Geben Sie den öffentlichen Namen oder die IP-Adresse ein, die von Clients zum Herstellen einer Verbindung mit dem Remote Zugriffs Server verwendet wird**, **2-Edge1.contoso.com** ein, und klicken Sie dann auf **weiter**.
5. Vergewissern Sie sich auf der Seite **Netzwerkadapter**, dass der **externe Adapter Internet**, der **interne Adapter 2-Corpnet**, das Zertifikat **CN = 2-Edge1.contoso.com** ist, und klicken Sie dann auf **weiter**.
6. Geben Sie auf der Seite **Präfix Konfiguration** unter **IPv6-Präfix**, das **DirectAccess-Client Computern zugewiesen** ist Folgendes ein : **2001: db8:2: 2000::/64**, und klicken Sie dann auf **weiter**.
7. Klicken Sie auf der Seite **Client Unterstützung** auf **Client Computern, auf denen Windows 7 ausgeführt wird, auf diesen Einstiegspunkt zugreifen**, und klicken Sie auf **Hinzufügen**.
8. Geben Sie im Dialogfeld **Gruppen auswählen** unter **Geben Sie die zu ausgewählenden Objektnamenein** **Win7\_Clients\_Site2** ein, klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.
9. Klicken Sie auf der Seite **Einstellungen des Client -Gruppenrichtlinien Objekts** auf **weiter**.
10. Klicken Sie auf der Seite **Server-GPO-Einstellungen** auf **weiter**.
11. Klicken Sie auf der Seite **Zusammenfassung** auf **Commit**.
12. Klicken Sie im Dialogfeld **Einstiegspunkt hinzufügen** auf **Schließen**, und klicken Sie dann im Assistenten zum Hinzufügen von Einstiegspunkten auf **Schließen**.

# Schritt 12. Testen der DirectAccess-Konnektivität

09.04.2020 • 16 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Bevor Sie die Konnektivität von Client Computern testen können, wenn Sie sich im Internet oder in homenet-Netzwerken befinden, müssen Sie sicherstellen, dass Sie über die richtigen Gruppenrichtlinien Einstellungen verfügen.

- So überprüfen Sie, ob Clients die richtige Gruppenrichtlinie haben
- Testen der DirectAccess-Konnektivität über das Internet über Edge1
- Verschieben von CLIENT2 in die Sicherheitsgruppe Win7\_Clients\_Site2
- Testen der DirectAccess-Konnektivität über das Internet bis 2 Edge1

## Erforderliche Komponenten

Verbinden Sie beide Client Computer mit dem Netzwerk "Corpnet", und starten Sie beide Client Computer neu.

## Überprüfen, ob Clients über die richtige Gruppenrichtlinie verfügen

1. Klicken Sie auf CLIENT1 auf **Start**, geben Sie **PowerShell**. ein, klicken Sie mit der rechten Maustaste auf **PowerShell**, klicken Sie auf **erweitert** und dann auf **als Administrator ausführen**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Geben Sie im Windows PowerShell-Fenster **ipconfig** ein, und drücken Sie die EINGABETASTE.  
Stellen Sie sicher, dass die IPv4-Adresse des Corpnet-Adapters mit 10.0.0 beginnt.
3. Geben Sie im Windows PowerShell-Fenster **Get-dnsclientnrptpolicy** ein, und drücken Sie die EINGABETASTE. Die Einträge in der Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) für Direct Access werden angezeigt.
  - .Corp.contoso.com: Diese Einstellungen geben an, dass alle Verbindungen mit Corp.contoso.com von einem der DirectAccess-DNS-Server mit der IPv6-Adresse 2001: db8:1:: 2 oder 2001: db8:2:: 20 aufgelöst werden sollten.
  - NLS.Corp.contoso.com: Diese Einstellungen geben an, dass eine Ausnahme für den Namen nls.Corp.contoso.com vorliegt.
4. Lassen Sie das Windows PowerShell-Fenster für das nächste Verfahren geöffnet.
5. Klicken Sie auf CLIENT2 auf **Start**, **Alle Programme**, **Zubehör**, **Windows PowerShell**, klicken Sie mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie dann auf **als Administrator ausführen**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
6. Geben Sie im Windows PowerShell-Fenster **ipconfig** ein, und drücken Sie die EINGABETASTE.  
Stellen Sie sicher, dass die IPv4-Adresse des Corpnet-Adapters mit 10.0.0 beginnt.
7. Geben Sie im Windows PowerShell-Fenster **netsh Namespace Show Policy** ein, und drücken Sie die

## EINGABETASTE.

In der Ausgabe sollten zwei Abschnitte vorhanden sein:

- . Corp.contoso.com: Diese Einstellungen geben an, dass alle Verbindungen mit Corp.contoso.com vom DirectAccess-DNS-Server mit der IPv6-Adresse "2001: db8:1:: 2" aufgelöst werden sollen.
- NLS.Corp.contoso.com: Diese Einstellungen geben an, dass eine Ausnahme für den Namen nls.Corp.contoso.com vorliegt.

8. Lassen Sie das Windows PowerShell-Fenster für das nächste Verfahren geöffnet.

## Testen der DirectAccess-Konnektivität über das Internet über Edge1

1. UnPlug 2: Edge1 aus dem Internet Netzwerk.
2. Entfernen Sie CLIENT1 und CLIENT2 vom Corpnet-Switch, und verbinden Sie Sie mit dem Internet-Switch. Warten Sie 30 Sekunden.
3. Geben Sie auf CLIENT1 im Windows PowerShell-Fenster **ipconfig/all** ein, und drücken Sie die EINGABETASTE.
4. Überprüfen Sie die Ausgabe des Befehls "ipconfig".

Der Client Computer ist jetzt mit dem Internet verbunden und verfügt über eine öffentliche IPv4-Adresse. Wenn der DirectAccess-Client über eine öffentliche IPv4-Adresse verfügt, verwendet er die IPv6-Übergangs Technologien Teredo oder IP-HTTPS, um die IPv6-Nachrichten über ein IPv4-Internet zwischen dem DirectAccess-Client und dem Remote Zugriffs Server zu Tunneln. Beachten Sie, dass Teredo die bevorzugte Übergangstechnologie ist.

5. Geben Sie im Windows PowerShell-Fenster **ipconfig/flushdns** ein, und drücken Sie die EINGABETASTE. Dadurch werden namens Auflösungs Einträge geleert, die möglicherweise noch im Client-DNS-Cache vorhanden sind, wenn der Client Computer mit dem Unternehmensnetzwerk verbunden war.
6. Deaktivieren Sie die Teredo-Schnittstelle, um sicherzustellen, dass der Client Computer mit dem folgenden Befehl IP-HTTPS verwendet, um eine Verbindung mit Corpnet herzustellen:

```
netsh interface teredo set state disable
```

7. Stellen Sie sicher, dass Sie über Edge1 verbunden sind. Geben Sie **netsh interface httpstunnel Show Interfaces Show Interfaces** ein, und drücken Sie die EINGABETASTE.

Die Ausgabe sollte URL: <https://edge1.contoso.com:443/IPHTTSPsenthalten>.

### TIP

Auf CLIENT1 können Sie auch den folgenden Windows PowerShell-Befehl ausführen: **Get-nettiphttpsconfiguration**. In der Ausgabe werden die verfügbaren Server-URL-Verbindungen und das derzeit aktive Profil angezeigt.

8. Geben Sie im Windows PowerShell-Fenster **Ping App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse angezeigt werden, die App1 zugewiesen ist, in diesem Fall "2001: db8:1:: 3".
9. Geben Sie im Windows PowerShell-Fenster **Ping 2-App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse, die 2-App1 zugewiesen ist, angezeigt werden, in diesem Fall "2001: db8:2:: 3".
10. Geben Sie im Windows PowerShell-Fenster **Ping App2** ein, und drücken Sie die EINGABETASTE. Es sollten

Antworten von der NAT64-Adresse angezeigt werden, die von Edge1 zu APP2 zugewiesen wird. in diesem Fall lautet der Wert **FDC9:9f4e: eb1b: 7777:: A00:4**. Beachten Sie, dass die fett formatierten Werte variieren, weil die Adresse generiert wird.

Die Möglichkeit zum Ping-APP2 ist wichtig, da der Erfolg anzeigt, dass Sie eine Verbindung mithilfe von NAT64/DNS64 herstellen konnten, da APP2 eine reine IPv4-Ressource ist.

11. Öffnen Sie Internet Explorer, geben Sie in der Internet Explorer-Adressleiste **https://app1/** ein, und drücken Sie die EINGABETASTE. Die Standard-IIS-Website auf APP1 wird angezeigt.
12. Geben Sie in der Internet Explorer-Adressleiste **https://2-app1/** ein, und drücken Sie die EINGABETASTE. Die Standard Website wird unter 2-App1 angezeigt.
13. Geben Sie in der Internet Explorer-Adressleiste **https://app2/** ein, und drücken Sie die EINGABETASTE. Die Standardwebsite auf APP2 wird angezeigt.
14. Geben Sie auf dem **Start** Bildschirm\\2-app1\filesein, und drücken Sie dann die EINGABETASTE.  
Doppelklicken Sie auf die Beispiel Textdatei.  
  
Dadurch wird veranschaulicht, dass Sie eine Verbindung mit dem Dateiserver in der corp2.Corp.contoso.com-Domäne herstellen konnten, wenn eine Verbindung über Edge1 besteht.
15. Geben Sie auf dem **Start** Bildschirm\\app2\filesein, und drücken Sie dann die EINGABETASTE.  
Doppelklicken Sie auf die neue Textdokumentdatei.  
  
Dies zeigt, dass Sie eine Verbindung mit einem reinen IPv4-Server herstellen konnten, indem Sie SMB zum Abrufen einer Ressource in der Ressourcen Domäne verwenden.
16. Geben Sie auf dem **Start** BildschirmWF. mscein, und drücken Sie dann die EINGABETASTE.
17. Beachten Sie in der Konsole **Windows-Firewall mit erweiterter Sicherheit**, dass nur das **öffentliche Profil** aktiv ist. Die Windows-Firewall muss aktiviert sein, damit DirectAccess ordnungsgemäß funktioniert. Wenn die Windows-Firewall deaktiviert ist, funktioniert die DirectAccess-Konnektivität nicht.
18. Erweitern Sie im linken Bereich der Konsole den Knoten **Überwachung**, und klicken Sie auf den Knoten **Verbindungs Sicherheitsregeln**. Es sollten die aktiven Verbindungs Sicherheitsregeln angezeigt werden: **DirectAccess Policy-clientdecorp**, **DirectAccess Policy-ClientToDNS64NAT64PrefixExemption**, **DirectAccess Policy-clientdeinfratund DirectAccess Policy-clienttonlaausgenommen**. Führen Sie im mittleren Bereich einen Bildlauf nach rechts durch, um die **ersten Authentifizierungsmethoden** und **2. Authentifizierungsmethoden** Spalten anzuzeigen. Beachten Sie, dass die erste Regel (clientescorp) Kerberos V5 verwendet, um den intranettunnel einzurichten, und die dritte Regel (clientesinfrastructure) verwendet NTLMv2, um den Infrastruktur Tunnel einzurichten.
19. Erweitern Sie im linken Bereich der Konsole den Knoten **Sicherheits Zuordnungen**, und klicken Sie auf den Knoten **Hauptmodus**. Beachten Sie die Infrastruktur Tunnel-Sicherheits Zuordnungen mit NTLMv2 und der intranettunnel-Sicherheits Zuordnung mithilfe von Kerberos V5. Klicken Sie mit der rechten Maustaste auf den Eintrag, der **Benutzer (Kerberos V5)** als **2. Authentifizierungsmethode** anzeigt, und klicken Sie auf **Eigenschaften**. Beachten Sie, dass auf der Registerkarte **Allgemein** die **zweite lokale Authentifizierungs-ID** **corp\user1** lautet, die angibt, dass sich user1 erfolgreich bei der Corp-Domäne mithilfe von Kerberos authentifizieren konnte.
20. Wiederholen Sie diesen Vorgang aus Schritt 3 auf client2.

## Verschieben von CLIENT2 in die Sicherheitsgruppe Win7\_Clients\_Site2

1. Klicken Sie auf DC1 auf **Start**, geben Sie **DSA**, mscein, und drücken Sie dann die EINGABETASTE.
2. Öffnen Sie **Corp.contoso.com/users** in der Konsole Active Directory Benutzer und Computer, und

doppelklicken Sie auf **Win7\_Clients\_Site1**.

3. Klicken Sie im Dialogfeld **Win7\_Clients\_Site1 Eigenschaften** auf die Registerkarte **Mitglieder**, klicken Sie auf **client2**, klicken Sie auf **Entfernen**, klicken Sie auf **Ja**, und klicken Sie dann auf **OK**.
4. Doppelklicken Sie auf **Win7\_Clients\_Site2**, und klicken Sie dann im Dialogfeld **Win7\_Clients\_Site2 Eigenschaften** auf die Registerkarte **Mitglieder**.
5. Klicken Sie auf **Hinzufügen**, klicken Sie im Dialogfeld **Benutzer, Kontakte, Computer oder Dienst Konten auswählen** auf **Objekttypen**, wählen Sie **Computeraus**, und klicken Sie dann auf **OK**.
6. Geben Sie unter **Geben Sie die zu ausgewählenden Objektnamen ein** den Namen **client2ein**, und klicken Sie auf **OK**
7. Starten Sie **CLIENT2** neu, und melden Sie sich mit dem Konto **Corp/user1** an.
8. Öffnen Sie auf **CLIENT2** ein Windows PowerShell-Fenster mit erhöhten Rechten, geben Sie **netsh Namespace Show Policy** ein, und drücken Sie EINGABETASTE.

In der Ausgabe sollten zwei Abschnitte vorhanden sein:

- **. Corp.contoso.com:** Diese Einstellungen geben an, dass alle Verbindungen mit Corp.contoso.com vom DirectAccess-DNS-Server mit der IPv6-Adresse 2001: db8:2:: 20 aufgelöst werden sollen.
- **NLS.Corp.contoso.com:** Diese Einstellungen geben an, dass eine Ausnahme für den Namen nls.Corp.contoso.com vorliegt.

## Testen der DirectAccess-Konnektivität über das Internet bis 2 Edge1

1. Verbinden Sie **2 Edge1** mit dem Internet Netzwerk.
2. Entfernen Sie **Edge1** aus dem Internet Netzwerk.
3. Öffnen Sie auf **CLIENT1** ein Windows PowerShell-Fenster mit erhöhten Rechten.
4. Geben Sie im Windows PowerShell-Fenster **ipconfig/flushdns** ein, und drücken Sie die EINGABETASTE. Dadurch werden namens Auflösungs Einträge geleert, die möglicherweise noch im Client-DNS-Cache vorhanden sind, wenn der Client Computer mit dem Unternehmensnetzwerk verbunden war.
5. Stellen Sie sicher, dass Sie über **2-Edge1** verbunden sind. Geben Sie **netsh interface httpstunnel Show Interfaces Show Interfaces** ein, und drücken Sie die EINGABETASTE.

Die Ausgabe sollte URL: <https://2-edge1.contoso.com:443/IPHTTPSSenthalten>.

### TIP

Auf **CLIENT1** können Sie auch den folgenden Befehl ausführen: **Get-nettiphttpsconfiguration**. In der Ausgabe werden die verfügbaren Server-URL-Verbindungen und das derzeit aktive Profil angezeigt.

### NOTE

**CLIENT1** ändert automatisch den Server, über den die Verbindung mit Unternehmensressourcen hergestellt wird. Wenn in der Ausgabe des Befehls eine Verbindung mit **Edge1** angezeigt wird, warten Sie ca. fünf Minuten, und versuchen Sie es dann erneut.

6. Geben Sie im Windows PowerShell-Fenster **Ping App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse angezeigt werden, die **App1** zugewiesen ist, in diesem Fall "2001: db8:1:: 3".

7. Geben Sie im Windows PowerShell-Fenster **Ping 2-App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse, die 2-App1 zugewiesen ist, angezeigt werden, in diesem Fall "2001: db8:2::3".
8. Geben Sie im Windows PowerShell-Fenster **Ping App2** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der NAT64-Adresse angezeigt werden, die von Edge1 zu APP2 zugewiesen wird. in diesem Fall lautet der Wert **FDC9:9f4e: eb1b: 7777:: A00:4**. Beachten Sie, dass die fett formatierten Werte variieren, weil die Adresse generiert wird.

Die Möglichkeit zum Ping-APP2 ist wichtig, da der Erfolg anzeigt, dass Sie eine Verbindung mithilfe von NAT64/DNS64 herstellen konnten, da APP2 eine reine IPv4-Ressource ist.

9. Öffnen Sie Internet Explorer, geben Sie in der Internet Explorer-Adressleiste **https://app1/** ein, und drücken Sie die EINGABETASTE. Die Standard-IIS-Website auf APP1 wird angezeigt.
10. Geben Sie in der Internet Explorer-Adressleiste **https://2-app1/** ein, und drücken Sie die EINGABETASTE. Die Standardwebsite auf APP2 wird angezeigt.
11. Geben Sie in der Internet Explorer-Adressleiste **https://app2/** ein, und drücken Sie die EINGABETASTE. Die Standard Website wird auf APP3 angezeigt.
12. Geben Sie auf dem **Start** Bildschirm\\app1\file ein, und drücken Sie dann die EINGABETASTE. Doppelklicken Sie auf die Beispiel Textdatei.

Dadurch wird veranschaulicht, dass Sie eine Verbindung mit dem Dateiserver in der Corp.contoso.com-Domäne herstellen konnten, wenn eine Verbindung über 2-Edge1 besteht.

13. Geben Sie auf dem **Start** Bildschirm\\app2\file ein, und drücken Sie dann die EINGABETASTE. Doppelklicken Sie auf die neue Textdokumentdatei.  
Dies zeigt, dass Sie eine Verbindung mit einem reinen IPv4-Server herstellen konnten, indem Sie SMB zum Abrufen einer Ressource in der Ressourcen Domäne verwenden.
14. Wiederholen Sie diesen Vorgang auf CLIENT2 aus Schritt 3.

# Schritt 13 Testen der DirectAccess-Konnektivität hinter einem NAT-Gerät

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Wenn ein DirectAccess-Client hinter einem NAT-Gerät oder einem Webproxyserver mit dem Internet verbunden wird, verwendet der DirectAccess-Client entweder Teredo oder IP-HTTPS zur Verbindungsherstellung mit dem RAS-Server. Wenn das NAT-Gerät ausgehenden UDP-Port 3544 für die öffentliche IP-Adresse des RAS-Servers aktiviert, wird Teredo verwendet. Wenn kein Teredo-Zugriff verfügbar ist, fällt der DirectAccess-Client auf IP-HTTPS über den ausgehenden TCP-Port 443 zurück, wodurch der Zugriff durch Firewalls oder Webproxyserver über den herkömmlichen SSL-Port ermöglicht wird. Falls eine Authentifizierung für den Webproxy erforderlich ist, wird die IP-HTTPS-Verbindung fehlschlagen. IP-HTTPS-Verbindungen schlagen auch fehl, wenn vom Webproxy eine ausgehende SSL-Prüfung durchgeführt wird, da die HTTPS-Sitzung am Webproxy anstatt am RAS-Server beendet wird.

Die folgenden Verfahren werden auf beiden Clientcomputern ausgeführt:

1. Testen Sie die Teredo-Konnektivität. Der erste Satz von Tests wird ausgeführt, wenn der DirectAccess-Client für die Verwendung von Teredo konfiguriert ist. Das ist die automatische Einstellung, wenn das NAT-Gerät ausgehenden Zugriff auf den UDP-Port 3544 ermöglicht. Führen Sie zuerst die Tests auf CLIENT1 aus, und führen Sie dann die Tests auf CLIENT2 aus.
2. Testen Sie die IP-HTTPS-Konnektivität. Die zweite Testreihe wird durchgeführt, wenn der DirectAccess-Client für die Verwendung von IP-HTTPS konfiguriert ist. Um IP-HTTPS-Konnektivität vorzuführen, wird Teredo auf den Clientcomputern deaktiviert. Führen Sie zuerst die Tests auf CLIENT1 aus, und führen Sie dann die Tests auf CLIENT2 aus.

## Erforderliche Komponenten

Starten Sie Edge1 und 2 Edge1, wenn Sie nicht bereits ausgeführt werden, und stellen Sie sicher, dass Sie mit dem Internet-Subnetz verbunden sind.

Bevor Sie diese Tests durchführen, entfernen Sie CLIENT1 und CLIENT2 vom Internet-Switch, und verbinden Sie Sie mit dem homenet-Switch. Wenn Sie gefragt werden, welche Art von Netzwerk Sie für das aktuelle Netzwerk definieren möchten, wählen Sie **Heimnetzwerkaus**.

## Testen der Teredo-Konnektivität

1. Öffnen Sie auf CLIENT1 ein Windows PowerShell-Fenster mit erhöhten Rechten.
2. Aktivieren Sie den Teredo-Adapter, geben Sie **Netsh Interface Teredo Set State enterpriseclient**, und drücken Sie dann die EINGABETASTE.
3. Geben Sie im Windows PowerShell-Fenster **ipconfig/all** ein, und drücken Sie die EINGABETASTE.
4. Prüfen Sie die Ausgabe des Befehls "ipconfig".

Dieser Computer ist jetzt hinter einem NAT-Gerät mit dem Internet verbunden und hat eine private IPv4-Adresse erhalten. Wenn sich der DirectAccess-Client hinter einem NAT-Gerät befindet und eine private IPv4-Adresse zugeordnet wurde, wird Teredo als IPv6-Übergangstechnologie bevorzugt. Wenn Sie sich die

Ausgabe des Befehls ipconfig ansehen, sollte ein Abschnitt für Tunnel Adapter Teredo Tunneling Pseudo Schnittstelle und dann eine Beschreibung für den Microsoft Teredo-Tunneling-Adapter mit einer IP-Adresse angezeigt werden, die mit 2001:0 mit einem Teredo-Wert beginnt. Adresse. Das Standard Gateway für den Teredo-Tunnel Adapter sollte als ":" aufgeführt werden.

5. Geben Sie im Windows PowerShell-Fenster **ipconfig/flushdns** ein, und drücken Sie die EINGABETASTE.  
Dadurch werden Namensauflösungseinträge geleert, die eventuell noch im Client-DNS-Cache vorhanden sind, seitdem der Clientcomputer mit dem Internet verbunden wurde.
6. Geben Sie im Windows PowerShell-Fenster **Ping App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse von APP1 "2001:db8:1::3" angezeigt werden.
7. Geben Sie im Windows PowerShell-Fenster **Ping App2** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der NAT64-Adresse angezeigt werden, die von Edge1 zu APP2 zugewiesen wird. in diesem Fall lautet der Wert **FDC9:9f4e: eb1b: 7777:: A00:4**. Beachten Sie, dass die fett formatierten Werte variieren, weil die Adresse generiert wird.
8. Geben Sie im Windows PowerShell-Fenster **Ping 2-App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse "2-App1, 2001: db8:2:: 3" angezeigt werden.
9. Öffnen Sie Internet Explorer, geben Sie in der Internet Explorer-Adressleiste **https://2-app1/** ein, und drücken Sie die EINGABETASTE. Die IIS-Standard Website wird unter 2-App1 angezeigt.
10. Geben Sie in der Internet Explorer-Adressleiste **https://app2/** ein, und drücken Sie die EINGABETASTE. Die Standardwebsite auf APP2 wird angezeigt.
11. Geben Sie auf dem **Start** Bildschirm\\app2\\file ein, und drücken Sie dann die EINGABETASTE.  
Doppelklicken Sie auf die neue Textdokumentdatei. Dadurch wird bewiesen, dass Sie eine Verbindung zu einem reinen IPv4-Server herstellen konnten, indem Sie mit SMB eine Ressource auf einem reinen IPv4-Host abgerufen haben.
12. Wiederholen Sie diesen Vorgang auf client2.

## Testen von IP-HTTPS-Konnektivität

1. Öffnen Sie auf CLIENT1 ein Windows PowerShell-Fenster mit erhöhten Rechten, geben Sie **Netsh Interface Teredo Set State deaktiviert** ein, und drücken Sie die EINGABETASTE. Dadurch wird Teredo auf dem Clientcomputer deaktiviert. Der Clientcomputer kann sich nun selbst für IP-HTTPS konfigurieren. Nach Ausführung des Befehls wird die Antwort **OK** angezeigt.
2. Geben Sie im Windows PowerShell-Fenster **ipconfig/all** ein, und drücken Sie die EINGABETASTE.
3. Prüfen Sie die Ausgabe des Befehls "ipconfig". Dieser Computer ist jetzt hinter einem NAT-Gerät mit dem Internet verbunden und hat eine private IPv4-Adresse erhalten. Teredo ist deaktiviert, und der DirectAccess-Client fällt auf IP-HTTPS zurück. Wenn Sie sich die Ausgabe des Befehls "ipconfig" ansehen, sehen Sie einen Abschnitt für Tunnel Adapter **iphttpsinterface** mit einer IP-Adresse, die mit "2001: db8:1: 1000" oder "2001: db8:2: 2000" übereinstimmt. Dies ist eine IP-HTTPS-Adresse basierend auf den Präfixen, die konfiguriert beim Einrichten von DirectAccess. Für den **iphttpsinterface**-Tunnel Adapter wird kein Standard Gateway aufgeführt.
4. Geben Sie im Windows PowerShell-Fenster **ipconfig/flushdns** ein, und drücken Sie die EINGABETASTE.  
Dadurch werden Namensauflösungseinträge geleert, die eventuell noch im Client-DNS-Cache vorhanden sind, seitdem der Clientcomputer mit dem Unternehmensnetzwerk verbunden war.
5. Geben Sie im Windows PowerShell-Fenster **Ping App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse von APP1 "2001:db8:1::3" angezeigt werden.

6. Geben Sie im Windows PowerShell-Fenster **Ping App2** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der NAT64-Adresse angezeigt werden, die von Edge1 zu APP2 zugewiesen wird. In diesem Fall lautet der Wert **FDC9:9f4e: eb1b: 7777:: A00:4**. Beachten Sie, dass die fett formatierten Werte variieren, weil die Adresse generiert wird.
7. Geben Sie im Windows PowerShell-Fenster **Ping 2-App1** ein, und drücken Sie die EINGABETASTE. Es sollten Antworten von der IPv6-Adresse "2-App1, 2001: db8:2:: 3" angezeigt werden.
8. Öffnen Sie Internet Explorer, geben Sie in der Internet Explorer-Adressleiste **https://2-app1/** ein, und drücken Sie die EINGABETASTE. Die IIS-Standard Website wird unter 2-App1 angezeigt.
9. Geben Sie in der Internet Explorer-Adressleiste **https://app2/** ein, und drücken Sie die EINGABETASTE. Die Standardwebsite auf APP2 wird angezeigt.
10. Geben Sie auf dem **Start** Bildschirm\\app2\\file ein, und drücken Sie dann die EINGABETASTE. Doppelklicken Sie auf die neue Textdokumentdatei. Dadurch wird bewiesen, dass Sie eine Verbindung zu einem reinen IPv4-Server herstellen konnten, indem Sie mit SMB eine Ressource auf einem reinen IPv4-Host abgerufen haben.
11. Wiederholen Sie diesen Vorgang auf client2.

# Schritt 14. Momentaufnahme der Konfiguration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dadurch wird die Testumgebung für die DirectAccess-Multisite abgeschlossen. Gehen Sie folgendermaßen vor, um diese Konfiguration zu speichern, sodass Sie schnell zu einer funktionierenden DirectAccess-Konfiguration mit mehreren Standorten zurückkehren können, von der Sie andere Test Umgebungs Anleitungen für DirectAccess, Test Umgebungs Anleitungen oder für Ihre eigenen Experimente und Lernaktionen testen können. :

1. Schließen Sie alle Fenster auf allen physischen oder virtuellen Computern in der Testumgebung, und fahren Sie die Computer dann normal herunter.
2. Wenn Ihre Testumgebung auf virtuellen Computern basiert, speichern Sie eine Momentaufnahme der einzelnen virtuellen Computer, und benennen Sie die Momentaufnahmen tlg DirectAccess Multisite. Wenn Ihr Lab physische Computer verwendet, erstellen Sie Datenträger Images, um die Konfiguration der DirectAccess-Testumgebung zu speichern.

# Testumgebungsanleitung: Vorführung von DirectAccess mit OTP-Authentifizierung und RSA SecurID

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der Remote Zugriff ist eine Server Rolle im Betriebssystem Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012, das Remote Benutzern den sicheren Zugriff auf interne Netzwerkressourcen über DirectAccess oder virtuelle private Netzwerke (Virtual Private Networks, VPNs) mit dem Routing ermöglicht. und RAS-Dienst (RRAS). Diese Anleitung enthält Schritt-für-Schritt-Anweisungen zum Erweitern der [Test Umgebungs Anleitung: veranschaulichen der Einrichtung von DirectAccess Single Server mit gemischemtem IPv4 und IPv6](#), um eine Konfiguration des einmaligen Zugriffs per Remote Zugriff zu veranschaulichen.

## **WARNING**

Der Entwurf dieser Test Umgebungs Anleitung umfasst Infrastruktur Server, z. b. einen Domänen Controller und eine Zertifizierungsstelle (Certification Authority, ca), die entweder Windows Server 2012 R2 oder Windows Server 2012 ausführen. Die Verwendung dieser Test Umgebungs Anleitung zum Konfigurieren von Infrastruktur Servern, auf denen andere Betriebssysteme ausgeführt werden, wurde nicht getestet, und Anweisungen zum Konfigurieren anderer Betriebssysteme sind in diesem Handbuch nicht enthalten.

## Informationen zur Anleitung

Der Remote Zugriff in Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 bietet Unterstützung für die Client Authentifizierung mit OTP. Im Rahmen dieser Testumgebung wird nur RSA SecurID verwendet, um die OTP-Funktionalität mit Remote Zugriff zu veranschaulichen. Andere auf RADIUS basierende OTP-Lösungen werden ebenfalls unterstützt, sind jedoch außerhalb des Umfangs dieses Testlabors. Diese Anleitung enthält Anweisungen zum Konfigurieren und Veranschaulichen des Remotezugriffs mit sechs Servern und zwei Clientcomputern. Der abgeschlossene Remote Zugriff mit OTP-Test Labor simuliert ein Intranet, das Internet und ein Heimnetzwerk und veranschaulicht die Remote Zugriffs Funktionalität in verschiedenen Internetverbindungs Szenarien.

## **IMPORTANT**

Diese Testumgebung ist eine Machbarkeitsstudie mit der minimalen Anzahl an Computern. Die in dieser Anleitung beschriebene Konfiguration ist nur für Testzwecke geeignet und sollte nicht in einer Produktionsumgebung verwendet werden.

# Übersicht über das Testumgebungsszenario

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der Remote Zugriff ist eine Server Rolle in den Betriebssystemen Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012, die Remote Benutzern den sicheren Zugriff auf interne Netzwerkressourcen über DirectAccess oder virtuelle private Netzwerke (Virtual Private Networks, VPNs) mit dem RRAS (Routing and Remote Access Service). Diese Anleitung enthält Schritt-für-Schritt-Anweisungen zum Erweitern der [Test Umgebungs Anleitung: veranschaulichen der Einrichtung von DirectAccess Single Server mit gemischemtem IPv4 und IPv6](#), um eine Konfiguration des einmaligen Zugriffs per Remote Zugriff zu veranschaulichen.

## **WARNING**

Der Entwurf dieser Test Umgebungs Anleitung umfasst Infrastruktur Server, z. b. einen Domänen Controller und eine Zertifizierungsstelle (Certification Authority, ca), auf denen entweder Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird. Die Verwendung dieser Test Umgebungs Anleitung zum Konfigurieren von Infrastruktur Servern, auf denen andere Betriebssysteme ausgeführt werden, wurde nicht getestet, und Anweisungen zum Konfigurieren anderer Betriebssysteme sind in diesem Handbuch nicht enthalten.

## Informationen zur Anleitung

Der Remote Zugriff in Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 bietet Unterstützung für die Client Authentifizierung mit OTP. Im Rahmen dieser Testumgebung wird nur RSA SecurID verwendet, um die OTP-Funktionalität mit Remote Zugriff zu veranschaulichen. Andere auf RADIUS basierende OTP-Lösungen werden ebenfalls unterstützt, sind jedoch außerhalb des Umfangs dieses Testlabors. Diese Anleitung enthält Anweisungen zum Konfigurieren und Veranschaulichen des Remotezugriffs mit sechs Servern und zwei Clientcomputern. Der abgeschlossene Remote Zugriff mit OTP-Test Labor simuliert ein Intranet, das Internet und ein Heimnetzwerk und veranschaulicht die Remote Zugriffs Funktionalität in verschiedenen Internetverbindungs Szenarien.

## **IMPORTANT**

Diese Testumgebung ist eine Machbarkeitsstudie mit der minimalen Anzahl an Computern. Die in dieser Anleitung beschriebene Konfiguration ist nur für Testzwecke geeignet und sollte nicht in einer Produktionsumgebung verwendet werden.

# Konfigurationsanforderungen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die folgenden Komponenten sind erforderlich, um den Remote Zugriff im Testlabor zu konfigurieren:

- Die Produkt-CD oder-Dateien für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.
- Neun Computer oder virtuelle Computer, die die Mindesthardwareanforderungen für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 erfüllen auf drei dieser Computer sind zwei Netzwerkadapter installiert.
- Die Produkt-CD oder-Dateien für Windows 10® oder Windows® 8.
- Die Produkt-CD oder-Dateien für Windows 7 Ultimate.
- Drei Computer oder virtuelle Computer, die die Mindesthardwareanforderungen für Windows 10®, Windows 8 oder Windows 7 erfüllen auf einem dieser Computer sind zwei Netzwerkadapter installiert.

# Schritt 1 vervollständigen der DirectAccess-Konfiguration

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt besteht darin, alle Schritte in der [Test Umgebungs Anleitung zum Veranschaulichen der Einrichtung eines einzelnen Servers mit gemischem IPv4 und IPv6](#) auszuführen. Wenn Sie die Schritte in dieser Test Umgebungs Anleitung bereits ausgeführt und eine Momentaufnahme oder ein Datenträger Image der Testumgebung gespeichert haben, können Sie die Momentaufnahme oder das Image wiederherstellen und mit dem nächsten Schritt beginnen.

# Schritt 2 App1 konfigurieren

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Führen Sie die folgenden Schritte aus, um App1 für die OTP-Unterstützung vorzubereiten:

1. Zum Erstellen und Bereitstellen einer Zertifikat Vorlage, die zum Signieren von OTP-Zertifikat Anforderungen verwendet wird. Konfigurieren Sie eine Zertifikat Vorlage zum Signieren von OTP-Zertifikat Anforderungen.
2. Zum Erstellen und Bereitstellen einer Zertifikat Vorlage für OTP-Zertifikate, die von der Unternehmens Zertifizierungsstelle ausgestellt wurden. Konfigurieren Sie eine Zertifikat Vorlage für OTP-Zertifikate, die von der Unternehmens Zertifizierungsstelle ausgestellt wurden.

## WARNING

Der Entwurf dieser Test Umgebungs Anleitung umfasst Infrastruktur Server, z. b. einen Domänen Controller und eine Zertifizierungsstelle (Certification Authority, ca), die entweder Windows Server 2012 R2 oder Windows Server 2012 ausführen. Die Verwendung dieser Test Umgebungs Anleitung zum Konfigurieren von Infrastruktur Servern, auf denen andere Betriebssysteme ausgeführt werden, wurde nicht getestet, und Anweisungen zum Konfigurieren anderer Betriebssysteme sind in diesem Handbuch nicht enthalten.

## So erstellen Sie eine Zertifikat Vorlage, die zum Signieren von OTP-Zertifikat Anforderungen verwendet wird

1. Führen Sie **certtmpl.mscaus**, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie in der Konsole Zertifikat Vorlagen im Detailbereich mit der rechten Maustaste auf die Computer Vorlage, und klicken Sie auf **Doppelte Vorlage**.
3. Wählen Sie im Dialogfeld **Eigenschaften der neuen Vorlage** auf der Registerkarte **Kompatibilität** in der Liste **Zertifizierungs Stelle** das gewünschte Betriebssystem aus, und klicken Sie im Dialogfeld **resultierende Änderungen** auf OK. Wählen Sie in der Liste **Zertifikat Empfänger** das gewünschte Betriebssystem aus, und klicken Sie im Dialogfeld **resultierende Änderungen** auf OK.
4. Klicken Sie im Dialogfeld **Eigenschaften der neuen Vorlage** auf die Registerkarte **Allgemein**.
5. Geben Sie auf der Registerkarte **Allgemein** unter **Vorlagen Anzeige Name den Namen** daotpraein. Legen Sie die **Gültigkeitsdauer** auf 2 Tage fest, und legen Sie den **Erneuerungs Zeitraum** auf 1 Tag fest. Wenn die Warnung **Zertifikat Vorlagen** angezeigt wird, klicken Sie auf OK.
6. Klicken Sie auf die Registerkarte **Sicherheit** und dann auf **Hinzufügen**.
7. Klicken Sie im Dialogfeld **Benutzer, Computer, Dienst Konten oder Gruppen auswählen** auf **Objekttypen**. Wählen Sie im Dialogfeld **Objekttypen** die Option **Computeraus**, und klicken Sie dann auf OK. Geben Sie im Feld **Geben Sie die zu ausgewählenden Objektnamen ein** den Namen Edge1 ein, klicken Sie auf OK, und aktivieren Sie in der Spalte **zulassen** die Kontrollkästchen **Lesen, registrieren** und **automatisch registrieren**. Klicken Sie in der Spalte **zulassen** auf **Authentifizierte Benutzer**, aktivieren Sie das Kontrollkästchen **Lesen**, und deaktivieren Sie alle anderen Kontrollkästchen. Klicken Sie auf **Domänen Computer**, und deaktivieren Sie in der Spalte **zulassen** die Option **registrieren**. Klicken Sie auf **Domänen-Admins** und **Organisations- Admins**, und klicken Sie in der Spalte **zulassen** für beide auf **voll**

Zugriff. Klicken Sie auf **Übernehmen**.

8. Klicken Sie auf die Registerkarte **Antragsteller Name**, und klicken Sie dann auf **aus diesen Active Directory Informationen erstellen**. Geben Sie im Format "Name des Antragstellers" den Namen DNS-Namenein, vergewissern Sie sich, dass das Feld **DNS-Name** aktiviert ist, und klicken Sie auf **OK**.
9. Wählen Sie auf der Registerkarte **Erweiterungen** die Option **Anwendungsrichtlinien** aus, und klicken Sie dann auf **Bearbeiten**. Entfernen Sie alle vorhandenen Anwendungsrichtlinien. Klicken Sie auf **Hinzufügen**, und klicken Sie im Dialogfeld **Anwendungs Richtlinie hinzufügen** auf **neu**, geben Sie im Feld **Name** Folgendes ein, und klicken Sie auf **1.3.6.1.4.1.311.81.1.1**, und klicken Sie dann auf **OK**. Klicken Sie im Dialogfeld **Anwendungs Richtlinie hinzufügen** auf **OK**. Klicken Sie unter **Anwendungsrichtlinien Erweiterung bearbeiten** auf **OK**. Klicken Sie im Dialogfeld **Eigenschaften der neuen Vorlage** auf **OK**.

So erstellen und stellen Sie eine Zertifikat Vorlage für OTP-Zertifikate bereit, die von der Unternehmens Zertifizierungsstelle ausgestellt wurden

1. Klicken Sie in der Konsole Zertifikat Vorlagen im Detailbereich mit der rechten Maustaste auf die **Smartcard-Anmelde** Vorlage, und klicken Sie auf **Doppelte Vorlage**.
2. Klicken Sie im Dialogfeld **Eigenschaften der neuen Vorlage** auf der Registerkarte **Kompatibilität** in der Liste **Zertifizierungs Stelle** auf das Betriebssystem, das Sie verwenden möchten, und klicken Sie im Dialogfeld **resultierende Änderungen** auf **OK**. Wählen Sie in der Liste **Zertifikat Empfänger** das Betriebssystem aus, das Sie verwenden möchten, und klicken Sie im Dialogfeld **resultierende Änderungen** auf **OK**.
3. Klicken Sie im Dialogfeld **Eigenschaften der neuen Vorlage** auf die Registerkarte **Allgemein**.
4. Geben Sie auf der Registerkarte **Allgemein** unter **Vorlagen Anzeige Name den Namen daotplogonein**. Klicken Sie in der Dropdown Liste unter **Gültigkeitsdauer** auf **Stunden**, klicken Sie im Dialogfeld **Zertifikat Vorlagen** auf **OK**, und stellen Sie sicher, dass die Anzahl der Stunden auf 1 festgelegt ist. Geben Sie in **Erneuerungs Zeitraum** den Wert **0** ein.

#### **IMPORTANT**

**Windows Server 2003**-Zertifizierungsstelle. In Fällen, in denen sich die Zertifizierungsstelle auf einem Computer befindet, auf dem Windows Server 2003 ausgeführt wird, muss die Zertifikat Vorlage auf einem anderen Computer konfiguriert werden. Dies ist erforderlich, da das Festlegen der **Gültigkeitsdauer** in Stunden nicht möglich ist, wenn Windows-Versionen vor Windows Server 2008 und Windows Vista ausgeführt werden. Wenn auf dem Computer, den Sie zum Konfigurieren der Vorlage verwenden, die Active Directory Zertifikat Dienste-Server Rolle nicht installiert ist, oder wenn es sich um einen Client Computer handelt, müssen Sie möglicherweise das Zertifikat Vorlagen-Snap-in installieren. Weitere Informationen finden Sie unter [Installieren des Zertifikat Vorlagen-Snap-Ins](#).

**Windows Server 2008 R2**-Zertifizierungsstelle. Wenn Sie bereits eine Zertifizierungsstelle (Certification Authority, ca) bereitgestellt haben, auf der Windows Server 2008 R2 ausgeführt wird, müssen Sie den **Erneuerungs Zeitraum** für die Zertifikat Vorlage auf 1 oder 2 Stunden festlegen, und der **Gültigkeits Zeitraum** muss länger sein als der **Erneuerungs Zeitraum**, aber nicht mehr als vier Stunden. Wenn Sie für eine Zertifizierungsstelle, auf der Windows Server 2008 R2 ausgeführt wird, eine **Gültigkeitsdauer** von Zertifikat Vorlagen mit einer Zertifizierungsstelle konfigurieren, die auf Windows Server R2 ausgeführt wird, kann der DirectAccess-Installations-Assistent die Zertifikat Vorlage nicht erkennen

5. Klicken Sie auf die Registerkarte **Sicherheit**, wählen Sie in der Spalte **Zulassen** die Option **Authentifizierte Benutzer** aus, und aktivieren Sie die Kontrollkästchen **Lesen** und **registrieren**. Klicken Sie auf **OK**. Klicken Sie auf **Domänen-Admins** und **Organisations- Admins**, und klicken Sie in der Spalte **zulassen** für beide auf **voll Zugriff**. Klicken Sie auf **Übernehmen**.

6. Klicken Sie auf die Registerkarte **Antragsteller Name**, und klicken Sie dann auf **aus diesen Active Directory Informationen erstellen**. Wählen Sie im Format "Antragsteller Name" die Option **Vollständiger definierter Name** aus, vergewissern Sie sich, dass das Feld **Benutzer Prinzipal Name (UPN)** aktiviert ist, und klicken Sie auf übernehmen **Apply**
7. Aktivieren Sie die Registerkarte **Server**, aktivieren Sie das Kontrollkästchen **keine Zertifikate und Anforderungen in der Zertifizierungsstellen Datenbank speichern**, deaktivieren Sie das Kontrollkästchen **keine Sperr Informationen in ausgestellten Zertifikaten einschließen**, und klicken Sie dann im Dialogfeld **Eigenschaften der neuen Vorlage** auf **anwenden**.
8. Klicken Sie auf die Registerkarte **Ausstellungs Anforderungen**, aktivieren Sie das Kontrollkästchen **diese Anzahl von autorisierten Signaturen:**, und legen Sie den Wert auf 1 fest. Wählen Sie unter **Signatur den Richtlinientyp erforderlich in** der Liste die Option **Anwendungs Richtlinie** aus, und wählen Sie in der Liste **Anwendungs Richtlinie** die Option **da OTP RA** aus. Klicken Sie im Dialogfeld **Eigenschaften der neuen Vorlage** auf **OK**.
9. Klicken Sie auf die Registerkarte **Erweiterungen**, und klicken Sie unter **Anwendungsrichtlinien** auf **Bearbeiten**. Löschen Sie die **Client Authentifizierung**, behalten Sie **smartcardlogon** bei, und klicken Sie zweimal auf **OK**.
10. Schließen Sie die Zertifikatvorlagenkonsole.
11. Geben Sie auf dem Bildschirm **Start** den Befehl **certrv. mscein**, und drücken Sie dann die EINGABETASTE.
12. Erweitern Sie in der Konsole Struktur der Zertifizierungsstelle **Corp-App1-ca-1**, klicken Sie auf **Zertifikat Vorlagen**, klicken Sie mit der rechten Maustaste auf **Zertifikat Vorlagen**, zeigen Sie auf **neu**, und klicken Sie dann auf **Auszustellende Zertifikat Vorlage**.
13. Klicken Sie in der Liste der Zertifikat Vorlagen auf **daotpra** und **daotplogon**, und klicken Sie dann auf **OK**.
14. Im Detailbereich der-Konsole sollte die **daotpra** -Zertifikat Vorlage mit dem **beabsichtigten Zweck** " **da OTP RA** " und der " **daotplogon** "-Zertifikat Vorlage mit dem **beabsichtigten Zweck** der **Smartcardanmeldung** angezeigt werden.
15. Starten Sie die Dienste neu.
16. Schließen Sie die Konsole Zertifizierungsstelle.
17. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Geben Sie **certutil. exe-setreg DBFlags + DBFLAGS\_ENABLEVOLATILEREQUESTS** ein, und drücken Sie die EINGABETASTE.
18. Lassen Sie das Eingabe Aufforderungs Fenster für den nächsten Schritt geöffnet.

# Schritt 3 DC1 konfigurieren

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

DC1 fungiert als Domänen Controller, DNS-Server und DHCP-Server für die Corp.contoso.com-Domäne.  
Konfigurieren Sie DC1 wie folgt:

**Überprüfen, ob user1 einen Benutzer Prinzipal Namen auf DC1 definiert ist**

1. Öffnen Sie auf DC1 Server-Manager, und klicken Sie im linken Bereich auf AD DS . Klicken Sie mit der rechten Maustaste auf DC1 , und wählen Sie **Active Directory Benutzer und Computer** Erweitern Sie im linken Bereich **Corp. Configuration. com\users**, und doppelklicken Sie auf user1.
2. Überprüfen Sie auf der Registerkarte **Konto** , ob der **Benutzer Anmelde Name** auf user1 festgelegt ist. Wenn dies nicht der Wert ist, geben Sie User1 in das Feld **Benutzer Anmelde Name** ein.
3. Klicken Sie auf OK. Schließen Sie die Konsole Active Directory-Benutzer und -Computer.

# Schritt 4 installieren und Konfigurieren von RSA und Edge1

09.04.2020 • 24 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

RSA ist der RADIUS-und OTP-Server und wird vor dem Konfigurieren von RADIUS und OTP installiert.

Zum Konfigurieren der RSA-Bereitstellung führen Sie die folgenden Schritte aus:

1. Installieren Sie das Betriebssystem auf dem RSA-Server. Installieren Sie Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 auf dem RSA-Server.
2. Konfigurieren von TCP/IP auf RSA Konfigurieren Sie die TCP/IP-Einstellungen auf dem RSA-Server.
3. Kopieren Sie die Authentifizierungs-Manager-Installationsdateien auf den RSA-Server. Nachdem Sie das Betriebssystem auf RSA installiert haben, kopieren Sie die Authentifizierungs-Manager-Dateien auf den RSA-Computer.
4. Fügen Sie den RSA-Server der Corp-Domäne hinzu. Verknüpfen Sie RSA mit der Corp-Domäne.
5. Deaktivieren Sie die Windows-Firewall auf RSA. Deaktivieren Sie die Windows-Firewall auf dem RSA-Server.
6. Installieren Sie den RSA Authentication Manager auf dem RSA-Server. Installieren Sie den RSA Authentication Manager.
7. Konfigurieren Sie den RSA Authentication Manager. Konfigurieren Sie den Authentifizierungs-Manager.
8. Erstellen Sie daprobeuser. Erstellen Sie ein Benutzerkonto zu Testzwecken.
9. Installieren Sie das RSA SecurID-Software Token auf CLIENT1. Installieren Sie das RSA SecurID-Software Token auf CLIENT1.
10. Konfigurieren Sie Edge1 als RSA-Authentifizierungs-Agent. Konfigurieren Sie den RSA-Authentifizierungs-Agent auf Edge1.
11. Konfigurieren Sie Edge1 zur Unterstützung der OTP-Authentifizierung. Konfigurieren Sie OTP für DirectAccess, und überprüfen Sie die Konfiguration.

## Installieren des Betriebssystems auf dem RSA-Server

1. Starten Sie unter RSA die Installation von Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012.
2. Befolgen Sie die Anweisungen, um die Installation abzuschließen, indem Sie Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 (vollständige Installation) und ein sicheres Kennwort für das lokale Administrator Konto angeben. Melden Sie sich mit dem lokalen Administratorkonto an.
3. Verbinden Sie RSA mit einem Netzwerk, das über Internet Zugriff verfügt, und führen Sie Windows Update aus, um die neuesten Updates für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 zu installieren, und trennen Sie dann die Verbindung mit dem Internet.
4. Stellen Sie eine Verbindung mit dem Subnetz "Corpnet" her.

## Konfigurieren von TCP/IP auf RSA

1. Klicken Sie in Aufgaben zur Erstkonfiguration auf **Netzwerk konfigurieren**.
2. Klicken Sie unter **Netzwerkverbindungen** mit der rechten Maustaste auf **LAN- Verbindung**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)** , und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf **Folgende IP-Adresse verwenden**. Geben Sie im Feld **IP-Adresse** die Adresse 10.0.0.5 ein. Geben Sie im Feld **Subnetzmaske** den Wert 255.255.255.0 ein. Geben Sie unter **Standard Gateway** den Namen 10.0.0.2 ein. Klicken Sie auf **folgende DNS-Serveradressen verwenden**, geben Sie unter **Bevorzugter DNS-Server** den Namen 10.0.0.1 ein.
5. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
6. Geben Sie unter **DNS-Suffix für diese Verbindung** Corp.contoso.com ein, und klicken Sie dann zweimal auf **OK** .
7. Klicken Sie im Dialogfeld **Eigenschaften von LAN- Verbindung** auf **Schließen**.
8. Schließen Sie das Fenster **Netzwerkverbindungen**.

## Kopieren von Authentifizierungs-Manager-Installationsdateien auf den RSA-Server

1. Erstellen Sie auf dem RSA-Server den Ordner "c:\rsa-Installation".
2. Kopieren Sie den Inhalt des RSA Authentication Manager 7.1 SP4-Mediums in den Installationsordner "c:\rsa".
3. Erstellen Sie den Unterordner c:\rsa installation\license und Token.
4. Kopieren Sie die RSA-Lizenzdateien nach c:\rsa installation\license und Token.

## Fügen Sie den RSA-Server der Corp-Domäne hinzu.

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Systemeigenschaften** auf der Registerkarte **Computername** auf **Ändern**.
3. Geben Sie unter **Computer Name** den Namen RSA ein. Klicken Sie unter **Mitglied von** auf **Domäne**, geben Sie Corp.contoso.com ein, und klicken Sie dann auf **OK**.
4. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie **User1** und sein Kennwort ein, und klicken Sie auf **OK**.
5. Klicken Sie im Dialogfeld Domäne Willkommen auf **OK**.
6. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
7. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
8. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.
9. Nachdem der Computer neu gestartet wurde, geben Sie **User1** und das Kennwort ein, wählen Sie Corp in der Dropdown Liste **Anmelden an:** aus, und klicken Sie auf **OK**.

## Deaktivieren der Windows-Firewall auf RSA

1. Klicken Sie auf **Start**, klicken Sie auf **System Steuerung**, klicken Sie auf **System und Sicherheit** und dann auf **Windows-Firewall**.
2. Klicken Sie auf **Windows-Firewall aktivieren oder deaktivieren**.
3. **Deaktivieren** Sie die Windows-Firewall für alle Einstellungen.
4. Klicken Sie auf **OK**, und schließen Sie Windows-Firewall.

## Installieren Sie den RSA Authentication Manager auf dem RSA-Server.

1. Wenn die Sicherheits Warnmeldung während des Vorgangs zu einem beliebigen Zeitpunkt angezeigt wird, klicken Sie auf **Ausführen**, um fortzufahren.
2. Öffnen Sie den Installationsordner c:\rsa, und doppelklicken Sie auf **Autorun.exe**.
3. Klicken Sie auf **jetzt installieren**, klicken Sie auf **weiter**, wählen Sie die Top-Option für die Americas aus, und klicken Sie auf **weiter**.
4. Wählen Sie **Ich akzeptiere die Bedingungen des Lizenzvertrags aus**, und klicken Sie auf **weiter**.
5. Wählen Sie **primäre Instanz** aus, und klicken Sie auf **weiter**.
6. Geben Sie im Feld **Verzeichnis Name: c:\rsaein**, und klicken Sie auf **weiter**.
7. Überprüfen Sie, ob der Servername (RSA.Corp.contoso.com) und die IP-Adresse richtig sind, und klicken Sie auf **weiter**.
8. Navigieren Sie zu c:\rsa installation\license und Token, und klicken Sie auf **weiter**.
9. Klicken Sie auf der Seite **Lizenzdatei überprüfen** auf **weiter**.
10. Geben Sie in das Feld **Benutzer-ID ein**, und geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** ein sicheres Kennwort ein. Klicken Sie auf **Weiter**.
11. Übernehmen Sie auf dem Bildschirm Protokoll Auswahl die Standardeinstellungen, und klicken Sie auf **weiter**.
12. Klicken Sie auf dem Bildschirm Zusammenfassung auf **Installieren**.
13. Klicken Sie nach Abschluss der Installation auf **Fertigstellen**.

## Konfigurieren des RSA-Authentifizierungs-Managers

1. Wenn die RSA-Sicherheits Konsole nicht automatisch geöffnet wird, doppelklicken Sie auf dem RSA-Computer Desktop auf "RSA Security Console".
2. Wenn das Sicherheitszertifikat Warnung/Sicherheitswarnung angezeigt wird, klicken Sie auf **diese Website fortsetzen**, oder klicken Sie auf **Ja**, um den Vorgang fortzusetzen, und fügen Sie diese Website den vertrauenswürdigen Sites hinzu.
3. Geben Sie **Administrator** im Feld **Benutzer-ID** ein, und klicken Sie auf **OK**.
4. Geben Sie im Feld **Kennwort** das Kennwort für das Administrator Konto ein, und klicken Sie auf **Anmelden**.
5. Fügt Tokeninformationen ein.
  - a. Klicken Sie in der **RSA-Sicherheits Konsole** auf **Authentifizierung**, und klicken Sie auf **SecurID Tokens**.
  - b. Klicken Sie auf **Token importieren Auftrag**, und klicken Sie dann auf **neue hinzufügen**.

- c. Klicken Sie im Abschnitt **Import Optionen** auf **Durchsuchen**. Navigieren Sie zu der XML-Token-Datei in C:.. Ordner RSA installation\license und Token, und klicken Sie auf **Öffnen**.
  - d. Klicken Sie unten auf der Seite auf **Auftrag übermitteln**.
6. Erstellen Sie einen neuen OTP-Benutzer.
- a. Klicken Sie in der **RSA-Sicherheits Konsole** auf die Registerkarte **Identität**, klicken Sie auf **Benutzer** und dann auf **neue hinzufügen**.
  - b. Im **Nachnamen**: Abschnitt **User** und im Abschnitt **User ID: Section Type User1** (UserID muss mit dem für dieses Lab verwendeten AD-Benutzernamen identisch sein). Geben Sie in den Abschnitten **Kennwort:** und **Kennwort bestätigen:** ein sicheres Kennwort ein. Deaktivieren Sie das Kontrollkästchen "**Benutzer muss Kennwort bei der nächsten Anmeldung ändern**", und klicken Sie auf **Speichern**.
7. Weisen Sie user1 einem der importierten Token zu.
- a. Klicken Sie auf der Seite **Benutzer** auf **User1**, und klicken Sie auf **SecurID Tokens**.
  - b. Klicken Sie auf **SecurID Tokens**, und klicken Sie auf **Token zuweisen**.
  - c. Klicken Sie unter der Überschrift **Seriennummer** auf die erste aufgeführte Zahl, und klicken Sie auf **zuweisen**.
  - d. Klicken Sie auf das zugewiesene Token, und klicken Sie auf **Bearbeiten**. Wählen Sie im Abschnitt **SecurID-PIN-Verwaltung** für **Benutzer Authentifizierungsanforderung** die Option **PIN nicht erforderlich (nur Tokencode)** aus.
  - e. Klicken Sie auf **Token Speichern und verteilen**.
  - f. Klicken Sie im Abschnitt **Grundlagen** auf der Seite **Software Token verteilen** auf **Issue Token File (sdtid)**.
  - g. Deaktivieren Sie auf der Seite **Software Token verteilen** im Abschnitt **tokendateioptionen** das Kontrollkästchen **Kopierschutz aktivieren**. Klicken Sie auf **kein Kennwort** und weiter.
  - h. Klicken Sie im Abschnitt **Downloaddatei** auf der Seite **Software Token verteilen** auf **jetzt herunterladen**. Klicken Sie auf **Speichern**. Navigieren Sie zu c:\rsa-Installation, und klicken Sie auf **Speichern** und **Schließen**.
  - i. Minimieren Sie die **RSA-Sicherheits Konsole** für die spätere Verwendung.
8. Konfigurieren Sie den Authentifizierungs-Manager als RADIUS-Server.
- a. Doppelklicken Sie auf dem RSA-Computer Desktop auf "**RSA-Sicherheits Betriebs Konsole**".
  - b. Wenn das Sicherheitszertifikat Warnung/Sicherheitswarnung angezeigt wird, klicken Sie auf **diese Website fortsetzen**, oder klicken Sie auf **Ja**, um den Vorgang fortzusetzen, und fügen Sie diese Website den vertrauenswürdigen Sites hinzu
  - c. Geben Sie Benutzer-ID und Kennwort ein, und klicken Sie auf **Anmelden**.
  - d. Klicken Sie auf **Bereitstellungs Konfiguration-RADIUS-Server konfigurieren**.
  - e. Geben Sie auf der Seite **zusätzliche Anmelde Informationen erforderlich** die Benutzer-ID und das Kennwort des Administrators ein, und klicken Sie
  - f. Geben Sie auf der Seite **RADIUS-Server konfigurieren** dasselbe Kennwort ein, das für den Administrator Benutzer für die geheimen Schlüssel und das **Master Kennwort** verwendet wurde. Geben Sie die Administrator Benutzer-ID und das Kennwort ein, und klicken Sie auf **Konfigurieren**

- g. Vergewissern Sie sich, dass die Meldung "der RADIUS-Server wurde erfolgreich konfiguriert" angezeigt wird. Klicken Sie auf **Fertig**. Schließen Sie die RSA-Betriebs Konsole.
- h. Wechseln Sie zurück zur "**RSA-Sicherheits Konsole**" .
- i. Klicken Sie auf der Registerkarte **RADIUS** auf **RADIUS-Server**. Vergewissern Sie sich, dass **RSA.Corp.contoso.com** aufgeführt ist.
9. Konfigurieren Sie den RSA-Server als RSA-Authentifizierungs Client.
- Klicken Sie auf der Registerkarte **RADIUS** auf **RADIUS-Clients** , und **fügen Sie neue hinzu**.
  - Aktivieren Sie das Kontrollkästchen **beliebiger RADIUS-Client** .
  - Geben Sie im Feld **gemeinsamer geheimer Schlüssel** ein sicheres Kennwort Ihrer Wahl ein. Dieses Kennwort wird später beim Konfigurieren von Edge1 für OTP verwendet.
  - Lassen Sie das Feld **IP-Adresse** leer, und **Erstellen** Sie den Eintrag als **Standard-RADIUS**.
  - Klicken Sie auf **ohne RSA-Agent speichern**.
10. Erstellen Sie Dateien, die zum Konfigurieren von Edge1 als RSA-Authentifizierungs-Agent erforderlich sind.
- Markieren Sie auf der Registerkarte **Zugriff** die **Authentifizierungs-Agents**, und klicken Sie auf **neue hinzufügen**.
  - Geben Sie **Edge1** in das Feld **Hostname** ein, und klicken Sie auf **IP auflösen**.
  - Beachten Sie, dass die IP-Adresse für Edge1 jetzt im Feld **IP-Adresse** angezeigt wird. Klicken Sie auf **Speichern**.
11. Generieren Sie eine Konfigurationsdatei für den Edge1-Server (AM\_Config.zip).
- Markieren Sie auf der Registerkarte **Zugriff** die **Authentifizierungs-Agents**, und klicken Sie auf **Konfigurationsdatei generieren**.
  - Klicken Sie auf der Seite **Konfigurationsdatei generieren** auf **Konfigurationsdatei generieren**, und klicken Sie dann auf **jetzt herunterladen**.
  - Klicken Sie auf **Speichern**, navigieren Sie zu C: RSA-Installation, und klicken Sie auf **Speichern**.
  - Klicken Sie im Dialogfeld **Download abgeschlossen** auf **Schließen** .
12. Generieren Sie eine geheime Knoten Datei für den Edge1-Server (EDGE1\_NodeSecret.zip).
- Markieren Sie auf der Registerkarte **Zugriff** die **Authentifizierungs-Agents**, und klicken Sie auf **vorhandene verwalten**.
  - Klicken Sie auf den aktuell konfigurierten Knoten Edge1, und klicken Sie auf **Knoten Geheimnis verwalten**.
  - Aktivieren Sie das Kontrollkästchen **neuen zufälligen Knoten erstellen**, und **exportieren Sie das Knoten Geheimnis in eine Datei** .
  - Geben Sie das Kennwort ein, das für den Administrator Benutzer in den Feldern **Verschlüsselungs Kennwort** und **Verschlüsselungs Kennwort bestätigen** verwendet wird, und klicken Sie auf **Speichern**.
  - Klicken Sie auf der Seite für die Datei mit dem **geheimen Knoten Schlüssel** auf **Download Now**
  - Klicken Sie im Dialogfeld **Datei Download** auf **Speichern**, navigieren Sie zu c:\rsa-Installation, und klicken Sie auf **Speichern**. Klicken Sie im Dialogfeld **Download abgeschlossen** auf **Schließen** .

- g. Über den RSA Authentication Manager Media Copy \ auth\_mgr \Windows-x86\_64 \am\rsa-ace\_nsload \Win32-5.0-x86\ agent\_nsload. exe zu c:\rsa Installation.

## Erstellen von daprobeuser

1. Klicken Sie in der RSA-Sicherheits Konsole auf die Registerkarte Identität , klicken Sie auf Benutzer und dann auf neue hinzufügen.
2. Geben Sie im Abschnitt Nachname die Bezeichnung Type Probееin, und geben Sie im Abschnitt User ID: den Typ daprobeuserein. Geben Sie in den Abschnitten Kennwort: und Kennwort bestätigen: ein sicheres Kennwort ein. Deaktivieren Sie das Kontrollkästchen "Benutzer muss Kennwort bei der nächsten Anmeldung ändern", und klicken Sie auf Speichern.

## Installieren des RSA SecurID-Software Tokens auf CLIENT1

Verwenden Sie dieses Verfahren, um das SecurID-Software Token auf CLIENT1 zu installieren.

### **SecurID-Software Token installieren**

1. Erstellen Sie auf dem Computer Client1 den Ordner c:\rsa-Dateien. Kopieren Sie die Datei Software\_Tokens.zip aus der c:\rsa-Installation auf dem RSA-Computer in c:\rsa-Dateien. Extrahieren Sie die Datei User1\_000031701832.sdtid in c:\rsa-Dateien auf CLIENT1.
2. Greifen Sie auf die RSA SecurID-Software Token-Medienquelle zu, und doppelklicken Sie im Ordner SecurID Softwaretoken Client App auf RSASECURIDTOKEN410, um die RSA SecurID-Installation zu starten. Wenn die Meldung Datei öffnen-Sicherheitswarnung angezeigt wird, klicken Sie auf Ausführen.
3. Klicken Sie im Dialogfeld RSA SecurID Software Token-InstallShield Wizard zweimal auf weiter .
4. Akzeptieren Sie den Lizenzvertrag, und klicken Sie auf weiter.
5. Wählen Sie im Dialogfeld Installationstyp die Option typisch aus, klicken Sie auf weiter und dann auf Installieren.
6. Falls das Dialogfeld Benutzerkontensteuerung angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf Ja.
7. Aktivieren Sie das Kontrollkästchen RSA SecurID-Software Token starten , und klicken Sie auf Fertigstellen.
8. Klicken Sie auf aus Datei importieren.
9. Klicken Sie auf Durchsuchen, wählen Sie c:\rsa Files \ User1\_000031701832.sdtid aus, und klicken Sie auf Öffnen.
10. Klicken Sie zweimal auf OK .

## Konfigurieren von Edge1 als RSA-Authentifizierungs-Agent

Verwenden Sie dieses Verfahren, um Edge1 zum Ausführen der RSA-Authentifizierung zu konfigurieren.

### **Konfigurieren des RSA-Authentifizierungs-Agents**

1. Öffnen Sie auf Edge1 Windows-Explorer, und erstellen Sie den Ordner c:\rsa-Dateien. Navigieren Sie zu den RSA ACE-Installationsmedien.
2. Kopieren Sie die Dateien agent\_nsload. exe, AM\_Config.zip und EDGE1\_NodeSecret.zip aus dem RSA-Medium in c:\rsa-Dateien.
3. Extrahieren Sie den Inhalt der beiden ZIP-Dateien an die folgenden Speicherorte:

- a. C:\Windows\System32
  - b. C:\windows\syswow64\
4. Kopieren Sie agent\_nsload.exe nach c:\windows\SysWOW64\.
  5. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, und navigieren Sie zu c:\windows\SysWOW64.
  6. Geben Sie **agent\_nsload.exe -f nodesecret.rec -p** ein wobei das sichere Kennwort ist, das Sie während der ersten RSA-Konfiguration erstellt haben. Drücken Sie die EINGABETASTE.
  7. Kopieren Sie c:\windows\syswow64\securid nach c:\Windows\System32.

## Konfigurieren von Edge1 für die Unterstützung der OTP-Authentifizierung

Verwenden Sie dieses Verfahren, um OTP für DirectAccess zu konfigurieren und die Konfiguration zu überprüfen.

### Konfigurieren von OTP für DirectAccess

1. Öffnen Sie auf Edge1 Server-Manager, und klicken Sie im linken Bereich auf **Remote Zugriff**.
2. Klicken Sie im Bereich Server mit der rechten Maustaste auf **Edge1**, und wählen Sie **Remote Zugriffs Verwaltung** aus.
3. Klicken Sie auf **Konfiguration**.
4. Klicken Sie im Fenster DirectAccess-Setup unter Schritt 2-RAS-Server auf **Bearbeiten**.
5. Klicken Sie dreimal auf **Weiter**, und wählen Sie im Abschnitt **Authentifizierung** die Option **zweistufige Authentifizierung** aus, und vergewissern Sie sich, dass die Option **Computer Zertifikate verwenden** aktiviert ist. Vergewissern Sie sich, dass die Stamm Zertifizierungsstelle auf CN = Corp-App1-ca festgelegt ist. Klicken Sie auf **Weiter**.
6. Doppelklicken Sie im Abschnitt "OTP RADIUS-Server" auf das Feld "leerer Server Name".
7. Geben Sie im Dialogfeld **RADIUS-Server hinzufügen RSA** in das Feld **Server Name** ein. Klicken Sie neben dem Feld **gemeinsamer geheimer Schlüssel** auf **ändern**, und geben Sie das Kennwort ein, das Sie beim Konfigurieren der RADIUS-Clients auf dem RSA-Server in den Feldern **neuer geheimer Schlüssel** und **neues Geheimnis bestätigen** verwendet haben. Klicken Sie zweimal auf **OK**, und klicken Sie auf **Weiter**.

#### NOTE

Wenn sich der RADIUS-Server in einer anderen Domäne als der RAS-Server befindet, muss im Feld **Server Name** der voll qualifizierte Domänen Name des RADIUS-Servers angegeben werden.

8. Wählen Sie im Abschnitt **OTP-Zertifizierungsstellen** Server App1.Corp.contoso.com aus, und klicken Sie auf **Hinzufügen**. Klicken Sie auf **Weiter**.
9. Klicken Sie auf der Seite **OTP-Zertifikat Vorlagen** auf **Durchsuchen**, um eine Zertifikat Vorlage auszuwählen, die für die Registrierung von Zertifikaten verwendet wird, die für die OTP-Authentifizierung ausgestellt wurden, und wählen Sie im Dialogfeld **Zertifikat Vorlagen** die Option **daotplogon**. Klicken Sie auf **OK**. Klicken Sie auf **Durchsuchen**, um eine Zertifikat Vorlage auszuwählen, die zum Registrieren des vom RAS-Server verwendeten Zertifikats zum Signieren von OTP-Zertifikat Registrierungsanforderungen verwendet wird, und wählen Sie im Dialogfeld **Zertifikat Vorlagen** die Option **daotprraus**. Klicken Sie auf **OK**. Klicken Sie auf **Weiter**.
10. Klicken Sie auf der Seite **Setup des Remote Zugriffs Servers** auf **Fertigstellen**, und klicken Sie dann auf **Fertig stellen** im Assistenten für DirectAccess-Experten

11. Klicken Sie im Dialogfeld **Remote Zugriffs Überprüfung** auf über **nehmen, warten Sie**, bis die DirectAccess-Richtlinie aktualisiert wurde, und klicken Sie dann auf **Schließen**.
12. Geben Sie im **Start BildschirmPowerShell**. exeein, klicken Sie mit der rechten Maustaste auf **PowerShell**, klicken Sie auf **erweitert**, und klicken Sie dann auf **als Administrator ausführen**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
13. Geben Sie im Windows PowerShell-Fenster **gpupdate/force** ein, und drücken Sie die EINGABETASTE.
14. Schließen Sie die Remote Zugriffs-Verwaltungskonsole, und öffnen Sie Sie erneut. Vergewissern Sie sich, dass alle OTP-Einstellungen

# Schritt 5 Überprüfen der OTP-Integrität auf Edge1

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die folgenden Prozeduren überprüfen, ob OTP ordnungsgemäß konfiguriert wurde und funktionieren, indem Sie die DirectAccess-Server Integritäts Überwachung auf

## **Überprüfen der OTP-Integrität auf Edge1 mithilfe der DirectAccess-Server Integritäts Überwachung**

1. Öffnen Sie auf Edge1 die Remote Zugriffs-Verwaltungs Konsole.
2. Klicken Sie auf **Vorgangs Status**.
3. Vergewissern Sie sich, dass der Status von OTP **funktioniert**.

# Schritt 6 Testen der DirectAccess-Konnektivität aus dem homenet-Subnetz

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die Bereitstellung des einmaligen Kennworts für DirectAccess ist jetzt fertiggestellt, und Sie können damit beginnen, die Konnektivität aus dem homenet-Subnetz zu testen.

## So testen Sie die OTP-Funktionalität aus dem homenet-Subnetz auf CLIENT1

1. Stellen Sie auf CLIENT1 sicher, dass Sie als **User1** angemeldet sind.
2. Geben Sie auf dem **Start BildschirmPowerShell**. `exeein`, klicken Sie mit der rechten Maustaste auf **PowerShell**, klicken Sie auf **erweitert**, und klicken Sie dann auf **als Administrator ausführen**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
3. Geben Sie im Windows PowerShell-Fenster `gupdate/forceein`, und drücken Sie die EINGABETASTE.
4. Entfernen Sie CLIENT1 aus dem Corpnet-Subnetz, und verbinden Sie es mit dem homenet-Subnetz.
5. Öffnen Sie auf CLIENT1 Internet Explorer, geben Sie in der Adressleiste <https://app1.corp.contoso.com/> ein, und drücken Sie die EINGABETASTE. Drücken Sie F5.

Die Site sollte nicht geöffnet werden.

6. Geben Sie auf dem **Start BildschirmRSAein**, und klicken Sie auf **RSA SecurID Token**.
7. Warten Sie, bis der RSA SecurID-Token das einmalige Kennwort ändert, und klicken Sie dann auf **Kopieren**.
8. Klicken Sie im Infobereich auf das Symbol **Netzwerkverbindungen**, um auf die DirectAccess-Medienverwaltung zuzugreifen.
9. Klicken Sie auf die **DirectAccess-Verbindung** von Configuration Manager, und klicken Sie auf **weiter**.
10. Drücken Sie STRG + ALT + ENTF, und klicken Sie auf die Kachel **einmal Kennwort (OTP)**.
11. Fügen Sie die zuvor kopierte achtstellige Ziffer in den Code ein, und klicken Sie auf **OK**. Warten Sie, bis die Authentifizierung fertiggestellt ist. Der Status der DirectAccess-Arbeitsplatz Verbindung wird nun **verbunden**.
12. Geben Sie in Internet Explorer in der Adressleiste <https://app1.corp.contoso.com/> ein, und drücken Sie die EINGABETASTE. Drücken Sie F5. Die Standard-IIS-Website auf APP1 wird angezeigt.
13. Geben Sie in der Internet Explorer-Adressleiste <https://app2.corp.contoso.com/> ein, und drücken Sie die EINGABETASTE. Drücken Sie F5. Die IIS-Standard Website wird auf APP2 angezeigt.
14. Geben Sie auf dem **Start Bildschirm\\app1\\filesein**, und drücken Sie die EINGABETASTE.
15. Doppelklicken Sie im Fenster freigegebene Ordner **Dateien** auf die Datei " **example.txt** ". Der Inhalt der Datei "example.txt" wird angezeigt.
16. Geben Sie auf dem **Start Bildschirm\\app2\\filesein**, und drücken Sie die EINGABETASTE.
17. Doppelklicken Sie im Fenster "freigegebene Ordner **Dateien** " auf die **neue Textdatei "Document.txt"**.

Der Inhalt der neuen Datei "Text Document.txt" wird angezeigt.

# Schritt 7 Testen der DirectAccess-Konnektivität über das Internet

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Die Bereitstellung des einmaligen Kennworts für DirectAccess wurde aus dem homenet-Subnetz getestet und kann nun über das Internet getestet werden.

## So testen Sie die OTP-Funktionalität über das Internet auf CLIENT1

1. Auf CLIENT1 stellen Sie sicher, dass Sie als **User1** angemeldet sind. Verbinden Sie CLIENT1 mit dem Corpnet-Subnetz.
2. Geben Sie auf dem **Start BildschirmPowerShell. exe** ein, klicken Sie mit der rechten Maustaste auf **PowerShell**, klicken Sie auf **erweitert**, und klicken Sie dann auf **als Administrator ausführen**. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
3. Geben Sie im Windows PowerShell-Fenster **gpupdate/force** ein, und drücken Sie die EINGABETASTE.
4. Entfernen Sie die CLIENT1 aus dem homenet-Subnetz, verbinden Sie Sie mit dem Internet, und starten Sie den Computer neu.

5. Öffnen Sie auf CLIENT1 Internet Explorer, geben Sie in der Adressleiste <https://app1.corp.contoso.com/> ein, und drücken Sie die EINGABETASTE. Drücken Sie F5.

Die Site sollte nicht geöffnet werden.

6. Geben Sie auf dem **Start BildschirmRSA** ein, und klicken Sie auf **RSA SecurID Token**.
7. Warten Sie, bis der RSA SecurID-Token das einmalige Kennwort ändert, und klicken Sie dann auf **Kopieren**.
8. Klicken Sie im Infobereich auf das Symbol **Netzwerkverbindungen**, um auf die DirectAccess-Medienverwaltung zuzugreifen.
9. Klicken Sie auf **Arbeitsplatz Verbindung** und dann auf **weiter**.
10. Drücken Sie STRG + ALT + ENTF, und klicken Sie auf die Kachel **einmal Kennwort (OTP)**.
11. Fügen Sie die zuvor kopierte achtstellige Ziffer in den Code ein, und klicken Sie auf **OK**. Warten Sie, bis die Authentifizierung fertiggestellt ist. Der Status der DirectAccess-Arbeitsplatz Verbindung wird nun **verbunden**.
12. Geben Sie in Internet Explorer in der Adressleiste <https://app1.corp.contoso.com/> ein, und drücken Sie die EINGABETASTE. Drücken Sie F5. Die Standard-IIS-Website auf APP1 wird angezeigt.
13. Geben Sie in der Internet Explorer-Adressleiste <https://app2.corp.contoso.com/> ein, und drücken Sie die EINGABETASTE. Drücken Sie F5. Die IIS-Standard Website wird auf APP2 angezeigt.
14. Geben Sie auf dem **Start Bildschirm\\app1\\file** ein, und drücken Sie die EINGABETASTE.
15. Doppelklicken Sie im Fenster freigegebene Ordner **Dateien** auf die Datei " **example. txt** ". Der Inhalt der Datei "example. txt" wird angezeigt.
16. Geben Sie auf dem **Start Bildschirm\\app2\\file** ein, und drücken Sie die EINGABETASTE.

17. Doppelklicken Sie im Fenster "freigegebene Ordner Dateien " auf die **neue Textdatei "Document. txt "**.  
Der Inhalt der neuen Datei "Text Document. txt" wird angezeigt.

# DirectAccess – bekannte Probleme

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

## Empfohlene Hotfixes und Updates für Windows Server 2012 DirectAccess

Über den folgenden Link werden die Dokumente des technischen Supports von Microsoft für DirectAccess aufgelistet, die Sie vor der Bereitstellung überprüfen und anwenden sollten, um eine nicht verwendbare Konfiguration zu vermeiden.

- [Empfohlene Hotfixes und Updates für Windows Server 2012 DirectAccess](#)

# DirectAccess-Kapazitätsplanung

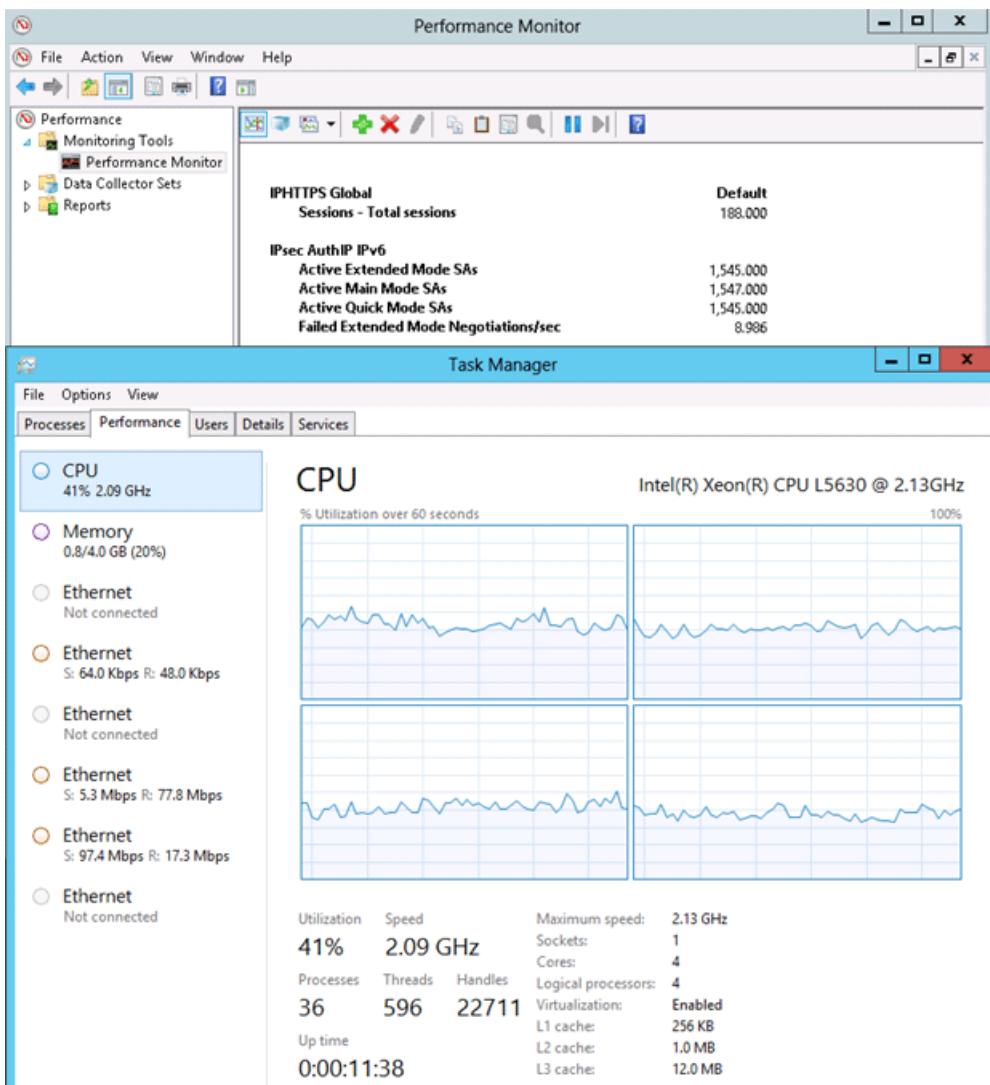
09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Dokument ist ein Bericht zur DirectAccess-Serverleistung von Windows Server 2012. Anhand von Tests wurde die Durchsatzkapazität für Highend-Computerhardware und Lowend-Computerhardware ermittelt. Die CPU-Leistung der Highend- und Lowend-Hardware war vom Durchsatz an Netzwerkdatenverkehr und den Arten der verwendeten Clients abhängig. Eine typische DirectAccess-Bereitstellung (die Grundlage für diese Tests) besteht zu einem Drittel (30 %) aus IPHTTPS-Clients und zu zwei Dritteln (70 %) aus Teredo-Clients. Teredo-Clients bieten teilweise eine höhere Leistung als IPHTTPS-Clients, weil für Windows Server 2012 die empfangsseitige Skalierung (Receive Side Scaling, RSS) verwendet wird, bei der die Nutzung aller CPU-Cores möglich ist. Da bei diesen Tests RSS aktiviert ist, ist das Hyperthreading deaktiviert. Außerdem unterstützt TCP/IP unter Windows Server 2012 den UDP-Datenverkehr, sodass mit Teredo-Clients der Lastenausgleich über mehrere CPUs hinweg durchgeführt werden kann.

Die Daten wurden sowohl für einen Lowend-Server (4 Core, 4 GB) als auch für Hardware erfasst, die eher im Bereich der Highend-Server anzusiedeln ist (8 Core, 8 GB). Im folgenden finden Sie einen Screenshot des neuen Windows 8-Task-Managers auf der Low-End-Hardware mit 750 Clients (562 Teredo, 188 IPHTTPS), die ~ 77 MS/Sek. ausführen. Dies dient zum Simulieren von Benutzern, die keine Smartcard-Anmelde Informationen darstellen.

Diese Testergebnisse zeigen, dass die Leistung von Teredo unter Windows 8 höher als für IPHTTPS ist. Gegenüber Windows 7 hat sich die Bandbreitenauslastung jedoch sowohl für Teredo als auch für IPHTTPS verbessert.



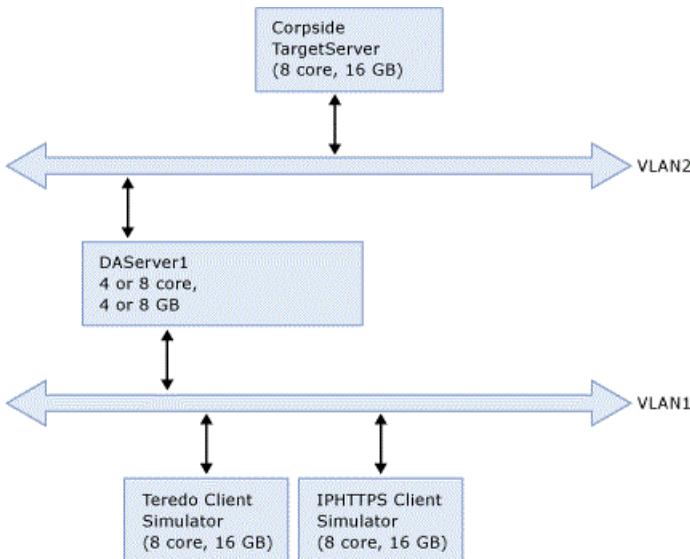
## Testumgebung für Highend-Hardware

Die folgende Tabelle enthält die Ergebnisse, die mit der Testumgebung zum Ermitteln der Leistung für Highend-Hardware erzielt wurden. In diesem Dokument wird auf alle Testergebnisse und Analysen ausführlich eingegangen.

Konfiguration-Hardware	Lowend-Hardware (4 GB RAM, 4 Core)	Highend-Hardware (8 GB RAM, 8 Core)
Doppelter Tunnel -PKI -Einschließlich DNS64/NAT64	750 gleichzeitige Verbindungen bei 50 % CPU, 50 % Arbeitsspeicher mit Corpnet-NIC-Durchsatz von 75 MBit/s. Das %quot;Stretch Target%quot; beträgt 1.000 Benutzer bei 50 % CPU.	1500 gleichzeitige Verbindungen bei 50% CPU, 50% Arbeitsspeicher mit Corpnet-NIC-Durchsatz 150 Mbit/s.

## Testumgebung

### Perf Bench-Topologie



Die Testumgebung für die Leistung ist eine Bench mit fünf Computern. Für den Lowend-Hardwaretest wurde ein 4-Core-DirectAccess-Server mit 4 GB verwendet, und für den Highend-Hardwaretest wurde ein 8-Core-DirectAccess-Server mit 16 GB verwendet. Für Lowend- und Highend-Testumgebungen wurde Folgendes verwendet: ein Back-End-Server (Absender) und zwei Clientcomputer (Empfänger). Die Empfänger sind auf die beiden Clientcomputer aufgeteilt. Andernfalls wären die Empfänger an die CPU gebunden und würden so zu einer Beschränkung der Anzahl von Clients und der Bandbreite führen. Auf der empfangenden Seite wurde ein Simulator zum Simulieren von Hunderten von Clients eingesetzt (Simulation von HTTPS- oder Teredo-Clients). IPsec und DOSp wurden jeweils konfiguriert. RSS ist auf dem DirectAccess-Server aktiviert. Die RSS-Warteschlangengröße ist auf 8 festgelegt. Ohne Konfiguration von RSS weist ein Prozessor eine hohe Auslastung auf, während die anderen Cores über eine zu geringe Auslastung verfügen. Außerdem ist zu beachten, dass der DirectAccess-Server ein 4-Core-Computer mit deaktiviertem Hyperthreading ist. Das Hyperthreading ist deaktiviert, da RSS nur auf physischen Cores funktioniert und die Nutzung von Hyperthreading zu fehlerhaften Ergebnissen führt. (Dies bedeutet, dass nicht alle Cores einheitlich geladen werden.)

## Testergebnisse für Lowend-Hardware:

Die Tests wurden sowohl mit 1.000 Clients als auch mit 750 Clients durchgeführt. In allen Fällen wurde der Datenverkehr zu 70 % auf Teredo und zu 30 % auf IPHTTPS aufgeteilt. Bei allen Tests verlief der TCP-Datenverkehr über Nat64, indem zwei IPsec-Tunnel pro Client verwendet wurden. In allen Tests war die Arbeitsspeicherauslastung gering und die CPU-Auslastung akzeptabel.

### Einzelner Testergebnisse:

Die folgenden Abschnitte enthalten Informationen zu den einzelnen Tests. Im Titel eines Abschnitts sind jeweils die wichtigsten Elemente des Tests gefolgt von einer Zusammenfassung der Ergebnisse angegeben. In einer Tabelle sind dann die ausführlichen Ergebnisse aufgeführt.

#### Low-End-Leistung: 750 Clients, 70/30 Split, 84,17 MBit/Sek. Durchsatz:

Die folgenden drei Tests zeigen die Ergebnisse für Lowend-Hardware. In den unten angegebenen Testläufen wurden 750 Clients mit einem Durchsatz von 84,17 MBit/s und einer Datenverkehrsaufteilung von 562 (Teredo) zu 188 (IPHTTPS) verwendet. Teredo-MTU war auf 1.472 festgelegt, und Teredo-Shunt war aktiviert. Die CPU-Auslastung erreichte bei den drei Tests im Durchschnitt 46,42 %. Die durchschnittliche Arbeitsspeicherauslastung, die als Prozentsatz der zugesicherten Bytes des gesamten verfügbaren Arbeitsspeichers von 4 GB ausgedrückt wird, lag bei 25,95 %.

Szenario	Cpuavg (aus Indikator)	Mbit/s (Corp-Seite)	Mbit/s (Internet seitig)	Aktive qmsa	Aktives mmsa	Arbeitsspeicher Auslastung (4-GB-System)
Low-End-HW. 562 Teredo-Clients. 188 IPHTTPS-Clients.	47,7472542	84,3	119,13	1502,05	1502,1	26,27%
Low-End-HW. 562 Teredo-Clients. 188 IPHTTPS-Clients.	46,3889778	84,146	118,73	1501,25	1501,2	25,90%
Low-End-HW. 562 Teredo-Clients. 188 IPHTTPS-Clients.	45,113082	84,0494	118,43	1546,14	1546,1	25,68%

#### 1000 Clients, 70/30 Teilung, 78 MS/Sek. Durchsatz:

Mit den folgenden drei Tests wurde die Leistung für Lowend-Hardware ermittelt. In den unten angegebenen Testläufen wurden 1.000 Clients mit einem durchschnittlichen Durchsatz von ca. 78,64 MBit/s und einer Datenverkehrsaufteilung von 700 (Teredo) zu 300 (IPHTTPS) verwendet. Teredo-MTU war auf 1.472 festgelegt, und Teredo-Shunt war aktiviert. Die CPU-Auslastung erreichte im Durchschnitt ca. 50,7 %. Die durchschnittliche Arbeitsspeicherauslastung, die als Prozentsatz der zugesicherten Bytes des gesamten verfügbaren Arbeitsspeichers von 4 GB ausgedrückt wird, lag bei ca. 28,7%.

Szenario	Cpuavg (aus Indikator)	Mbit/s (Corp-Seite)	Mbit/s (Internet seitig)	Aktive qmsa	Aktives mmsa	Arbeitsspeicher Auslastung (4-GB-System)
Low-End-HW. 700 Teredo-Clients. 300 IPHTTPS-Clients.	51,28406247	78,6432	113,19	2002,42	1502,1	25,59%
Low-End-HW. 700 Teredo-Clients. 300 IPHTTPS-Clients.	51,06993128	78,6402	113,22	2001,4	1501,2	30,87%

Low-End-HW. 700 Teredo-Clients. 300 IPHTTPS-Clients.	49,75235617	78,6387	113,2	2002,6	1546,1	30,66%
--	-------------	---------	-------	--------	--------	--------

#### 1000 Clients, 70/30 Teilung, 109 MS/Sek. Durchsatz:

In den folgenden drei Testläufen wurden 1.000 Clients mit einem durchschnittlichen Durchsatz von ca. 109,2 MBit/s und einer Datenverkehrsaufteilung von 700 (Teredo) zu 300 (IPHTTPS) verwendet. Teredo-MTU war auf 1.472 festgelegt, und Teredo-Shunt war aktiviert. Die CPU-Auslastung erreichte bei den drei Tests im Durchschnitt ca. 59,06%. Die durchschnittliche Arbeitsspeicherauslastung, die als Prozentsatz der zugesicherten Bytes des gesamten verfügbaren Arbeitsspeichers von 4 GB ausgedrückt wird, lag bei ca. 27,34 %.

Szenario	Cpuavg (aus Indikator)	Mbit/s (Corp-Seite)	Mbit/s (Internet seitig)	Aktive qmsa	Aktives mmsa	Arbeitsspeicher Auslastung (4-GB-System)
Low-End-HW. 700 Teredo-Clients. 300 IPHTTPS-Clients.	59,81640675	108,305	153,14	2001,64	2001,6	24,38%
Low-End-HW. 700 Teredo-Clients. 300 IPHTTPS-Clients.	59,46473798	110,969	157,53	2005,22	2005,2	28,72%
Low-End-HW. 700 Teredo-Clients. 300 IPHTTPS-Clients.	57,89089768	108,305	153,14	1999,53	2018,3	24,38%

#### Testergebnisse für Highend-Hardware:

Die Tests wurden mit 1.500 Clients durchgeführt. Der Datenverkehr wurde zu 70 % auf Teredo und zu 30 % auf IPHTTPS aufgeteilt. Bei allen Tests verlief der TCP-Datenverkehr über Nat64, indem zwei IPsec-Tunnel pro Client verwendet wurden. In allen Tests war die Arbeitsspeicherauslastung gering und die CPU-Auslastung akzeptabel.

#### Einzelner Testergebnisse:

Die folgenden Abschnitte enthalten Informationen zu den einzelnen Tests. Im Titel eines Abschnitts sind jeweils die wichtigsten Elemente des Tests gefolgt von einer Zusammenfassung der Ergebnisse angegeben. In einer Tabelle sind dann die ausführlichen Ergebnisse aufgeführt.

#### 1500 Clients, 70/30 Teilung, 153,2 Mbits/s Durchsatz

Die folgenden fünf Tests zeigen die Ergebnisse für Highend-Hardware. In den unten angegebenen Testläufen wurden 1.500 Clients mit einem durchschnittlichen Durchsatz von 153,2 MBit/s und einer Datenverkehrsaufteilung von 1050 (Teredo) zu 450 (IPHTTPS) verwendet. Die CPU-Auslastung erreichte bei den fünf Tests im Durchschnitt 50,68%. Die durchschnittliche Arbeitsspeicherauslastung, die als Prozentsatz der zugesicherten Bytes des gesamten verfügbaren Arbeitsspeichers von 8 GB ausgedrückt wird, lag bei 22,25 %.

Szenario	Cpuavg (aus Indikator)	Mbit/s (Corp-Seite)	Mbit/s (Internet seitig)	Aktive qmsa	Aktives mmsa	Arbeitsspeicher Auslastung (4-GB-System)
High-End-HW. 1050 Teredo-Clients. 450 IPHTTPS-Clients.	51,712437	157,029	216,29	3000,31	3046	21,58%
High-End-HW. 1050 Teredo-Clients. 450 IPHTTPS-Clients.	48,86020205	151,012	206,53	3002,86	3045,3	21,15%
High-End-HW. 1050 Teredo-Clients. 450 IPHTTPS-Clients.	52,23979519	155,511	213,45	3001,15	3002,9	22,90%
High-End-HW. 1050 Teredo-Clients. 450 IPHTTPS-Clients.	51,26269767	155,09	212,92	3000,74	3002,4	22,91%
High-End-HW. 1050 Teredo-Clients. 450 IPHTTPS-Clients.	50,15751307	154,772	211,92	3000,9	3002,1	22,93%
High-End-HW. 1050 Teredo-Clients. 450 IPHTTPS-Clients.	49,83665607	145,994	201,92	3000,51	3006	22,03%

**Performance Monitor**

File Action View Window Help

Performance Tools

- Monitoring Tools
- Data Collector Sets
  - User Defined
    - IPHTTPS-perf-test
    - Server Manager Perf
  - System
    - Event Trace Sessions
    - Startup Event Trace Sessions
- Reports

IPHTTPS Global

	Default
Sessions - Total sessions	450.000

IPsec AuthIP IPv6

Active Extended Mode SAs	3,004.000
Active Main Mode SAs	3,005.000
Active Quick Mode SAs	3,004.000
Failed Extended Mode Negotiations/sec	27.001

**Task Manager**

File Options View

Processes Performance Users Details Services

CPU 49% 2.22 GHz

Memory 1.7/16.0 GB (11%)

Ethernet S: 56.0 Kbps R: 16.0 Kbps

Ethernet Not connected

Ethernet S: 8.9 Mbps R: 149 Mbps

Ethernet S: 185 Mbps R: 30.9 Mbps

**CPU** Intel(R) Xeon(R) CPU L5630 @ 2.13GHz

% Utilization over 60 seconds

Utilization Speed Maximum speed: 2.13 GHz

49%	2.22 GHz	Maximum speed:	2.13 GHz
Processes	Threads	Sockets:	2
37	824	Cores:	8
Up time		Logical processors:	8
		Virtualization:	Enabled
		L1 cache:	512 KB
		L2 cache:	2.0 MB
		L3 cache:	24.0 MB

[Fewer details](#) | [Open Resource Monitor](#)

# DirectAccess-Offline-Domänenbeitritt

09.04.2020 • 13 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Handbuch werden die Schritte zum Ausführen eines Offline-Domänen Beitritts mit DirectAccess erläutert. Während eines Offline-Domänen Beitritts ist ein Computer so konfiguriert, dass er einer Domäne ohne physische oder VPN-Verbindung Beitritt.

Das Handbuch umfasst folgende Abschnitte:

- Übersicht über den Offline Domänen Beitritt
- Anforderungen an den Offline-Domänen Beitritt
- Offline-Domänen Beitrittsprozess
- Schritte zum Durchführen eines Offline-Domänen Beitritts

## Übersicht über den Offline Domänen Beitritt

Die in Windows Server 2008 R2 eingeführten Domänen Controller enthalten ein Feature namens Offline-Domänen Beitritt. Mit dem Befehlszeilen-Hilfsprogramm Djoin. exe können Sie einen Computer einer Domäne hinzufügen, ohne physisch einen Domänen Controller zu kontaktieren, während der Domänen Beitritts Vorgang abgeschlossen ist. Die allgemeinen Schritte zur Verwendung von "Djoin. exe" lauten wie folgt:

1. Führen Sie **Djoin/Provision** aus, um die Metadaten des Computer Kontos zu erstellen. Bei der Ausgabe dieses Befehls handelt es sich um eine txt-Datei, die ein Base-64-codiertes BLOB enthält.
2. Führen Sie **Djoin/requestODJ** aus, um die Computer Konto Metadaten aus der txt-Datei in das Windows-Verzeichnis des Ziel Computers einzufügen.
3. Starten Sie den Zielcomputer neu, und der Computer wird der Domäne hinzugefügt.

### Szenario "Offline-Domänen Beitritt mit DirectAccess-Richtlinien"

Der DirectAccess-Offline-Domänen Beitritt ist ein Prozess, mit dem Computer, auf denen Windows Server 2016, Windows Server 2012, Windows 10 oder Windows 8 ausgeführt wird, einer Domäne beitreten können, ohne dass Sie physisch mit dem Unternehmensnetzwerk verbunden oder über VPN verbunden ist. Dadurch ist es möglich, Computer einer Domäne von Orten aus hinzuzufügen, an denen keine Verbindung mit einem Unternehmensnetzwerk besteht. Der Offline-Domänen Beitritt für DirectAccess bietet Clients DirectAccess-Richtlinien, um die Remote Bereitstellung zuzulassen.

Bei einem Domänen Beitritt wird ein Computer Konto erstellt und eine Vertrauensstellung zwischen einem Computer mit einem Windows-Betriebssystem und einer Active Directory Domäne hergestellt.

## Vorbereiten des Offline-Domänen Beitritts

1. Erstellen Sie das Computer Konto.
2. Inventarisieren Sie die Mitgliedschaft aller Sicherheitsgruppen, zu denen das Computer Konto gehört.
3. Erfassen Sie die erforderlichen Computer Zertifikate, Gruppenrichtlinien und Gruppenrichtlinien Objekte, die auf die neuen Clients angewendet werden sollen.

. In den folgenden Abschnitten werden die Anforderungen an das Betriebssystem und die Anmelde Informationen für die Ausführung eines DirectAccess-Offline-Domänen Beitritts mithilfe von Djoin.exe erläutert

## Anforderungen an das Betriebssystem

Sie können Djoin.exe nur für DirectAccess auf Computern ausführen, auf denen Windows Server 2016, Windows Server 2012 oder Windows 8 ausgeführt wird. Auf dem Computer, auf dem Sie Djoin.exe ausführen, um Computer Kontodata in AD DS bereitzustellen, muss Windows Server 2016, Windows 10, Windows Server 2012 oder Windows 8 ausgeführt werden. Auf dem Computer, den Sie der Domäne hinzufügen möchten, muss auch Windows Server 2016, Windows 10, Windows Server 2012 oder Windows 8 ausgeführt werden.

## Anforderungen bezüglich der Anmeldeinformationen

Zum Ausführen eines Offline-Domänen Beitritts müssen Sie über die erforderlichen Rechte zum Verknüpfen von Arbeitsstationen zur Domäne verfügen. Mitglieder der Gruppe "Domänen-Admins" verfügen standardmäßig über diese Rechte. Wenn Sie kein Mitglied der Gruppe "Domänen-Admins" sind, muss ein Mitglied der Gruppe "Domänen-Admins" eine der folgenden Aktionen ausführen, damit Sie Arbeitsstationen zur Domäne hinzufügen können:

- Verwenden Sie Gruppenrichtlinie, um die erforderlichen Benutzerrechte zu erteilen. Mit dieser Methode können Sie Computer im Container Standard Computer und in jeder Organisationseinheit erstellen, die später erstellt wird (wenn keine Zugriffs Steuerungs Einträge (ACEs) hinzugefügt werden).
- Bearbeiten Sie die Zugriffs Steuerungs Liste (ACL) des Containers "Standard Computer" für die Domäne, um Ihnen die richtigen Berechtigungen zu delegieren.
- Erstellen Sie eine Organisationseinheit, und bearbeiten Sie die ACL für diese Organisationseinheit, um Ihnen die Berechtigung zum **Erstellen** von untergeordneten Elementen zu erteilen Übergeben Sie den **/machineOU** -Parameter an den **Djoin/Provision** -Befehl.

In den folgenden Verfahren wird gezeigt, wie Sie den Benutzerberechtigungen für Gruppenrichtlinie erteilen und wie Sie die richtigen Berechtigungen delegieren.

### Erteilen von Benutzerrechten zum Hinzufügen von Arbeitsstationen zur Domäne

Mit dem Gruppenrichtlinien-Verwaltungskonsole (GPMC) können Sie die Domänen Richtlinie ändern oder eine neue Richtlinie mit Einstellungen erstellen, mit denen dem Benutzerrechte zum Hinzufügen von Arbeitsstationen zu einer Domäne erteilt werden.

Sie müssen mindestens Mitglied der Gruppe **Domänen-Admins** oder einer entsprechenden Gruppe sein, um Benutzerrechte gewähren zu können. Ausführliche Informationen zur Verwendung der entsprechenden Konten und Gruppenmitgliedschaften finden Sie unter **lokale und Domänen Standard Gruppen** (<https://go.microsoft.com/fwlink/?LinkId=83477>).

So erteilen Sie Rechte zum Verknüpfen von Arbeitsstationen mit einer Domäne

1. Klicken Sie auf **Start**, dann auf **Verwaltung** und anschließend auf **Gruppenrichtlinienverwaltung**.
2. Doppelklicken Sie auf den Namen der Gesamtstruktur, doppelklicken Sie auf **Domänen**, doppelklicken Sie auf den Namen der Domäne, der Sie einen Computer hinzufügen möchten, klicken Sie mit der rechten Maustaste auf **Standard Domänen Richtlinie**, und klicken Sie dann auf **Bearbeiten**.
3. Doppelklicken Sie in der Konsolen Struktur auf **Computer Konfiguration**, doppelklicken Sie auf **Richtlinien**, doppelklicken Sie auf **Windows-Einstellungen**, doppelklicken Sie auf **Sicherheitseinstellungen**, doppelklicken Sie auf **lokale Richtlinien**, und doppelklicken Sie dann auf **Zuweisen von Benutzerrechten**.
4. Doppelklicken Sie im Detail Bereich auf **Arbeitsstationen zur Domäne hinzufügen**.
5. Aktivieren Sie das Kontrollkästchen **Diese Richtlinien Einstellungen definieren**, und klicken Sie dann auf **Benutzer oder Gruppe hinzufügen**.

6. Geben Sie den Namen des Kontos ein, für das Sie dem Benutzerrechte erteilen möchten, und klicken Sie dann zweimal auf OK .

## Offline-Domänen Beitrittsprozess

Führen Sie Djoin.exe an einer Eingabeaufforderung mit erhöhten Rechten aus, um die Computer Konto Metadaten bereitzustellen. Wenn Sie den Bereitstellungs Befehl ausführen, werden die Metadaten des Computer Kontos in einer Binärdatei erstellt, die Sie als Teil des Befehls angeben.

Weitere Informationen zur NetProvisionComputerAccount-Funktion, die zum Bereitstellen des Computer Kontos während eines Offline-Domänen Beitritts verwendet wird, finden Sie unter [NetProvisionComputerAccount-Funktion](https://go.microsoft.com/fwlink/?LinkId=162426) (<https://go.microsoft.com/fwlink/?LinkId=162426>). Weitere Informationen zur Funktion "netrequestofflinedomainjoin", die lokal auf dem Zielcomputer ausgeführt wird, finden Sie unter "netrequestofflinedomainjoin"-Funktion (<https://go.microsoft.com/fwlink/?LinkId=162427>).

## Schritte zum Durchführen eines DirectAccess-Offline-Domänen Beitritts

Der Offline-Domänen Beitrittsprozess umfasst die folgenden Schritte:

1. Erstellen Sie ein neues Computer Konto für jeden der Remote Clients, und generieren Sie mithilfe des Befehls Djoin.exe von einem bereits in eine Domäne eingebundener Computer im Unternehmensnetzwerk ein Bereitstellungs Paket.
2. Hinzufügen des Client Computers zur Sicherheitsgruppe "directaccessclients"
3. Übertragen Sie das Bereitstellungs Paket sicher auf die Remote Computer, die der Domäne beitreten werden.
4. Wenden Sie das Bereitstellungs Paket an, und fügen Sie den Client der Domäne hinzu.
5. Starten Sie den Client neu, um den Domänen Beitritt abzuschließen und eine Verbindung herzustellen.

Beim Erstellen des Bereitstellungs Pakets für den Client sind zwei Optionen zu beachten. Wenn Sie den Assistenten für die ersten Schritte zum Installieren von DirectAccess ohne PKI verwendet haben, sollten Sie unten Option 1 verwenden. Wenn Sie den erweiterten Setup-Assistenten zum Installieren von DirectAccess mit PKI verwendet haben, sollten Sie unten Option 2 verwenden.

Führen Sie die folgenden Schritte aus, um den Offline-Domänen Beitritt auszuführen:

### Option1: Erstellen eines Bereitstellungs Pakets für den Client ohne PKI

1. Geben Sie an einer Eingabeaufforderung des Remote Zugriffs Servers den folgenden Befehl ein, um das Computer Konto bereitzustellen:

```
Djoin /provision /domain <your domain name> /machine <remote machine name> /policynames DA Client GPO  
name /rootcacerts /savefile c:\files\provision.txt /reuse
```

### Option2: Erstellen eines Bereitstellungs Pakets für den Client mit PKI

1. Geben Sie an einer Eingabeaufforderung des Remote Zugriffs Servers den folgenden Befehl ein, um das Computer Konto bereitzustellen:

```
Djoin /provision /machine <remote machine name> /domain <Your Domain name> /policynames <DA Client GPO  
name> /certtemplate <Name of client computer cert template> /savefile c:\files\provision.txt /reuse
```

### Hinzufügen des Client Computers zur Sicherheitsgruppe "directaccessclients"

1. Geben Sie auf dem Domänen Controller auf dem Bildschirm **Start** den Wert **aktiv** ein, und wählen Sie **Active Directory Benutzer und Computer** von **apps** aus.
2. Erweitern Sie die Struktur unter Ihrer Domäne, und wählen Sie den Container **Benutzer** aus.

3. Klicken Sie im Detailfenster mit der rechten Maustaste auf **directaccessclients**, und klicken Sie dann auf **Eigenschaften**.
4. Auf der Registerkarte **Mitglieder** klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Objekttypen**, wählen Sie **Computer** aus, und klicken Sie dann auf **OK**.
6. Geben Sie den hinzu zufügenden Client Namen ein, und klicken Sie dann auf **OK**.
7. Klicken Sie auf **OK**, um das Eigenschaften Dialogfeld von **directaccessclients** zu schließen, und schließen Sie dann **Active Directory Benutzer und Computer**.

Kopieren Sie das Bereitstellungs Paket, und wenden Sie es auf den Client Computer an.

1. Kopieren Sie das Bereitstellungs Paket aus c:\files\provision.txt auf dem Remote Zugriffs Server, auf dem es gespeichert wurde, auf dem Client Computer unter "c:\provision\provision.txt".
2. Öffnen Sie auf dem Client Computer eine Eingabeaufforderung mit erhöhten Rechten, und geben Sie dann den folgenden Befehl ein, um den Domänen Beitritt anzufordern:

```
Djoin /requestodj /loadfile C:\provision\provision.txt /windowspath %windir% /localos
```

3. Starten Sie den Client Computer neu. Der Computer wird der Domäne hinzugefügt. Nach dem Neustart wird der Client der Domäne hinzugefügt und verfügt über eine Verbindung mit dem Unternehmensnetzwerk mit DirectAccess.

## Weitere Informationen

[NetProvisionComputerAccount-Funktion](#)

[Netrequestofflinejoin-Funktion](#)

# Problembehandlung von DirectAccess

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Führen Sie die folgenden Schritte aus, um Probleme mit dem Remote Zugriff (DirectAccess) zu beheben.

Problem:	Lösung
Die DirectAccess-Konfiguration kann von der Remote Zugriffs-Verwaltungskonsole nicht angezeigt werden.	<p><b>So stellen Sie fehlende Konfigurationsinformationen wieder her</b></p> <ul style="list-style-type: none"><li>-Wenn Sie die Problembehandlung bei einer Bereitstellung mit mehreren Standorten durchlaufen, stellen Sie sicher, dass der dem Einstiegspunkt am nächsten liegenden Domänen Controller</li><li>-Verwenden Sie das Cmdlet <b>Get-daentrypointdc</b>, um den Namen des Domänen Controllers abzurufen, der dem Einstiegspunkt am nächsten ist. Wenn der Domänen Controller nicht ausgeführt wird, verwenden Sie das Cmdlet <b>Set-daentrypointdc</b>, um auf einen anderen Domänen Controller zu verweisen.</li><li>-Führen Sie <b>gpresult</b> über eine Eingabeaufforderung mit erhöhten Rechten auf dem Server aus, um sicherzustellen, dass der Server die DirectAccess-Gruppenrichtlinie Objekte erhält.</li><li>-Aktivieren Sie die Protokollierung der Benutzeroberfläche.</li><li>-Verwenden Sie den folgenden Befehl, um die Windows PowerShell-Protokollierung zu starten:</li></ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"><pre>logman create trace ETWTrace -ow -o c:\ETWTrace.etl -p {AAD4C46D-56DE-4F98-BDA2-B5EAEBDD2B04} 0xfffffffffffffff 0xff -nb 16 16 -bs 1024 -mode 0x2 -max 2048 -ets logman update trace ETWTrace -p {62DFF3DA-7513- 4FCA-BC73-25B111FBB1DB} 0xfffffffffffffff 0xff - ets</pre></div> <p>Schließen Sie die Benutzeroberfläche und öffnen Sie Sie erneut. -Deaktivieren der Windows PowerShell-Protokollierung. Sammeln Sie die Protokolldateien der Ereignis Ablauf Verfolgung. Erfassen Sie außerdem alle Protokolle aus dem Ordner "<b>%windir%\\Tracing</b>".</p>

<p>Fehler beim Anwenden der DirectAccess-Konfiguration</p>	<p><b>So aktualisieren Sie die DirectAccess-Konfiguration</b></p> <ul style="list-style-type: none"> <li>-Wenn Sie die Problembehandlung bei einer Bereitstellung mit mehreren Standorten durchlaufen, stellen Sie sicher, dass der dem Einstiegspunkt am nächsten liegenden Domänen Controller</li> <li>-Verwenden Sie das Cmdlet <b>Get-daentrypointdc</b>, um den Namen des Domänen Controllers abzurufen, der dem Einstiegspunkt am nächsten ist. Wenn der Domänen Controller nicht ausgeführt wird, verwenden Sie das Cmdlet <b>Set-daentrypointdc</b>, um auf einen anderen Domänen Controller zu verweisen.</li> <li>-Verwenden Sie den folgenden Befehl, um die Windows PowerShell-Protokollierung zu starten:</li> </ul> <pre>logman create trace ETWTrace -ow -o c:\ETWTrace.etl -p {AAD4C46D-56DE-4F98-BDA2-B5EAEBDD2B04} 0xffffffffffffffffffff 0xff -nb 16 16 -bs 1024 -mode 0x2 -max 2048 -ets logman update trace ETWTrace -p {62DFF3DA-7513- 4FCA-BC73-25B111FBB1DB} 0xffffffffffffffffffff 0xff - ets</pre> <ul style="list-style-type: none"> <li>-Klicken Sie auf übernehmen.</li> <li>-Wenn der Fehler auftritt, deaktivieren Sie die Windows PowerShell-Protokollierung, und erfassen Sie das Ereignis Ablauf Verfolgungs Protokoll.</li> </ul>
<p>DirectAccess ist konfiguriert, Clients können jedoch keine Verbindung mit internen Ressourcen herstellen.</p>	<p><b>So beheben Sie Probleme mit der Client Verbindung</b></p> <ul style="list-style-type: none"> <li>-Klicken Sie in der Remote Zugriffs-Verwaltungskonsole auf die Registerkarte <b>Betriebs Status</b>, und vergewissern Sie sich, dass alle Komponenten ein grünes Symbol aufweisen. Falls nicht, überprüfen Sie die Fehlerdetails, und führen Sie die Lösungsschritte aus.</li> <li>-Führen Sie den Remote Zugriffs Server-Best Practices Analyzer (BPA) aus. Wenn Warnungen oder Fehler vorliegen, führen Sie die Lösungsschritte aus, um das Problem zu beheben.</li> </ul>
<p>Probleme im Zusammenhang mit einer Konfiguration für mehrere Standorte (z. b. Aktivieren einer Multisite, Hinzufügen von Einstiegspunkten oder Festlegen des Domänen Controllers für einen Einstiegspunkt)</p>	<p>Befolgen Sie die Schritte unter Problembehandlung bei <a href="#">einer Bereitstellung für mehrere Standorte</a>.</p>
<p>Die Kachel Konfigurations Status auf dem Dashboard zeigt eine Warnung oder einen Fehler an.</p>	<p>Befolgen Sie die Schritte unter <a href="#">Überwachen des Konfigurations Verteilungs Status des Remote Zugriffs Servers</a>.</p>
<p>Probleme im Zusammenhang mit der Konfiguration des Lastenausgleichs (z. b. bei der Konfiguration tritt ein Fehler auf, wenn Sie einen Lastenausgleich aktivieren oder wenn beim Hinzufügen oder Entfernen von Servern zu einem Cluster Probleme auftreten)</p>	<p>Wenn Sie den Lastenausgleich aktivieren oder einen Knoten hinzufügen und die Konfiguration aktualisiert wurde, als Sie auf <b>anwenden</b> geklickt haben, der Cluster wurde auf dem Server jedoch nicht ordnungsgemäß ausgeführt. Führen Sie den folgenden Befehl aus: cmd. exe/c "reg Add hklm\system\currentcontrolset\services\ramgmtsvc\parameters\f/v Debugflag/t REG_DWORD/d" "0xffffffff" " ", um die Protokolle der Benutzeroberfläche auf dem neuen Server zu</p>

Der Vorgangs Status zeigt nach den folgenden Schritten einen Fehler oder eine Warnung an, um die Situation zu beheben

Wenn der Vorgangs Status falsche Informationen anzeigt (z. b. Fehler, auch nachdem Sie diese behoben haben), gilt Folgendes:

-Aktivieren Sie den Registrierungsschlüssel "cmd. exe"/c  
"reg Add  
hklm\system\currentcontrolset\services\ramgmzvc  
\parameters/f/v EnableTracing/t REG\_DWORD/d"  
"5" " ".  
-Aktualisieren Sie den Vorgangs Status, und erfassen Sie die Protokolle von % windir%\Tracing.

Die DirectAccess-Client Computer unter Windows 8 und höher melden "kein Internet" als Status für die DirectAccess-Verbindung, und die Netzwerkkonkurrenzstatus-Anzeige meldet eingeschränkte Konnektivität.

Dies kann vorkommen, wenn die Tunnel Erzwingung in der DirectAccess-Konfiguration aktiviert ist und daher nur IPHTTPS verwendet werden. Um dieses Problem zu beheben, können Sie einen Proxy Server erstellen und konfigurieren. Ncsi verwendet dann den Proxy Server zum Durchführen von Überprüfungen der Internet Konnektivität. Es wird empfohlen, dass Sie der Richtlinien Tabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) mithilfe des folgenden Verfahrens einen statischen Proxy hinzufügen.

Bevor Sie die Befehle in diesem Verfahren ausführen, müssen Sie sicherstellen, dass alle Domänen Namen, Computernamen und anderen Windows PowerShell-Befehls Variablen durch Werte ersetzt werden, die für die Bereitstellung geeignet sind.

#### Konfigurieren eines statischen Proxys für eine NRPT-Regel

1. zeigen Sie das "." an. NRPT-Regel:

```
Get-DnsClientNrptRule -GpoName  
"corp.example.com\DirectAccess Client Settings" -  
Server <DomainControllerNetBIOSName>
```

2. Notieren Sie sich den Namen (GUID) der "." NRPT-Regel. Der Name (GUID) sollte mit "da-{.}" beginnen.

3. Legen Sie den Proxy für "." fest. NRPT-Regel für  
**Proxy.Corp.example.com:8080**:

```
Set-DnsClientNrptRule -Name "DA-{.}" -Server  
<DomainControllerNetBIOSName> -GPOName  
"corp.example.com\DirectAccess Client Settings" -  
DAProxyServerName "proxy.corp.example.com:8080" -  
DAProxyType "UseProxyName"
```

4. zeigen Sie das "." an. Führen Sie erneut

```
Get-DnsClientNrptRule
```

 aus, und überprüfen Sie, ob  
**proxysqdn: Port** jetzt ordnungsgemäß konfiguriert ist.

5. aktualisieren Sie Gruppenrichtlinie, indem Sie  
`gpupdate /force` auf einem DirectAccess-Client  
ausführen, wenn der Client intern verbunden ist. zeigen  
Sie dann die NRPT mithilfe `Get-DnsClientNrptPolicy`  
an, und überprüfen Sie, ob die ".-Regel proxysqdn:  
Port" angezeigt.

# Bereitstellen eines DirectAccess-Servers mit dem Assistenten für erste Schritte

09.04.2020 • 14 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema bietet eine Einführung in das DirectAccess-Szenario mit einem einzelnen DirectAccess-Server und ermöglicht Ihnen die Bereitstellung von DirectAccess über ein paar einfache Schritte.

Bevor Sie mit der Bereitstellung beginnen, sollten Sie sich die folgende Liste mit nicht unterstützten Konfigurationen, bekannten Problemen und Voraussetzungen ansehen:

In den folgenden Themen finden Sie Informationen zu Voraussetzungen und anderen Informationen vor der Bereitstellung von DirectAccess.

- [DirectAccess: Nicht unterstützte Konfigurationen](#)
- [Erforderliche Komponenten für die Bereitstellung von DirectAccess](#)

## Szenariobeschreibung

In diesem Szenario wird ein einzelner Computer mit Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 in einigen einfachen Assistenten Schritten als DirectAccess-Server mit Standardeinstellungen konfiguriert, ohne dass die Infrastruktur Einstellungen konfiguriert werden müssen. als Zertifizierungsstelle (Certification Authority, ca) oder Active Directory-Sicherheitsgruppen.

### NOTE

Informationen zum Konfigurieren einer erweiterten Bereitstellung mit benutzerdefinierten Einstellungen finden Sie unter [Deploy a Single DirectAccess Server with Advanced Settings](#).

## Inhalt dieses Szenarios

Zum Einrichten eines einfachen DirectAccess-Servers sind mehrere Planungs-und Bereitstellungs Schritte erforderlich.

### Erforderliche Komponenten

Bevor Sie mit der Bereitstellung dieses Szenarios beginnen, sollten Sie die Liste der wichtigen Anforderungen lesen:

- Windows-Firewall muss in allen Profilen aktiviert sein.
- Dieses Szenario wird nur unterstützt, wenn auf den Client Computern Windows 10, Windows 8.1 oder Windows 8 ausgeführt wird.
- ISATAP wird im Unternehmensnetzwerk nicht unterstützt. Wenn Sie ISATAP verwenden, sollten Sie es entfernen und das systemeigene IPv6 verwenden.
- Eine Public Key-Infrastruktur ist nicht erforderlich.

- Die Bereitstellung der zweistufigen Authentifizierung wird nicht unterstützt. Für die Authentifizierung sind Domänenanmeldeinformationen erforderlich.
- DirectAccess wird automatisch auf allen mobilen Computern in der aktuellen Domäne bereitgestellt.
- Datenverkehr zum Internet wird nicht über den DirectAccess-Tunnel übertragen. Die Konfiguration einer Tunnelerzwingung wird nicht unterstützt.
- Der DirectAccess-Server ist der Netzwerkadressenserver.
- Netzwerzugriffsschutz (Network Access Protection, NAP) wird nicht unterstützt.
- Das Ändern von Richtlinien außerhalb der DirectAccess-Verwaltungskonsole oder von PowerShell-Cmdlets wird nicht unterstützt.
- Zum Bereitstellen von mehreren Standorten, jetzt oder in Zukunft, stellen Sie zunächst [einen einzelnen DirectAccess-Server mit erweiterten Einstellungen](#) bereit.

## **Planungsschritte**

Die Planung besteht aus zwei Phasen:

1. Planen der DirectAccess-Infrastruktur. Diese Phase beschreibt die erforderlichen Planungsschritte zum Einrichten der Netzwerkinfrastruktur vor der DirectAccess-Bereitstellung. Dazu gehört die Planung von Netzwerk- und Servertopologie und DirectAccess-Netzwerkadressenserver.
2. Planen der DirectAccess-Bereitstellung. Diese Phase beschreibt die erforderlichen Planungsschritte zur Vorbereitung der DirectAccess-Bereitstellung. Dazu gehört die Planung für DirectAccess-Clientcomputer, Server- und Clientauthentifizierungsanforderungen, VPN-Einstellungen, Infrastrukturserver sowie Verwaltungs- und Anwendungsserver.

Ausführliche Planungsschritte finden Sie unter [Planen einer erweiterten DirectAccess-Bereitstellung](#).

## **Bereitstellungsschritte**

Die Bereitstellung besteht aus drei Phasen:

1. Konfigurieren der DirectAccess-Infrastruktur: Diese Phase umfasst das Konfigurieren von Netzwerk und Routing, das Konfigurieren der Firewallemstellungen (falls erforderlich), das Konfigurieren von Zertifikaten, DNS-Servern, Active Directory- und GPO-Einstellungen und DirectAccess Servers.
2. Konfigurieren von DirectAccess-Serveereinstellungen. Die Phase beinhaltet Schritte zum Konfigurieren von DirectAccess-Clientcomputern, DirectAccess-Server, Infrastrukturservern sowie Verwaltungs- und Anwendungsservern.
3. Überprüfen der Bereitstellung. Diese Phase umfasst Schritte zum Überprüfen, ob die Bereitstellung nach Bedarf funktioniert.

Informationen zu den Bereitstellungsschritten finden Sie unter [Install and Configure Basic DirectAccess](#).

## **Praktische Anwendungen**

Die Bereitstellung eines einzelnen Remotezugriffsservers bietet Folgendes:

- Einfache Zugriffsberechtigung. Verwaltete Client Computer, auf denen Windows 10, Windows 8.1, Windows 8 oder Windows 7 ausgeführt wird, können als DirectAccess-Clients konfiguriert werden. Diese Clients können immer, wenn sie im Internet sind, über DirectAccess auf interne Netzwerkressourcen zugreifen, ohne sich über eine VPN-Verbindung einzuloggen. Clientcomputer, die keines dieser Betriebssysteme verwenden, können über herkömmliche VPN-Verbindungen eine Verbindung mit dem internen Netzwerk herstellen.

- Einfache Verwaltung. Die Remoteverwaltung von DirectAccess-Clientcomputern im Internet ist mithilfe von RAS-Administratoren über DirectAccess möglich, selbst wenn die Clientcomputer sich nicht im internen Unternehmensnetzwerk befinden. Clientcomputer, die nicht den Unternehmensanforderungen entsprechen, können automatisch über Verwaltungsserver gewartet werden. Sowohl DirectAccess als auch VPN werden über dieselbe Konsole und mit denselben Assistenten verwaltet. Außerdem können einer oder mehrere RAS-Server über eine einzelne Remotezugriffs-Verwaltungskonsole verwaltet werden.

## In diesem Szenario enthaltene Rollen und Features

Die folgende Tabelle enthält die für dieses Szenario erforderlichen Rollen und Features:

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Remotezugriffs-Rolle	<p>Die Rolle wird über die Server-Manager-Konsole oder Windows PowerShell installiert bzw. deinstalliert. Diese Rolle umfasst DirectAccess (zuvor ein Feature unter Windows Server 2008 R2) sowie die Routing- und RAS-Dienste (zuvor ein Rollendienst unter der Serverrolle für Netzwerkrichtlinien- und Zugriffsdienste). Die Remotezugriffs-Rolle besteht aus zwei Komponenten:</p> <ol style="list-style-type: none"> <li>1. DirectAccess-und RRAS-VPN (Routing and Remote Access Services). DirectAccess und VPN werden in der Remote Zugriffs-Verwaltungskonsole verwaltet.</li> <li>2. RRAS-Routing. RRAS-Routing Features werden in der Legacy-Routing-und Remote Zugriffs Konsole verwaltet.</li> </ol> <p>Die RAS-Serverrolle ist von den folgenden Serverrollen/features abhängig:</p> <ul style="list-style-type: none"> <li>-Internetinformationsdienste (IIS)-Webserver: dieses Feature ist erforderlich, um den Netzwerkadressen Server auf dem Remote Zugriffs Server und den Standardweb Test zu konfigurieren.</li> <li>-Interne Windows-Datenbank. Wird zur lokalen Ressourcenerfassung auf dem Remotezugriffsserver verwendet.</li> </ul>
Feature "Tools für die Remotezugriffsverwaltung"	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"> <li>-Sie wird standardmäßig auf einem RAS-Server installiert, wenn die Remote Zugriffs Rolle installiert ist, und unterstützt die Benutzeroberfläche der Remote Verwaltungskonsole und Windows PowerShell-Cmdlets.</li> <li>-Es kann optional auf einem Server installiert werden, auf dem die Remote Zugriffs-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.</li> </ul> <p>Das Feature "Tools für die Remotezugriffsverwaltung" besteht aus den folgenden Komponenten:</p> <ul style="list-style-type: none"> <li>-Remote Zugriffs-GUI</li> <li>-Remote Zugriffs Modul für Windows PowerShell</li> </ul> <p>Abhängigkeiten umfassen:</p> <ul style="list-style-type: none"> <li>-Gruppenrichtlinien-Verwaltungskonsole</li> <li>-RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li> <li>-Windows PowerShell 3,0</li> <li>-Tools und Infrastruktur für die grafische Verwaltung</li> </ul>

# Hardwareanforderungen

Für dieses Szenario müssen die folgenden Hardwareanforderungen erfüllt werden:

- Serveranforderungen:
  - Ein Computer, der die Hardwareanforderungen für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 erfüllt.
  - Auf dem Server muss mindestens ein Netzwerkadapter installiert, aktiviert und mit dem internen Netzwerk verbunden sein. Werden zwei Adapter verwendet, sollte ein Adapter mit dem internen Unternehmensnetzwerk und der andere mit dem externen Netzwerk (Internet oder privates Netzwerk) verbunden sein.
  - Mindestens ein Domänencontroller. RAS-Server und DirectAccess-Clients müssen Domänenmitglieder sein.
- Clientanforderungen:
  - Auf einem Client Computer muss Windows 10, Windows 8.1 oder Windows 8 ausgeführt werden.

## IMPORTANT

Wenn auf einigen oder allen Client Computern Windows 7 ausgeführt wird, müssen Sie den erweiterten Setup-Assistenten verwenden. Der in diesem Dokument beschriebene Setup-Assistent für die ersten Schritte unterstützt keine Client Computer, auf denen Windows 7 ausgeführt wird. Anweisungen zur Verwendung von Windows 7-Clients mit DirectAccess finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).

## NOTE

Nur die folgenden Betriebssysteme können als DirectAccess-Clients verwendet werden: Windows 10 Enterprise, Windows 8.1 Enterprise, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 8 Enterprise, Windows Server 2008 R2, Windows 7 Enterprise und Windows 7 Ultimate.

- Anforderungen an Infrastruktur und Verwaltungsserver:
  - Falls ein VPN aktiviert und kein statischer IP-Adressenpool konfiguriert ist, müssen Sie einen DHCP-Server bereitstellen, um VPN-Clients automatisch IP-Adressen zuzuweisen.
- Es ist ein DNS-Server erforderlich, auf dem Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 SP2 oder Windows Server 2008 R2 ausgeführt wird.

# Software Anforderungen

Für dieses Szenario gelten eine Reihe von Anforderungen:

- Serveranforderungen:
  - Der Remotezugriffsserver muss Domänenmitglied sein. Der Server kann an der Schwelle zum internen Netzwerks oder geschützt durch eine Edgefirewall oder ein anderes Gerät bereitgestellt werden.
  - Wird der RAS-Server durch eine Edgefirewall oder ein NAT-Gerät geschützt, muss das Gerät so konfiguriert sein, dass ein- und ausgehender Datenverkehr für den RAS-Server zugelassen wird.
  - Die Person, die den Remotezugriff auf dem Server einrichtet, muss lokale Administratorberechtigungen für den Server und Benutzerberechtigungen für die Domäne besitzen.

Zusätzlich benötigt der Administrator Berechtigungen für die Gruppenrichtlinien, die bei der DirectAccess-Bereitstellung verwendet werden. Um die Features nutzen zu können, die die DirectAccess-Bereitstellung auf mobile Computer beschränken, ist die Berechtigung zum Erstellen von WMI-Filters für den Domänencontroller erforderlich.

- RAS-Client-Anforderungen:
  - DirectAccess-Clients müssen Domänenmitglieder sein. Domänen, die Clients enthalten, können zur selben Gesamtstruktur gehören wie der Remotezugriffsserver oder eine bidirektionale Vertrauensstellung mit der Remotezugriffsserver-Gesamtstruktur innehaben.
  - Eine Active Directory-Sicherheitsgruppe wird benötigt, um die Computer aufzunehmen, die als DirectAccess-Clients konfiguriert werden. Wird beim Konfigurieren der DirectAccess-Cienteinstellungen keine Sicherheitsgruppe angegeben, wird das Client-Gruppenrichtlinienobjekt standardmäßig auf alle Laptopcomputer in der Sicherheitsgruppe „Domänencomputer“ angewendet. Nur die folgenden Betriebssysteme können als DirectAccess-Clients verwendet werden: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows 8 Enterprise, Windows 7 Enterprise und Windows 7 Ultimate.

## Siehe auch

Die folgende Tabelle enthält Links zu zusätzlichen Ressourcen.

ART DES INHALTS	VERWEISE
Remote Zugriff auf TechNet	<a href="#">Remote Zugriff-TechCenter</a>
Tools und Einstellungen	<a href="#">PowerShell-Cmdlets für den Remote Zugriff</a>
Communityressourcen	<a href="#">DirectAccess-wiki-Einträge</a>
Verwandte Technologien	<a href="#">Funktionsweise von IPv6</a>

# Planen einer allgemeinen DirectAccess-Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema werden die erforderlichen Planungsschritte für die Bereitstellung eines einzelnen DirectAccess-Servers beschrieben, auf dem Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 mit grundlegenden Features ausgeführt wird:

1. [Schritt 1: Planen der grundlegenden DirectAccess-Infrastruktur](#) Planen der Netzwerk- und Server Topologie, Firewalleinstellungen, Zertifikat Anforderungen, DNS und Active Directory.
2. [Schritt 2: Planen der grundlegenden Bereitstellung von DirectAccess-Bereitstellungs](#) Plan Clients und-Servern

## Nächster Schritt

Wenn Sie diese Planungsschritte abgeschlossen haben, können Sie mit der Bereitstellung des Servers beginnen. Anweisungen hierzu finden Sie unter [Installieren und Konfigurieren von Basic DirectAccess](#).

# Schritt 1 Planen der grundlegenden DirectAccess-Infrastruktur

09.04.2020 • 33 minutes to read • [Edit Online](#)

Der erste Schritt bei einer einfachen DirectAccess-Bereitstellung auf einem einzelnen Server ist die Planung der Infrastruktur, die für die Bereitstellung erforderlich ist. In diesem Thema werden die Schritte zur Planung der Infrastruktur beschrieben:

AUFGABE	BESCHREIBUNG
Planen der Netzwerktopologie und -einstellungen	Entscheiden Sie, wo der DirectAccess-Server (auf dem Edge oder hinter einer Netzwerk Adressübersetzung (NAT) Gerät oder Firewall) platziert werden soll, und planen Sie IP-Adressierung und Routing.
Planen der Firewallanforderungen	Planen Sie, DirectAccess über Edge-Firewalls zuzulassen.
Planen der Zertifikatanforderungen	DirectAccess kann Kerberos oder Zertifikate zur Clientauthentifizierung verwenden. In dieser einfachen DirectAccess-Bereitstellung wird ein Kerberos-Proxy automatisch konfiguriert, die Authentifizierung erfolgt über die Active Directory-Anmeldeinformationen.
Planen der DNS-Anforderungen	Planen Sie die DNS-Einstellungen für den DirectAccess-Server, Infrastrukturserver und die Client-Konnektivität.
Planen von Active Directory	Planen Sie Ihre Domänencontroller und die Active Directory-Anforderungen.
Planen von Gruppenrichtlinienobjekten	Entscheiden Sie, welche Gruppenrichtlinienobjekte in Ihrer Organisation erforderlich sind und wie diese erstellt oder bearbeitet werden.

Diese Planungsaufgaben müssen nicht in einer bestimmten Reihenfolge durchgeführt werden.

## Planen der Netzwerktopologie und -Einstellungen

### Planen von Netzwerkadapters und IP-Adressierung

1. Identifizieren Sie die Netzwerkadaptertopologie, die Sie verwenden möchten. DirectAccess kann mit folgenden Optionen eingerichtet werden:

- Mit zwei Netzwerkadapters: entweder am Edge mit einem Netzwerkadapter, der mit dem Internet verbunden ist, der andere mit dem internen Netzwerk oder hinter einem NAT-, Firewall-oder Routergerät, wobei ein Netzwerkadapter mit einem Umkreis Netzwerk und der andere mit dem internen Netzwerkadapter verbunden ist. Netzwerk.
- Hinter einem NAT-Gerät mit einem Netzwerkadapter wird der DirectAccess-Server hinter einem NAT-Gerät installiert, und der einzige Netzwerkadapter wird mit dem internen Netzwerk verbunden.

2. Identifizieren Sie Ihre IP-Adressierungsanforderungen:

DirectAccess verwendet IPv6 mit IPsec, um eine sichere Verbindung zwischen DirectAccess-Clientcomputern

und dem internen Unternehmensnetzwerk herzustellen. Jedoch erfordert DirectAccess nicht unbedingt Konnektivität mit dem IPv6-Internet oder nativen IPv6-Support auf internen Netzwerken. Stattdessen konfiguriert und verwendet es automatisch IPv6-Übergangs Technologien, um IPv6-Datenverkehr über das IPv4-Internet (IPv6-zu-IPv4-, Teredo-, IP-HTTPS-) und über Ihr IPv4--Intranet (NAT64 oder ISATAP) zu Tunnels. Eine Übersicht über diese Übergangstechnologien finden Sie in folgenden Ressourcen:

- [IPv6-Übergangs Technologien](#)
- [IP-HTTPS-tunnelingprotokollspezifikation](#)

3. Konfigurieren Sie erforderliche Adapter und Adressen entsprechend folgender Tabelle. Bei bereit Stellungen hinter einem NAT-Gerät mit einem einzelnen Netzwerkadapter sollten Sie Ihre IP-Adressen nur mit der Spalte **interner Netzwerkadapter** konfigurieren.

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER <sup>1</sup>	ROUTINGANFORDERUNGE N
IPv4-Intranet und IPv4-Internet	Konfigurieren Sie Folgendes: -Eine statische öffentliche IPv4-Adresse mit der entsprechenden Subnetzmaske. -Eine Standard Gateway-IPv4-Adresse Ihrer Internet Firewall oder eines lokalen Internetdienstanbieters (ISP) Router.	Konfigurieren Sie Folgendes: : Eine IPv4- Intranetadresse mit der entsprechenden Subnetzmaske. : Eine Verbindung- bestimmtes DNS-Suffix des Intranetnamespaces. Zudem sollte ein DNS- Server auf der internen Schnittstelle konfiguriert werden. -Konfigurieren Sie kein Standard Gateway auf Intranetschnittstellen.	Gehen Sie wie folgt vor, um den DirectAccess- Server so zu konfigurieren, dass er alle Subnetze auf dem internen IPv4- Netzwerk erreicht: 1. Listen Sie die IPv4- Adressbereiche für alle Speicherorte im Intranet auf. 2. verwenden Sie den Befehl <b>Route Add -p</b> oder <b>Netsh Interface IPv4 Add Route</b> , um die IPv4- Adressbereiche als statische Routen in der IPv4-Routing Tabelle des DirectAccess- Servers hinzuzufügen.

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv6-Internet und IPv6-Intranet	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>-Verwenden Sie die automatisch konfigurierte Adress Konfiguration, die von Ihrem ISP bereitgestellt wird.</li> <li>Verwenden Sie den Befehl <b>Route Print</b>, um sicherzustellen, dass in der IPv6-Routing Tabelle eine IPv6-Standardroute vorhanden ist, die auf den ISP-Router zeigt.</li> <li>: Bestimmen Sie, ob der ISP-und der Intranetrouter in RFC 4191 beschriebene Standard Router-Einstellungen verwenden, und verwenden Sie eine höhere Standardeinstellung als ihre lokalen Intranetrouter. Wenn beide Fälle zutreffen, ist keine weitere Konfiguration für die Standardroute erforderlich. Die höhere Präferenz für den ISP-Router stellt sicher, dass die aktive IPv6-Standardroute des DirectAccess-Servers auf das IPv6-Internet zeigt.</li> </ul> <p>Wenn Sie über eine systemeigene IPv6-Infrastruktur verfügen, kann die Internetschnittstelle außerdem auch die Domänencontroller im Intranet erreichen, da der DirectAccess-Server ein IPv6-Router ist. Fügen Sie in diesem Fall Paketfilter zum Domänen Controller im Umkreis Netzwerk hinzu, die Konnektivität mit der IPv6-Adresse der Internet-Schnittstelle des DirectAccess-Servers verhindern.</p>	<p>Konfigurieren Sie Folgendes:</p> <p>Wenn Sie keine Standard Einstellungsebenen verwenden, konfigurieren Sie Ihre Intranetschnittstellen mit dem Befehl <b>Netsh Interface IPv6 Set interfaceindex ignoredefaultroutes =aktiviert</b>. Dieser Befehl stellt sicher, dass der IPv6-Routingtabelle keine weiteren Standardrouten hinzugefügt werden, die auf Intranetrouter zeigen. Den SchnittstellenIndex Ihrer Intranetschnittstellen können Sie mit dem Befehl <b>netsh interface show interface</b> anzeigen.</p>	<p>Wenn Sie ein IPv6-Intranet haben, führen Sie folgende Schritte aus, um den DirectAccess-Server so zu konfigurieren, dass er alle IPv6-Speicherorte erreicht:</p> <ol style="list-style-type: none"> <li>1. Listen Sie die IPv6-Adressräume für alle Speicherorte im Intranet auf.</li> <li>2. verwenden Sie den Befehl <b>Netsh Interface IPv6 Add Route</b>, um die IPv6-Adressbereiche als statische Routen in der IPv6-Routing Tabelle des DirectAccess-Servers hinzuzufügen.</li> </ol>

IPv4-Internet und IPv6-Intranet	EXTERNER NETZWERKADAPTER Server leitet den Datenverkehr für	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
	die Standard-IPv6-Route mit dem Microsoft-IP6-zu-IP4-Adapter an ein IP6-zu-IP4-Relay im IPv4-Internet weiter. Sie können einen DirectAccess-Server für die IPv4-Adresse des Microsoft IPv6-zu-IPv4-Relay im IPv4-Internet (konfigurieren, das verwendet wird, wenn System eigenes IPv6 nicht im Unternehmensnetzwerk) bereitgestellt wird. verwenden Sie dazu den folgenden Befehl: Netsh Interface IPv6 6zu 4 Set Relay Name=192.88.99.1 State=aktivierter Befehl.		

#### NOTE

Beachten Sie Folgendes:

1. Wenn dem DirectAccess-Client eine öffentliche IPv4-Adresse zugewiesen wurde, verwendet diese die IP6-zu-IP4-Übergangstechnologie für die Verbindung mit dem Internet. Wenn der DirectAccess-Client mit IPv6-zu-IPv4 keine Verbindung mit dem DirectAccess-Server herstellen kann, wird IP-HTTPS verwendet.
2. Systemeigene IPv6-Clientcomputer können über eine systemeigene IPv6 eine Verbindung zum DirectAccess-Server herstellen, und es ist keine Übergangstechnologie erforderlich.

#### Planen der Firewallanforderungen

Wenn sich der DirectAccess-Server hinter einer Edge-Firewall befindet, sind folgende Ausnahmen für DirectAccess-Datenverkehr erforderlich, wenn sich der DirectAccess-Server auf dem IPv4-Internet befindet:

- IPv6-zu-IPv4-Datenverkehr-IP-Protokoll 41 eingehend und ausgehend.
- IP-HTTPS-Transmission Control Protocol (TCP) Zielport 443 und TCP-Quellport 443 ausgehend.
- Wenn Sie den Remotezugriff mit einem einzigen Netzwerkadapter bereitstellen und den Netzwerkadressenserver auf dem DirectAccess-Server installieren, sollte TCP-Port 62000 ebenfalls ausgenommen werden.

#### NOTE

Diese Ausnahme befindet sich auf dem DirectAccess-Server. Alle weiteren Ausnahmen befinden sich auf der Firewall.

Die folgenden Ausnahmen sind für DirectAccess-Datenverkehr erforderlich, wenn sich der DirectAccess-Server auf dem IPv6-Internet befindet:

- IP-Protokoll 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend.

Wenden Sie bei zusätzlichen Firewalls die folgenden internen Netzwerkfirewallausnahmen für DirectAccess-Datenverkehr an:

- ISATAP-Protokoll 41 eingehend und ausgehend
- TCP-/UDP für den gesamten IPv4-/IPv6-Datenverkehr

### **Planen der Zertifikat Anforderungen**

Zertifikatanforderungen für IPsec beinhalten ein Computerzertifikat, das von DirectAccess-Clientcomputern verwendet wird, wenn diese die IPsec-Verbindung zwischen dem Client und dem DirectAccess-Server herstellen, und einem Computerzertifikat, das von DirectAccess-Servern für das Aufbauen von IPsec-Verbindungen mit DirectAccess-Clients verwendet wird. Für DirectAccess in Windows Server 2012 R2 und Windows Server 2012 ist die Verwendung dieser IPSec-Zertifikate nicht obligatorisch. Der Assistent für erste Schritte konfiguriert den DirectAccess-Server als Kerberos-Proxy, damit die IPsec-Authentifizierung ohne erforderliche Zertifikate durchgeführt werden kann.

- 1. IP--HTTPS-Server.** Wenn Sie DirectAccess konfigurieren, wird der DirectAccess-Server automatisch als IP--HTTPS-Weblistener konfiguriert. Die IP--HTTPS-Website erfordert ein Website Zertifikat, und Client Computer müssen in der Lage sein, eine Verbindung mit der Zertifikat Sperr Liste (CRL-) Standort für das Zertifikat zu erhalten. Der Assistent zum Aktivieren von DirectAccess versucht, das SSTP VPN-Zertifikat zu verwenden. Wenn SSTP nicht konfiguriert ist, prüft er, ob im persönlichen Speicher des Computers ein Zertifikat für IP-HTTPS vorhanden ist. Wenn keine verfügbar ist, wird automatisch ein selbst-signiertes Zertifikat erstellt.
- 2. Netzwerkadressenserver.** Der Netzwerkadressen Server ist eine Website, mit der erkannt wird, ob sich Client Computer im Unternehmensnetzwerk befinden. Der Netzwerkadressen Server erfordert ein Website Zertifikat. DirectAccess-Clients müssen die CRL-Website für das Zertifikat kontaktieren können. Der Assistent zum Aktivieren des Remote Zugriffs prüft, ob im persönlichen Speicher des Computers ein Zertifikat für den Netzwerkadressen Server vorhanden ist. Wenn nicht vorhanden, wird automatisch ein selbst-signiertes Zertifikat erstellt.

Die einzelnen Zertifikatanforderungen werden in der folgenden Tabelle zusammengefasst:

IPSEC-AUTHENTIFIZIERUNG	IP--HTTPS-SERVER	NETZWERKADRESSEN SERVER
Eine interne Zertifizierungsstelle ist erforderlich, um Computer Zertifikate an den DirectAccess-Server und Clients für die IPsec-Authentifizierung auszugeben, wenn Sie nicht den Kerberos-Proxy für die Authentifizierung verwenden.	Öffentliche Zertifizierungsstelle: Es wird empfohlen, eine öffentliche Zertifizierungsstelle zum Ausstellen des IP--HTTPS-Zertifikats zu verwenden. Dadurch wird sichergestellt, dass der CRL-Verteilungs Punkt extern verfügbar ist.	Interne Zertifizierungsstelle: Sie können eine interne Zertifizierungsstelle verwenden, um das Netzwerkadressen Server-Website Zertifikat auszustellen. Stellen Sie sicher, dass der Sperrlisten-Verteilungspunkt eine hohe Verfügbarkeit vom internen Netzwerk aus hat.
	Interne Zertifizierungsstelle: Sie können eine interne Zertifizierungsstelle zum Ausstellen des IP--HTTPS-Zertifikats verwenden. Sie müssen jedoch sicherstellen, dass der CRL-Verteilungs Punkt extern verfügbar ist.	Selbst-signiertes Zertifikat: Sie können ein selbst-signiertes Zertifikat für die Netzwerkadressen Server-Website verwenden. Es ist jedoch nicht möglich, ein selbst-signiertes Zertifikat in bereit Stellungen mit mehreren Standorten zu verwenden.
	Selbst-signiertes Zertifikat: Sie können ein selbst-signiertes Zertifikat für den IP--HTTPS-Server verwenden; Sie müssen jedoch sicherstellen, dass der CRL-Verteilungs Punkt extern verfügbar ist. Ein selbst-signiertes Zertifikat kann nicht in einer Bereitstellung für mehrere Standorte verwendet werden.	

## Planen von Zertifikaten für IP-HTTPS und den Netzwerkadressen Server

Wenn Sie zu diesem Zweck ein Zertifikat bereistellen möchten, finden Sie dazu unter [Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) weitere Informationen. Wenn keine Zertifikate verfügbar sind, erstellt der Assistent für die ersten Schritte automatisch selbst-signierte Zertifikate für diese Zwecke.

### NOTE

Wenn Sie Zertifikate für IP-HTTPS und den Netzwerkadressen Server manuell bereistellen, stellen Sie sicher, dass die Zertifikate einen Antragsteller Namen aufweisen. Wenn das Zertifikat keinen Antragstellernamen hat, jedoch über einen alternativen Namen verfügt, wird es vom DirectAccess-Assistenten nicht akzeptiert.

## Planen der DNS-Anforderungen

In einer DirectAccess-Bereitstellung ist DNS für Folgendes erforderlich:

- **DirectAccess-Clientanforderungen.** DNS wird verwendet, um Anforderungen von DirectAccess-Clientcomputern aufzulösen, die sich nicht im internen Netzwerk befinden. DirectAccess-Clients versuchen, eine Verbindung zum DirectAccess-Netzwerkadressenserver herzustellen, um zu bestimmen, ob sie sich im Internet oder auf dem internen Netzwerk befinden: Bei erfolgreicher Verbindung werden die Clients als im Intranet befindlich identifiziert, DirectAccess wird nicht verwendet, und Clientanforderungen werden mithilfe des DNS-Servers aufgelöst, welcher auf dem Netzwerkadapter des Clientcomputers konfiguriert ist. Wenn keine Verbindung hergestellt werden kann, wird davon ausgegangen, dass sich die Clients im Internet befinden. DirectAccess-Clients verwenden die Richtlinien Tabelle für die Namensauflösung (NRPT-), um zu bestimmen, welcher DNS-Server beim Auflösen von namens Anforderungen verwendet werden soll. Sie können angeben, dass Clients DirectAccess-DNS64 oder einen anderen internen DNS-Server für die Auflösung von Namen verwenden. Wenn Sie eine Namensauflösung durchführen, wird die NRPT von DirectAccess-Clients verwendet, um festzulegen, wie eine Anfrage behandelt werden soll. Clients fordern einen voll qualifizierten Namen oder einen Namen für eine einzelne Bezeichnung an, z. B. `http://Internal`. Wenn ein einzelner Bezeichnungs Name Anforderungen ist, wird ein DNS-Suffix angehängt, um einen FQDN zu erstellen. Wenn die DNS-Abfrage einem Eintrag in der NRPT entspricht, und DNS4 oder ein Intranet-DNS-Server für den Eintrag angegeben wurde, wird die Abfrage für die Namensauflösung mithilfe des angegebenen Servers gesendet. Wenn eine Übereinstimmung vorhanden ist, aber kein DNS-Server angegeben wurde, weist dies auf eine Ausnahmeregel hin, und die normale Namensauflösung wird verwendet.

Wenn ein neues Suffix zur NRPT in der DirectAccess-Verwaltungskonsole hinzugefügt wird, können die Standard-DNS-Server für das Suffix automatisch erkannt werden, wenn Sie auf **Erkennen** klicken. Die automatische Erkennung funktioniert wie folgt:

1. Wenn das Unternehmensnetzwerk IPv4-basiert oder IPv4 und IPv6 ist, ist die Standardadresse die DNS64-Adresse des internen Adapters auf dem DirectAccess-Server.
2. Wenn das Unternehmensnetzwerk IPv6--basiert, ist die Standardadresse die IPv6-Adresse der DNS-Server im Unternehmensnetzwerk.

### • Infrastruktur Server

1. **Netzwerkadressenserver.** DirectAccess-Clients versuchen, den Netzwerkadressenserver zu erreichen, um zu bestimmen, ob sie sich auf dem internen Netzwerk befinden. Clients im internen Netzwerk müssen in der Lage sein, den Namen des Netzwerkadressenservers aufzulösen, befinden sie sich jedoch im Internet, dürfen sie den Namen nicht auflösen. Um dies zu gewährleisten, wird der FQDN des Netzwerkadressenservers standardmäßig als Ausnahmeregel zum NRPT hinzugefügt. Außerdem werden bei der Konfiguration von DirectAccess folgende Regeln automatisch erstellt:
  - a. Eine DNS-Suffixregel für die Stammdomäne oder den Domänennamen des DirectAccess-Servers und die IPv6-Adressen, die den auf dem DirectAccess-Server konfigurierten Intranet-

DNS-Servern entsprechen. Wenn der DirectAccess-Server z. B. Mitglied der Domäne corp.contoso.com ist, wird für das DNS-Suffix .corp.contoso.com eine Regel erstellt.

- b. Eine Ausnahmeregel für den FQDN des Netzwerkadressenservers. Wenn die Netzwerkadressen Server-URL z. b. <https://nls.Corp.contoso.com> ist, wird eine Ausnahme Regel für den voll qualifizierten Namen nls.Corp.contoso.com erstellt.

**IP--HTTPS-Server.** Der DirectAccess-Server fungiert als IP--HTTPS-Listener und verwendet das Serverzertifikat zur Authentifizierung bei IP--HTTPS-Clients. Der Name der IP--HTTPS muss von DirectAccess-Clients mit öffentlichen DNS-Servern aufgelöst werden können.

**Verbindungsprüfer.** DirectAccess erstellt einen Standardwebtest, der von DirectAccess-Clientcomputern dazu verwendet wird, die Verbindung mit dem internen Netzwerk zu prüfen. Damit der Test wie erwartet funktioniert, müssen folgende Namen manuell in dem DNS registriert werden:

- a. DirectAccess--WebProbe Host: sollte in die interne IPv4-Adresse des DirectAccess-Servers oder die IPv6-Adresse in einer reinen IPv6--Umgebung aufgelöst werden.
- b. DirectAccess--corpconnectivityhost-sollte in localhost (Loopback) Adresse aufgelöst werden. Ein A- und AAAA-Eintrag sollte erstellt werden, der A-Eintrag mit dem Wert 127.0.0.1 und der AAAA-Eintrag mit dem aus dem NAT64-Präfix und den letzten 32-Bit als 127.0.0.1 ermittelten Wert. Das NAT64-Präfix kann durch Ausführen des Cmdlets Get-netnattransitionconfiguration abgerufen werden.

Mithilfe anderer Webadressen über HTTP oder PING können Sie weitere Verbindungsprüfer erstellen. Für jeden Verbindungsprüfer muss ein DNS-Eintrag vorhanden sein.

#### DNS-Serveranforderungen

- Für DirectAccess-Clients müssen Sie einen DNS-Server verwenden, auf dem Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 oder ein beliebiger DNS-Server ausgeführt wird, der IPv6 unterstützt.

#### NOTE

Es wird nicht empfohlen, DNS-Server zu verwenden, auf denen Windows Server 2003 ausgeführt wird, wenn Sie DirectAccess bereitstellen. Windows Server 2003-DNS-Server unterstützen zwar IPv6-Datensätze, doch Windows Server 2003 wird nicht mehr von Microsoft unterstützt. Darüber hinaus sollten Sie DirectAccess nicht bereitstellen, wenn auf Ihren Domänencontrollern Windows Server 2003 aufgrund eines Problems mit dem Dateireplikationsdienst ausgeführt wird. Weitere Informationen finden Sie unter [DirectAccess: nicht unterstützte Konfigurationen](#).

#### Planen des Netzwerkadressen Servers

Der Netzwerkadressenserver ist eine Website, die erkennt, ob sich DirectAccess-Clients im Unternehmensnetzwerk befinden. Clients im Unternehmensnetzwerk verwenden kein DirectAccess, um interne Ressourcen zu erreichen, stattdessen stellen Sie direkt eine Verbindung her.

Der Assistent für erste Schritte richtet den Netzwerkadressenserver auf dem DirectAccess-Server automatisch ein und die Website wird beim Bereitstellen von DirectAccess automatisch erstellt. So ist eine einfache Installation möglich, ohne eine Zertifikatinfrastruktur verwenden zu müssen.

Wenn Sie einen Netzwerkadressen Server bereitstellen und keine selbst-signierten Zertifikate verwenden möchten, finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) Weitere Informationen.

#### Plan Active Directory

DirectAccess verwendet Active Directory und Active Directory Gruppenrichtlinien Objekte wie folgt:

- **Authentifizierung.** Active Directory wird für die Authentifizierung verwendet. Der DirectAccess-Tunnel

verwendet für den Benutzer die Kerberos-Authentifizierung, um auf interne Ressourcen zuzugreifen.

- **Gruppenrichtlinienobjekte.** DirectAccess erfasst Konfigurationseinstellungen in Gruppenrichtlinienobjekten, die auf DirectAccess-Server und -Clients angewendet werden.
- **Sicherheitsgruppen.** DirectAccess verwendet Sicherheitsgruppen, um DirectAccess-Clientcomputer und DirectAccess-Server zu erfassen und zu identifizieren. Die Gruppenrichtlinien werden auf die erforderlichen Sicherheitsgruppen angewendet.

## Active Directory Anforderungen

Bei der Planung von Active Directory für eine DirectAccess-Bereitstellung ist Folgendes erforderlich:

- Mindestens ein Domänen Controller, der unter Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008 installiert ist.

Wenn sich der Domänen Controller in einem Umkreis Netzwerk befindet (und daher über den Internet-Netzwerkadapter des DirectAccess-Servers erreichbar ist) verhindern Sie, dass der DirectAccess-Server ihn erreicht, indem Sie dem Domänen Controller Paketfilter hinzufügen, um die Konnektivität mit der IP-Adresse des Internet Adapters zu verhindern.

- Der DirectAccess-Server muss Domänenmitglied sein.
- DirectAccess-Clients müssen Domänenmitglieder sein. Clients können folgenden Domänen angehören:
  - Domänen, die zur gleichen Gesamtstruktur wie der DirectAccess-Server gehören.
  - Alle Domänen, die über eine zwei--Wege-Vertrauensstellung mit der DirectAccess-Server Domäne verfügen.
  - Eine beliebige Domäne in einer Gesamtstruktur, die zwei--Wege-Vertrauensstellung mit der Gesamtstruktur aufweist, zu der die DirectAccess-Domäne gehört.

### NOTE

- Der DirectAccess-Server kann nicht als Domänencontroller verwendet werden.
- Der für DirectAccess verwendete Active Directory Domänen Controller darf nicht vom externen Internet Adapter des DirectAccess-Servers aus erreichbar sein (der Adapter darf sich nicht im Domänen Profil der Windows-Firewall) befinden.

## Planen von Gruppenrichtlinie Objekten

Die beim Konfigurieren von DirectAccess konfigurierten DirectAccess-Einstellungen werden in Gruppenrichtlinien Objekten (GPO)erfasst. Die beiden Gruppenrichtlinienobjekte werden mit DirectAccess-Einstellungen aufgefüllt und wie folgt verteilt:

- **DirectAccess-Client-Gruppenrichtlinienobjekt.** Dieses Gruppenrichtlinienobjekt enthält die Client-Einstellungen, einschließlich der Einstellungen für die IPv6-Übergangstechnologie, der Einträge in der Richtlinientabelle für die Namensauflösung und der Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit. Das Gruppenrichtlinienobjekt wird auf die für die Clientcomputer angegebenen Sicherheitsgruppen angewendet.
- **DirectAccess-Server-Gruppenrichtlinienobjekt.** Dieses Gruppenrichtlinienobjekt enthält die DirectAccess-Konfigurationseinstellungen, die auf den als DirectAccess-Server konfigurierten Server in Ihrer Bereitstellung angewendet werden. Außerdem enthält es die Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit.

Es gibt zwei Möglichkeiten, Gruppenrichtlinienobjekte zu konfigurieren:

1. **Automatisch.** Sie können angeben, dass sie automatisch erstellt werden. Für jedes

Gruppenrichtlinienobjekt wird ein Standardname angegeben. Gruppenrichtlinienobjekte werden automatisch vom Assistenten für erste Schritte erstellt.

2. **Manuell**. Sie können Gruppenrichtlinienobjekte verwenden, die vom Active Directory-Administrator vordefiniert wurden.

Beachten Sie, dass keine anderen Gruppenrichtlinienobjekte mehr konfiguriert werden können, nachdem DirectAccess auf die Verwendung bestimmter Gruppenrichtlinienobjekte konfiguriert wurde.

#### **IMPORTANT**

Unabhängig davon, ob Sie automatisch oder manuell konfigurierte Gruppenrichtlinienobjekte verwenden, müssen Sie für die Erkennung langsamer Verbindungen eine Richtlinie hinzufügen, wenn die Clients 3G verwenden. Der Gruppenrichtlinie Pfad für Richtlinie: Konfigurieren Sie Gruppenrichtlinie Erkennung langsamer Verbindungen ist: Computer Konfiguration / Richtlinien / administrative Vorlagen / System / Gruppenrichtlinie.

#### **Caution**

Verwenden Sie das folgende Verfahren, um alle DirectAccess-Gruppenrichtlinie Objekte zu sichern, bevor Sie DirectAccess-Cmdlets ausführen: [Sichern und Wiederherstellen der DirectAccess-Konfiguration](#)

#### **Automatisch erstellte Gruppenrichtlinien Objekte-**

Beachten Sie bei der Verwendung von automatisch-erstellten Gruppenrichtlinien Objekten Folgendes:

Automatisch erstellte Gruppenrichtlinienobjekte werden entsprechend des Speicherorts und Verknüpfungszielparameters wie folgt angewendet:

- Bei Gruppenrichtlinienobjekten des DirectAccess-Servers zeigen der Speicherort und die Verknüpfungsparameter auf die Domäne, die den DirectAccess-Server enthält.
- Beim Erstellen der Gruppenrichtlinienobjekte wird der Speicherort auf eine Domäne festgelegt, auf der das Gruppenrichtlinienobjekt erstellt wird. Der Gruppenrichtlinienobjektname wird in jeder Domäne nachgeschlagen und mit DirectAccess-Einstellungen aufgefüllt, falls vorhanden. Das Verknüpfungsziel wird auf den Stamm der Domäne festgelegt, in der das Gruppenrichtlinienobjekt erstellt wurde. Für jede Domäne, die Clientcomputer enthält, wird ein Gruppenrichtlinienobjekt erstellt, und das Gruppenrichtlinienobjekt wird mit dem Stamm der entsprechenden Domäne verknüpft.

Beim Verwenden automatisch erstellter Gruppenrichtlinienobjekte benötigt der DirectAccess-Serveradministrator folgende Berechtigungen:

- Schreibberechtigungen für die Gruppenrichtlinienobjekte für jede Domäne.
- Verknüpfungsberechtigungen für alle ausgewählten Clientdomänenstämme.
- Verknüpfungsberechtigungen für die Server-Gruppenrichtlinien-Domänenstämme.
- Erstellen, Bearbeiten und Löschen von Sicherheitsberechtigungen, die für die Gruppenrichtlinienobjekte erforderlich sind.
- Es wird empfohlen, dass der DirectAccess-Administrator über Leserechte für Gruppenrichtlinienobjekte für jede Domäne verfügt. So kann DirectAccess prüfen, dass beim Erstellen von Gruppenrichtlinienobjekten keine Gruppenrichtlinienobjekte mit doppelten Namen vorhanden sind.

Beachten Sie, dass eine Warnung ausgegeben wird, wenn die korrekten Berechtigungen zum Verknüpfen der Gruppenrichtlinienobjekte nicht vorhanden sind. Der DirectAccess-Vorgang wird fortgesetzt, Verknüpfungen werden jedoch nicht erstellt. Wenn diese Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, selbst wenn die Berechtigungen zu einem späteren Zeitpunkt hinzugefügt werden. Stattdessen muss der Administrator die Links manuell erstellen.

#### **Manuelles-erstellte Gruppenrichtlinien Objekte**

Beachten Sie Folgendes, wenn Sie manuell erstellten GPOs verwenden:

- Die Gruppenrichtlinienobjekte sollten vorhanden sein, bevor Sie den Assistenten für erste Schritte mit dem Remotezugriff ausführen.
- Wenn Sie die DirectAccess-Einstellungen manuell erstellten Gruppenrichtlinien Objekten verwenden, benötigt der DirectAccess-Administrator vollständige GPO-Berechtigungen (bearbeiten, löschen und Ändern der Sicherheits) auf den manuell erstellten Gruppenrichtlinien Objekten.
- Beim Verwenden manuell erstellter Gruppenrichtlinienobjekte wird in der gesamten Domäne eine Suche nach einer Verknüpfung zum Gruppenrichtlinienobjekt durchgeführt. Wenn das Gruppenrichtlinienobjekt in der Domäne nicht verknüpft ist, wird im Domänenstamm automatisch eine Verknüpfung erstellt. Wenn die zum Erstellen der Verknüpfung erforderlichen Berechtigungen nicht verfügbar sind, wird eine Warnung ausgegeben.

Beachten Sie, dass eine Warnung ausgegeben wird, wenn die korrekten Berechtigungen zum Verknüpfen der Gruppenrichtlinienobjekte nicht vorhanden sind. Der DirectAccess-Vorgang wird fortgesetzt, Verknüpfungen werden jedoch nicht erstellt. Wenn diese Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, selbst wenn die Berechtigungen zu einem späteren Zeitpunkt hinzugefügt werden. Stattdessen muss der Administrator die Links manuell erstellen.

#### **Wiederherstellen eines gelöschten Gruppenrichtlinienobjekts**

Wenn ein Gruppenrichtlinien Objekt für den DirectAccess-Server, das Client- oder Anwendungsserver versehentlich gelöscht wurde und keine Sicherung verfügbar ist, müssen Sie die Konfigurationseinstellungen entfernen und die Konfiguration erneut-. Wenn eine Sicherung verfügbar ist, können Sie das Gruppenrichtlinienobjekt aus der Sicherung wiederherstellen.

In der **DirectAccess-Verwaltung** wird die folgende Fehlermeldung angezeigt: **GPO- nicht gefunden**. Führen Sie folgende Schritte aus, um die Konfigurationseinstellungen zu entfernen:

1. Führen Sie das PowerShell-Cmdlet **deinstallieren-Remote Accessaus**.
2. Öffnen Sie die **DirectAccess-Verwaltung**erneut-.
3. In der angezeigten Fehlermeldung werden Sie darauf hingewiesen, dass das Gruppenrichtlinienobjekt nicht gefunden werden konnte. Klicken Sie auf **Konfigurationseinstellungen entfernen**. Nach Abschluss des Abschlusses wird der Server in einen nicht-konfigurierten Zustand wieder hergestellt.

#### **Nächster Schritt**

- [Schritt 2: Planen der grundlegenden DirectAccess-Bereitstellung](#)

# Schritt 2 Planen der grundlegenden DirectAccess-Bereitstellung

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nach dem Planen der DirectAccess-Infrastruktur ist der nächste Schritt der Bereitstellung von DirectAccess auf einem einzelnen Server mit grundlegenden Einstellungen das Planen der Einstellungen für den Assistenten für die ersten Schritte.

AUFGABE	BESCHREIBUNG
Planen der Clientbereitstellung	Standardmäßig stellt der Assistent für die ersten Schritte DirectAccess für alle Laptops und Notebook Computer in der Domäne bereit, indem er einen WMI-Filter auf das Gruppenrichtlinien Objekt für die Client Einstellungen anwendet.
Planen der DirectAccess-Server Bereitstellung	Planen Sie die Bereitstellung des DirectAccess-Servers.

## Planen der Client Bereitstellung

Bei der Planung Ihrer Clientbereitstellung müssen zwei Entscheidungen getroffen werden:

1. Soll DirectAccess für alle oder nur für mobile Computer verfügbar sein?

Wenn Sie DirectAccess-Clients im Assistenten für die ersten Schritte konfigurieren, können Sie festlegen, dass nur Mobile Computer in den angegebenen Sicherheitsgruppen mithilfe von DirectAccess eine Verbindung herstellen können. Wenn Sie den Zugriff auf mobile Computer einschränken, konfiguriert DirectAccess automatisch einen WMI-Filter, um sicherzustellen, dass das DirectAccess-Client-GPO nur auf mobile Computer in den angegebenen Sicherheitsgruppen angewendet wird. Der DirectAccess-Administrator benötigt Berechtigungen zum Erstellen oder Ändern von WMI-Filtern für Gruppenrichtlinien, um diese Einstellung zu aktivieren.

2. In welchen Sicherheitsgruppen sollen die DirectAccess-Clientcomputer enthalten sein?

Die DirectAccess-Einstellungen befinden sich in dem Gruppenrichtlinienobjekt des DirectAccess-Clients. Das Gruppenrichtlinien Objekt wird auf Computer angewendet, die Teil der Sicherheitsgruppen sind, die Sie im Assistenten für die ersten Schritte angeben. Sie können angeben, dass Sicherheitsgruppen in einer beliebigen unterstützten Domäne enthalten sein sollen. Bevor Sie DirectAccess konfigurieren, sollten die Sicherheitsgruppen erstellt werden. Nachdem Sie die DirectAccess-Bereitstellung abgeschlossen haben, können Sie der Sicherheitsgruppe Computer hinzufügen. Beachten Sie jedoch, dass das Client-Gruppenrichtlinien Objekt nicht auf diese Clients angewendet wird, wenn Sie die Client Computer, die sich in einer anderen Domäne befinden, der Sicherheitsgruppe hinzufügen. Wenn Sie beispielsweise SG1 in Domäne A für DirectAccess-Clients erstellen und später Clients von Domäne B zu dieser Gruppe hinzufügen, wird das Client-Gruppenrichtlinienobjekt nicht auf Clients von Domäne B angewendet. Sie können dieses Problem vermeiden, indem Sie eine neue Client-Sicherheitsgruppe für jede Domäne erstellen, die die Clientcomputer enthält. Alternativ dazu können Sie auch das Add-DAClient-Cmdlet mit dem Namen des neuen Gruppenrichtlinienobjekts für die neue Domäne ausführen, wenn Sie keine neue Sicherheitsgruppe erstellen möchten.

# Planen der DirectAccess-Server Bereitstellung

Bei der Planung der Bereitstellung des DirectAccess-Servers müssen Sie eine Reihe von Entscheidungen treffen:

- **Netzwerktopologie** : bei der Bereitstellung eines DirectAccess-Servers sind zwei Topologien verfügbar:
  - **Zwei Adapter** : mit zwei Netzwerkadapters kann DirectAccess mit einem direkt mit dem Internet verbundenen Netzwerkadapter konfiguriert werden, während der andere mit dem internen Netzwerk verbunden ist. Alternativ kann der Server hinter einem Edgegerät installiert werden, wie z. B. einer Firewall oder einem Router. In dieser Konfiguration ist ein Netzwerkadapter mit dem Umkreisnetzwerk und der andere mit dem internen Netzwerk verbunden.
  - **Einzelner Netzwerkadapter** : in dieser Konfiguration wird der DirectAccess-Server hinter einem Edgegerät wie z. b. einer Firewall oder einem Router installiert. Der Netzwerkadapter ist mit dem internen Netzwerk verbunden.
- **Netzwerkadapter** : der DirectAccess-Assistent erkennt automatisch die auf dem DirectAccess-Server konfigurierten Netzwerkadapter. Sie können sicherstellen, dass die richtigen Adapter auf der Seite überprüfen ausgewählt sind.
- **IP-HTTPS-Zertifikat** : da in dieser Bereitstellung keine PKI erforderlich ist, stellt der Assistent automatisch selbst signierte Zertifikate für IP-HTTPS und den Netzwerkadressen Server (wenn keine Zertifikate vorhanden sind) bereit und aktiviert den Kerberos-Proxy automatisch. Der Assistent aktiviert auch NAT64 und DNS64 für die Protokoll Übersetzung in der reinen IPv4-Umgebung. Nachdem der Assistent die Konfiguration erfolgreich angewendet hat, klicken Sie auf **Schließen**.
- **Windows 7-Clients** : Sie können die Unterstützung für Windows 7-Clients nicht über den Assistanten für die ersten Schritte aktivieren. Dies kann über den erweiterten Setup-Assistenten aktiviert werden. Weitere Informationen finden Sie unter Bereitstellen [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#).
- **VPN-Konfiguration** : entscheiden Sie vor dem Konfigurieren von DirectAccess, ob Sie VPN-Zugriff auf Remote Clients bereitstellen möchten. Sie sollten VPN-Zugriff bereitstellen, wenn Sie in Ihrer Organisation über Client Computer verfügen, die keine DirectAccess-Konnektivität unterstützen (weil Sie entweder nicht verwaltet sind oder ein Betriebssystem ausführen, für das DirectAccess nicht unterstützt wird). Der Assistent für die ersten Schritte konfiguriert die VPN-IP-Adresszuweisung mithilfe von DHCP und konfiguriert VPN-Clients für die Authentifizierung mit Active Directory.
- **Erzwingen von Tunneln** : Wenn Sie die Tunnel Erzwingung verwenden oder in Zukunft hinzufügen möchten, sollten Sie die Bereitstellung [eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen](#) verwenden, um eine Konfiguration mit zwei Tunneln bereitzustellen. Aufgrund von Sicherheitsüberlegungen wird die Tunnel Erzwingung in einer einzelnen Tunnel Konfiguration nicht unterstützt.

## Vorheriger Schritt

- [Schritt 1: Planen der grundlegenden DirectAccess-Infrastruktur](#)

# Installieren und Konfigurieren von DirectAccess (allgemein)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Diese Übersicht bietet eine Einführung in die Konfigurationsschritte, die für die Bereitstellung eines einzelnen DirectAccess-Servers erforderlich sind, auf dem Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 mit grundlegenden Einstellungen ausgeführt wird.

- [Schritt 1: Konfigurieren der grundlegenden DirectAccess-Infrastruktur](#). Dieser Schritt umfasst die Konfiguration der Netzwerk- und Servereinstellungen sowie der DNS- und Active Directory-Einstellungen.
- [Schritt 2: Konfigurieren Sie den grundlegenden DirectAccess-Server](#). Dieser Schritt umfasst die Konfiguration der DirectAccess-Clientcomputer- und -Servereinstellungen.
- [Schritt 3: Überprüfen](#) Sie die bereit Stellungen. Dieser Schritt dient der Überprüfung Ihrer Bereitstellung.

Bevor Sie mit der Bereitstellung beginnen, müssen Sie die in [Planen einer einfachen DirectAccess-Bereitstellung](#) erläuterten Planungsschritte prüfen.

# Schritt 1 Konfigurieren der grundlegenden DirectAccess-Infrastruktur

09.04.2020 • 20 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird die Konfiguration der Infrastruktur beschrieben, die für eine grundlegende DirectAccess-Bereitstellung mit einem einzelnen DirectAccess-Server in einer gemischten IPv4- und IPv6-Umgebung erforderlich ist. Vergewissern Sie sich vor Beginn der Bereitstellungs Schritte, dass Sie die in [Planen einer einfachen DirectAccess-Bereitstellung](#)beschriebenen Planungsschritte abgeschlossen haben.

AUFGABE	BESCHREIBUNG
Konfigurieren von Servernetzwerkeinstellungen	Konfigurieren Sie die Servernetzwerkeinstellungen auf dem DirectAccess-Server.
Konfigurieren des Routings im Unternehmensnetzwerk	Konfigurieren Sie das Routing im Unternehmensnetzwerk, damit der Datenverkehr ordnungsgemäß weitergeleitet wird.
Konfigurieren von Firewalls	Konfigurieren Sie bei Bedarf zusätzliche Firewalls.
Konfigurieren des DNS-Servers	Konfigurieren Sie die DNS-Einstellungen für den DirectAccess-Server.
Konfigurieren von Active Directory	Fügen Sie der Active Directory-Domäne Clientcomputer und DirectAccess-Server hinzu.
Konfigurieren der Gruppenrichtlinienobjekte	Konfigurieren Sie bei Bedarf Gruppenrichtlinienobjekte für die Bereitstellung.
Konfigurieren von Sicherheitsgruppen	Konfigurieren Sie Sicherheitsgruppen, die DirectAccess-Clientcomputer und weitere Sicherheitsgruppen enthalten, die für die Bereitstellung erforderlich sind.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## Konfigurieren von Servernetzwerk Einstellungen

Für eine einzelne Serverbereitstellung in einer Umgebung mit IPv4 und IPv6 sind folgende Netzwerkschnittstelleneinstellungen erforderlich. Sämtliche IP-Adressen können im **Netzwerk- und Freigabecenter** von Windows mit der Option **Adapttereinstellungen ändern** konfiguriert werden.

- Edgetopologie
  - Eine öffentliche statische IPv4- oder IPv6-Adresse mit Internetzugriff.

#### **NOTE**

Zwei aufeinander folgende öffentliche IPv4-Adressen sind für Teredo erforderlich. Falls Sie Teredo nicht verwenden, können Sie eine einzelne, öffentliche, statische IPv4-Adresse konfigurieren.

- Eine einzelne, interne, statische IPv4- oder IPv6-Adresse
- Hinter einem NAT-Gerät (mit zwei Netzwerkadapters)
  - Eine einzelne, interne, statische IPv4- oder IPv6-Adresse mit Netzwerkzugriff
  - Eine einzelne statische IPv4- oder IPv6-Adresse mit Umkreisnetzwerkzugriff.
- Hinter einem NAT-Gerät (mit einem Netzwerkadapter)
  - Eine einzelne, statische IPv4- oder IPv6-Adresse.

#### **NOTE**

Für den Fall, dass der DirectAccess-Server zwei oder mehr Netzwerkadapter besitzt (einer, der in dem Domänenprofil klassifiziert ist, und der andere in einem öffentlichen/privaten Profil), jedoch nur eine einzelne NIC-Topologie verwendet wird, wird Folgendes empfohlen:

1. Vergewissern Sie sich, dass der zweite Netzwerkadapter und zusätzliche Netzwerkadapter im Domänenprofil klassifiziert sind.
2. Wenn die zweite NIC aus einem bestimmten Grund nicht für das Domänenprofil konfiguriert werden kann, muss der Bereich für die DirectAccess IPsec-Richtlinie manuell mithilfe der folgenden Windows PowerShell-Befehle festgelegt werden:

```
$gposession = Open-NetGPO -PolicyStore <Name of the server GPO>
Set-NetIPsecRule -DisplayName <Name of the IPsec policy> -GPOSession $gposession -Profile Any
Save-NetGPO -GPOSession $gposession
```

Die Namen der IPsec-Richtlinien lauten „DirectAccess-DaServerToInfra“ und „DirectAccess-DaServerToCorp“.

## Konfigurieren des Routings im Unternehmensnetzwerk

Konfigurieren Sie das Routing im Unternehmensnetzwerk wie folgt:

- Wenn in der Organisation eine systemeigene IPv6-Adresse bereitgestellt wird, fügen Sie ihr eine Route hinzu, damit die Router im internen Netzwerk den IPv6-Datenverkehr zurück über den Remotezugriffsserver leiten.
- Konfigurieren Sie die IPv4- und IPv6-Routen der Organisation manuell auf den Remotezugriffsservern. Fügen Sie eine öffentliche Route hinzu, sodass der gesamte Datenverkehr mit Organisations-IPv6-Präfix (/48) an das interne Netzwerk weitergeleitet wird. Fügen Sie außerdem für IPv4-Datenverkehr explizite Routen hinzu, damit IPv4-Datenverkehr an das interne Netzwerk weitergeleitet wird.

## Konfigurieren von Firewalls

Wenden Sie bei zusätzlichen Firewalls in der Bereitstellung die folgenden Firewallausnahmen mit Internetzugriff für RAS-Datenverkehr an, wenn der RAS-Server sich im IPv4-Internet befindet:

- IPv6-zu-IPv4-Datenverkehr-IP-Protokoll 41 eingehend und ausgehend.
- IP-HTTPS-TCP (Transmission Control Protocol)-Zielport 443 und TCP-Quellport 443 ausgehend. Hat der

RAS-Server nur einen Netzwerkadapter und der Netzwerkadressenserver ist auf dem RAS-Server, wird auch TCP-Port 62000 benötigt.

**NOTE**

Diese Ausnahme muss auf dem RAS-Server konfiguriert werden. Alle anderen Ausnahmen müssen in der Edgefirewall konfiguriert werden.

**NOTE**

Bei Teredo- und IP6-zu-IP4-Datenverkehr sollten diese Ausnahmen für beide aufeinander folgenden öffentlichen IPv4-Adressen mit Internetzugriff auf dem RAS-Server angewendet werden. Bei IP-HTTPS müssen die Ausnahmen nur auf die Adresse angewendet werden, die zur Auflösung des externen Namens des Servers dient.

Wenden Sie bei zusätzlichen Firewalls die folgenden Firewallausnahmen mit Internetzugriff für RAS-Datenverkehr an, wenn der RAS-Server sich im IPv6-Internet befindet:

- IP-Protokoll 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend.

Wenden Sie bei zusätzlichen Firewalls die folgenden internen Netzwerkfirewallausnahmen für RAS-Datenverkehr an:

- ISATAP-Protokoll 41 eingehend und ausgehend
- TCP/UDP für den gesamten IPv4/IPv6-Datenverkehr

## Konfigurieren des DNS-Servers

Sie müssen einen DNS-Eintrag für die Netzwerkadressenserver-Website für das interne Netzwerk in Ihrer Bereitstellung manuell konfigurieren.

### So erstellen Sie die DNS-Einträge für den Netzwerkadressen Server und den ncsi-Test

1. Führen Sie auf dem internen Netzwerk-DNS-Server **dnsmgmt. msc** aus, und drücken Sie dann die EINGABETASTE.
2. Erweitern Sie im linken Bereich der **DNS-Manager**-Konsole die Forward-Lookupzone für Ihre Domäne. Klicken Sie mit der rechten Maustaste auf die Domäne, und anschließend auf **Neuer Host (A oder AAAA)**.
3. Geben Sie im Dialogfeld **Neuer Host** in das Feld **Name (bei Nichtangabe wird übergeordnete Domäne verwendet)** den DNS-Namen für die Netzwerkadressenserver-Website (mit diesem Namen verbinden sich die DirectAccess-Clients mit dem Netzwerkadressenserver) ein. Geben Sie in das Feld **IP-Adresse** die IPv4-Adresse des Netzwerkadressenservers ein und klicken Sie dann auf **Host hinzufügen**. Klicken Sie im Dialogfeld **DNS** auf **OK**.
4. Geben Sie im Dialogfeld **Neuer Host** in das Feld **Name (bei Nichtangabe wird übergeordnete Domäne verwendet)** den DNS-Namen des Webtests ein (der Name für Standard-Webtests lautet directaccess-webprobehost). Geben Sie in das Feld **IP-Adresse** die IPv4-Adresse des Webtests ein und klicken Sie dann auf **Host hinzufügen**. Wiederholen Sie diesen Vorgang für directaccess-corpconnectivityhost und manuell erstellte Verbindungsprüfer. Klicken Sie im Dialogfeld **DNS** auf **OK**.
5. Klicken Sie auf **Fertig**.

### Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes

Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address  
<network_location_server_IPv4_address>  
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address  
<network_location_server_IPv6_address>
```

Außerdem müssen Sie die DNS-Einträge für folgende Elemente konfigurieren:

- **Der IP-HTTPS-Server** : DirectAccess-Clients müssen in der Lage sein, den DNS-Namen des Remote Zugriffs Servers aus dem Internet aufzulösen.
- **CRL -Sperr Überprüfung**: DirectAccess verwendet Zertifikat Sperr Überprüfungen für die IP-HTTPS-Verbindung zwischen DirectAccess-Clients und dem RAS-Server sowie für die HTTPS-basierte Verbindung zwischen dem DirectAccess-Client und dem Netzwerkadressen Server. In beiden Fällen müssen DirectAccess-Clients in der Lage sein, auf den Zertifikatsperrlisten-Verteilungspunkt zuzugreifen und ihn aufzulösen.

## Konfigurieren von Active Directory

Der Remotezugriffsserver und alle DirectAccess-Clientcomputer müssen zu einer Active Directory-Domäne zusammengeführt werden. DirectAccess-Clientcomputer müssen Mitglied folgender Domänenarten sein:

- Domänen, die zur gleichen Gesamtstruktur wie der Remotezugriffsserver gehören.
- Domänen, die zu Gesamtstrukturen mit einer bidirektionalen Vertrauensstellung zur Remotezugriffsserver-Gesamtstruktur gehören.
- Domänen mit bidirektionaler Vertrauensstellung zur Remotezugriffsserverdomäne.

### So fügen Sie den RAS-Server einer Domäne hinzu

1. Klicken Sie im Server-Manager auf **Lokaler Server**. Klicken Sie im Detailbereich auf den Link neben **Computername**.
2. Klicken Sie im Dialogfeld **System Eigenschaften** auf die Registerkarte **Computer Name**. Klicken Sie auf der Registerkarte **Computer Name** auf ändern.
3. Geben Sie unter **Computernamen** den Namen des Computers ein, falls Sie beim Beitritt des Servers zur Domäne auch den Computernamen ändern. Klicken Sie unter **Mitglied von Domäne**, und geben Sie dann den Namen der Domäne ein, für die der Beitritt des Servers durchgeführt werden soll, z. B. `%quot;corp.contoso.com%quot;`, und klicken Sie dann auf **OK**.
4. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, der über die Berechtigung zum Durchführen des Beitritts von Computern zur Domäne verfügt. Klicken Sie anschließend auf **OK**.
5. Klicken Sie auf **OK**, wenn das Begrüßungsdialogfeld für die Domäne angezeigt wird.
6. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
7. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
8. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.

### So fügen Sie Clientcomputer zur Domäne hinzu

1. Führen Sie **Explorer.exe** aus.
2. Klicken Sie mit der rechten Maustaste auf das Computersymbol und klicken Sie dann auf **Eigenschaften**.

3. Klicken Sie auf der Seite **System** auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
5. Geben Sie unter **Computername** den Namen des Computers ein, falls Sie beim Beitritt des Servers zur Domäne auch den Computernamen ändern. Klicken Sie unter **Mitglied von** auf **Domäne**, und geben Sie dann den Namen der Domäne ein, für die der Beitritt des Servers durchgeführt werden soll, z. B. `corp.contoso.com`, und klicken Sie dann auf **OK**.
6. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, der über die Berechtigung zum Durchführen des Beitritts von Computern zur Domäne verfügt. Klicken Sie anschließend auf **OK**.
7. Klicken Sie auf **OK**, wenn das Begrüßungsdialogfeld für die Domäne angezeigt wird.
8. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
9. Klicken Sie im Dialogfeld **Systemeigenschaften** auf „Schließen“. Klicken Sie bei Aufforderung auf **Jetzt neu starten**.

#### *Befehle in Windows PowerShell*

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

Beachten Sie, dass Sie nach der Eingabe des unten angegebenen Befehls `Add-Computer -DomainName <domain_name>` die Domänenanmeldeinformationen bereitstellen müssen.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

## Konfigurieren von GPOs

Zum Bereitstellen des Remote Zugriffs benötigen Sie mindestens zwei Gruppenrichtlinien Objekte: ein Gruppenrichtlinien Objekt enthält Einstellungen für den RAS-Server und eine enthält Einstellungen für DirectAccess-Client Computer. Wenn Sie den Remote Zugriff konfigurieren, erstellt der Assistent automatisch das erforderliche Gruppenrichtlinien Objekt. Wenn Ihre Organisation jedoch eine Benennungs Konvention erzwingt oder Sie nicht über die erforderlichen Berechtigungen zum Erstellen oder Bearbeiten von Gruppenrichtlinien Objekten verfügen, müssen Sie vor dem Konfigurieren des Remote Zugriffs erstellt werden.

Informationen zum Erstellen eines Gruppenrichtlinien Objekts finden Sie unter [Erstellen und Bearbeiten eines Gruppenrichtlinie Objekts](#).

## **IMPORTANT**

Der Administrator kann das DirectAccess-Gruppenrichtlinien Objekt mit den folgenden Schritten manuell mit einer Organisationseinheit verknüpfen:

1. Verknüpfen Sie die erstellten Gruppenrichtlinienobjekte mit den entsprechenden Organisationseinheiten, bevor Sie DirectAccess konfigurieren.
2. Wenn Sie DirectAccess konfigurieren, sollten Sie eine Sicherheitsgruppe für die Clientcomputer angeben.
3. Der Remotezugriffsadministrator verfügt möglicherweise über Berechtigungen zum Verknüpfen der Gruppenrichtlinienobjekte mit der Domäne, oder das ist nicht der Fall. In beiden Fällen werden die Gruppenrichtlinienobjekte automatisch konfiguriert. Wenn die Gruppenrichtlinienobjekte bereits mit einer Organisationseinheit verknüpft sind, werden die Verknüpfungen nicht entfernt. Die Gruppenrichtlinienobjekte werden auch nicht mit der Domäne verknüpft. Für ein Server-Gruppenrichtlinienobjekt muss die Organisationseinheit das Servercomputerobjekt enthalten, andernfalls wird das Gruppenrichtlinienobjekt mit dem Domänenstamm verknüpft.
4. Wenn Sie vor dem Ausführen des DirectAccess-Assistenten keine Verknüpfung zur Organisationseinheit hinzugefügt haben, kann der Administrator die DirectAccess-Gruppenrichtlinienobjekte nach Abschluss der Konfiguration mit den erforderlichen Organisationseinheiten verknüpfen. Die Verknüpfung zur Domäne kann entfernt werden. Die Schritte zum Verknüpfen eines Gruppenrichtlinien Objekts mit einer Organisationseinheit finden Sie [hier](#).

## **NOTE**

Wenn ein Gruppenrichtlinien Objekt manuell erstellt wurde, kann es während der DirectAccess-Konfiguration vorkommen, dass das Gruppenrichtlinien Objekt nicht verfügbar ist. Das Gruppenrichtlinien Objekt wurde möglicherweise nicht auf den nächstgelegenen Domänen Controller des Verwaltungs Computers repliziert. In diesem Fall kann der Administrator warten, bis die Replikation abgeschlossen ist oder er kann die Replikation erzwingen.

## **WARNING**

Die Verwendung einer anderen Methode als dem DirectAccess-Setup-Assistenten zum Konfigurieren von DirectAccess, wie z. b. das direkte Ändern von DirectAccess-Gruppenrichtlinie Objekten oder das manuelle Ändern der Standardrichtlinien Einstellungen auf dem Server oder Client, wird nicht unterstützt.

# Konfigurieren von Sicherheitsgruppen

Die DirectAccess-Einstellungen, die in den Gruppenrichtlinien Objekten des Client Computers enthalten sind, werden nur auf Computer angewendet, die Mitglieder der Sicherheitsgruppe sind, die Sie beim Konfigurieren des Remote Zugriffs angeben.

## **So erstellen Sie eine Sicherheitsgruppe für DirectAccess-Clients**

1. Führen Sie DSA. `mscaus`. Erweitern Sie in der Konsole Active Directory-Benutzer und -Computers im linken Bereich die Domäne, die die Sicherheitsgruppe enthält, klicken Sie mit der rechten Maustaste auf **Benutzer**, zeigen Sie auf **Neu** und klicken Sie dann auf **Gruppe**.
2. Geben Sie im Dialogfeld **Neues Objekt - Gruppe** unter **Gruppenname** den Namen für die Sicherheitsgruppe ein.
3. Klicken Sie unter **Gruppenbereich** auf **Global**, unter **Gruppentyp** auf **Sicherheit** und anschließend auf **OK**.
4. Doppelklicken Sie auf die Sicherheitsgruppe der DirectAccess-Clientcomputer und dann im Dialogfeld **Eigenschaften** auf die Registerkarte **Mitglieder**.
5. Auf der Registerkarte **Mitglieder** klicken Sie auf **Hinzufügen**.

6. Wählen Sie im Dialogfeld zum **Auswählen von Benutzern, Kontakten Computern oder Dienstkonten** die Clientcomputer aus, für die DirectAccess aktiviert werden soll, und klicken Sie anschließend auf **OK**.

### Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

## Nächster Schritt

- [Schritt 2: Konfigurieren des DirectAccess-Basis Servers](#)

# Schritt 2 Konfigurieren des grundlegenden DirectAccess-Servers

09.04.2020 • 7 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird die Konfiguration der Client- und Servereinstellungen erläutert, die für einen einfachen DirectAccess erforderlich sind. Vergewissern Sie sich vor Beginn der Bereitstellungs Schritte, dass Sie die in [Planen einer einfachen DirectAccess-Bereitstellung](#) beschriebenen Planungsschritte abgeschlossen haben.

AUFGABE	BESCHREIBUNG
Installieren der Remotezugriffsrolle	Installieren Sie die Remotezugriffsrolle.
Konfigurieren von DirectAccess mithilfe des Assistenten für erste Schritte	Der neue Assistent für erste Schritte sorgt für eine beträchtliche Vereinfachung der Konfiguration. Der Assistent hilft dabei, die Komplexität von DirectAccess zu überwinden, und ermöglicht so ein automatisches Setup in wenigen einfachen Schritten. Für den Administrator bietet der Assistent ein nahtloses Erlebnis, da der Kerberos-Proxy automatisch so konfiguriert wird, dass keine interne PKI-Bereitstellung erforderlich ist.
Aktualisieren von Clients mit der DirectAccess-Konfiguration	Zum Erhalt der DirectAccess-Einstellungen müssen Clients die Gruppenrichtlinien aktualisieren, während sie mit dem Intranet verbunden sind.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## Installieren der Remote Zugriffs Rolle

Um den Remotezugriff bereitzustellen, müssen Sie die Remotezugriffsrolle auf einem Server in Ihrer Organisation installieren, der als Remotezugriffsserver fungiert.

### So installieren Sie die Remotezugriffsrolle

1. Klicken Sie auf dem Remote Zugriffs Server in der Server-Manager-Konsole im Dashboard auf **Rollen und Features hinzufügen**.
2. Klicken Sie dreimal auf **Weiter**, um zur Anzeige für die Serverrollenauswahl zu gelangen.
3. Wählen Sie im Dialogfeld **Serverrollen auswählen** die Option **Remotezugriff** aus, und klicken Sie dann auf **Weiter**.
4. Klicken Sie im Dialogfeld **Features auswählen** auf **Weiter**.
5. Klicken Sie auf **weiter**, und aktivieren Sie dann im Dialogfeld **Rollen Dienste auswählen** das Kontrollkästchen **DirectAccess und VPN (RAS)**.
6. Klicken Sie auf **Features hinzufügen**, klicken Sie auf **weiter** und dann auf **Installieren**.

7. Überprüfen Sie im Dialogfeld **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.

#### *Befehle in Windows PowerShell*

Mit dem folgenden Windows PowerShell-Cmdlet oder den folgenden Cmdlets wird die Remote Zugriffs Rolle installiert:

1. Öffnen Sie PowerShell als Administrator.
2. Remote Zugriffs Feature installieren:

```
Install-WindowsFeature RemoteAccess
```

3. Starten Sie den Computer neu:

```
Restart-Computer
```

4. Installieren Sie PowerShell für den Remote Zugriff:

```
Install-WindowsFeature RSAT-RemoteAccess-PowerShell
```

## Konfigurieren von DirectAccess mithilfe des Assistenten für erste Schritte

### **So konfigurieren Sie DirectAccess mithilfe des Assistenten für erste Schritte**

1. Klicken Sie im Server-Manager auf **Tools**, und klicken Sie anschließend auf **Remotezugriffsverwaltung**.
2. Wählen Sie in der Remote Zugriffs-Verwaltungskonsole im linken Navigationsbereich den zu konfigurierenden Rollen Dienst aus, und klicken Sie dann auf **Assistent für die ersten Schritte** ausführen.
3. Klicken Sie auf **Nur DirectAccess bereitstellen**.
4. Wählen Sie die Topologie Ihrer Netzwerkkonfiguration aus, und geben Sie den öffentlichen Namen ein, mit dem Remotezugriffsclients eine Verbindung herstellen. Klicken Sie auf **Weiter**.

#### **NOTE**

Standardmäßig stellt der Assistent für erste Schritte DirectAccess an alle Laptops und Notebookcomputer in der Domäne bereit, indem er einen WMI-Filter auf das Gruppenrichtlinienobjekt für die Clienteinstellungen anwendet.

5. Klicken Sie auf **Fertig stellen**.
6. Da in dieser Bereitstellung keine PKI verwendet wird, stellt der Assistent im Fall, dass keine Zertifikate gefunden werden, automatisch selbstsignierte Zertifikate für IP-HTTPS und den Netzwerkadressenserver bereit und aktiviert den Kerberos-Proxy. Außerdem aktiviert der Assistent NAT64 und DNS64 für die Protokollübersetzung in der auf IPv4 beschränkten Umgebung. Nachdem der Assistent die Konfiguration erfolgreich angewendet hat, klicken Sie auf **Schließen**.
7. Wählen Sie in der Konsolenstruktur der Remotezugriffs-Verwaltungskonsole auf **Vorgangsstatus**. Warten Sie, bis der Status aller Monitore "Wird ausgeführt" lautet. Klicken Sie im Bereich `Aufgaben` unter `Überwachung` regelmäßig auf **Aktualisieren**, um die Anzeige zu aktualisieren.

# Aktualisieren von Clients mit der DirectAccess-Konfiguration

## So aktualisieren Sie DirectAccess-Clients

1. Öffnen Sie PowerShell als Administrator.
2. Geben Sie im PowerShell-Fenster **gpupdate** ein, und drücken Sie dann die EINGABETASTE.
3. Warten Sie, bis die Computerrichtlinien erfolgreich aktualisiert wurden.
4. Geben Sie **Get-DnsClientNrptPolicy** ein, und drücken Sie die EINGABETASTE.

Die Einträge in der Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) für Direct Access werden angezeigt. Beachten Sie, dass die NLS-Serverausnahme angezeigt wird. Der Assistent für erste Schritte hat diesen DNS-Eintrag für den DirectAccess-Server automatisch erstellt und ein zugehöriges selbstsigniertes Zertifikat bereitgestellt, sodass der DirectAccess-Server als Netzwerkadressenserver fungieren kann.

5. Geben Sie **Get-NCSIPolicyConfiguration** ein, und drücken Sie dann die EINGABETASTE. Die vom Assistenten bereitgestellten Einstellungen für die Statusanzeige der Netzwerkkonnektivität werden angezeigt. Achten Sie auf den Wert von `&quot;DomainLocationDeterminationURL&quot;`. Sobald auf diese Netzwerkadressenserver-URL zugegriffen werden kann, ermittelt der Client, dass sie sich innerhalb des Unternehmensnetzwerks befindet, und die NRPT-Einstellungen werden nicht angewendet.
6. Geben Sie **Get-DAConnectionStatus**, und drücken Sie dann die EINGABETASTE. Da der Client die Netzwerkadressenserver-URL erreichen kann, wird der Status **Lokal verbunden** angezeigt.

## Vorheriger Schritt

- [Schritt 1: Konfigurieren der DirectAccess-Infrastruktur](#)

## Nächster Schritt

- [Schritt 3 Überprüfen der grundlegenden DirectAccess-bereit Stellungen](#)

# Schritt 3 Überprüfen von bereit Stellungen

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie überprüfen, ob die grundlegende DirectAccess-Bereitstellung ordnungsgemäß konfiguriert ist.

## So überprüfen Sie den Zugriff auf interne Ressourcen über DirectAccess

1. Stellen Sie eine Verbindung von einem DirectAccess-Clientcomputer mit dem Unternehmensnetzwerk her, und rufen Sie die Gruppenrichtlinie ab.
2. Klicken Sie im Infobereich auf das Symbol **Netzwerkverbindungen**, um auf die DirectAccess-Medienverwaltung zuzugreifen.
3. Klicken Sie auf die **DirectAccess-Verbindung**. Als Status wird **Lokal verbunden** angezeigt.
4. Verbinden Sie den Clientcomputer mit dem externen Netzwerk, und versuchen Sie, auf interne Ressourcen zuzugreifen.

Sie sollten auf alle Unternehmensressourcen zugreifen können.

## Vorheriger Schritt

- [Schritt 2: Konfigurieren des DirectAccess-Servers](#)

# Bereitstellen eines einzelnen DirectAccess-Servers mit erweiterten Einstellungen

09.04.2020 • 14 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Dieses Thema bietet eine Einführung in das DirectAccess-Szenario, in dem ein einzelner DirectAccess-Server verwendet wird, und ermöglicht es Ihnen, DirectAccess mit erweiterten Einstellungen bereitzustellen.

Bevor Sie mit der Bereitstellung beginnen, sollten Sie sich die folgende Liste mit nicht unterstützten Konfigurationen, bekannten Problemen und Voraussetzungen ansehen:

In den folgenden Themen finden Sie Informationen zu Voraussetzungen und anderen Informationen vor der Bereitstellung von DirectAccess.

- [DirectAccess: Nicht unterstützte Konfigurationen](#)
- [Erforderliche Komponenten für die Bereitstellung von DirectAccess](#)

## Szenariobeschreibung

In diesem Szenario wird ein einzelner Computer, auf dem entweder Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, als DirectAccess-Server mit erweiterten Einstellungen konfiguriert.

### NOTE

Wenn Sie nur eine grundlegende Bereitstellung mit einfachen Standardeinstellungen konfigurieren möchten, finden Sie unter [Deploy a Single DirectAccess Server Using the Getting Started Wizard](#) weitere Informationen. In dem einfachen Szenario wird DirectAccess über einen Assistenten mit Standardeinstellungen eingerichtet, ohne dass die Notwendigkeit zur Konfiguration von Infrastruktureinstellungen wie einer Zertifizierungsstelle oder Active Directory-Sicherheitsgruppen besteht.

## Inhalt dieses Szenarios

Um einen einzelnen DirectAccess-Server mit erweiterten Einstellungen einzurichten, müssen Sie einige Planungs- und Bereitstellungsschritte durchführen.

### Erforderliche Komponenten

Vor dem Beginn können Sie folgende Anforderungen überprüfen:

- Windows-Firewall muss in allen Profilen aktiviert sein.
- Der DirectAccess-Server ist der Netzwerkadressenserver.
- Sie möchten, dass alle Drahtloscomputer in der Domäne, in der der DirectAccess-Server installiert wird, DirectAccess-fähig sind. Wenn Sie DirectAccess bereitstellen, ist es automatisch auf allen mobilen Computern in der aktuellen Domäne aktiviert.

## **IMPORTANT**

Einige Technologien und Konfigurationen werden bei der Bereitstellung von DirectAccess nicht unterstützt.

- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) wird im Unternehmensnetzwerk nicht unterstützt.  
Wenn Sie ISATAP verwenden, müssen Sie es entfernen und das systemeigene IPv6 verwenden.

## **Planungsschritte**

Die Planung besteht aus zwei Phasen:

1. **Planen der DirectAccess-Infrastruktur.** Diese Phase beschreibt die erforderlichen Planungsschritte zum Einrichten der Netzwerkinfrastruktur vor der DirectAccess-Bereitstellung. Sie umfasst das Planen der Netzwerk- und Servertopologie, der Zertifikate, des Domain Name System (DNS), der Active Directory-Konfiguration, der Konfiguration der Gruppenrichtlinienobjekte und des DirectAccess-Netzwerkadressenservers.
2. **Planen der DirectAccess-Bereitstellung.** Diese Phase beschreibt die erforderlichen Planungsschritte zur Vorbereitung der DirectAccess-Bereitstellung. Dazu gehört die Planung für DirectAccess-Clientcomputer, Server- und Clientauthentifizierungsanforderungen, VPN-Einstellungen, Infrastrukturserver sowie Verwaltungs- und Anwendungsserver.

## **Bereitstellungsschritte**

Die Bereitstellung besteht aus drei Phasen:

1. **Konfigurieren der DirectAccess-Infrastruktur.** Diese Phase beinhaltet das Konfigurieren von Netzwerk und Routing, das Konfigurieren der Firewallemstellungen (falls erforderlich), das Konfigurieren von Zertifikaten, DNS-Servern, Active Directory- und Gruppenrichtlinienobjekt-Einstellungen und DirectAccess-Netzwerkadressenserver.
2. **Konfigurieren der DirectAccess-Servereinstellungen.** Die Phase beinhaltet Schritte zum Konfigurieren von DirectAccess-Clientcomputern, DirectAccess-Server, Infrastrukturservern sowie Verwaltungs- und Anwendungsservern.
3. **Überprüfen der Bereitstellung.** Diese Phase beinhaltet Schritte zur Überprüfung der DirectAccess-Bereitstellung.

Ausführliche Informationen zu den Bereitstellungsschritten finden Sie unter [Installieren und Konfigurieren des erweiterten DirectAccess](#).

## **Praktische Anwendungen**

Die Bereitstellung eines einzelnen DirectAccess-Servers bietet Folgendes:

- **Erleichterte Bedienung.** Verwaltete Client Computer, auf denen Windows 10, Windows 8.1, Windows 8 und Windows 7 ausgeführt wird, können als DirectAccess-Client Computer konfiguriert werden. Diese Clients können immer, wenn sie im Internet sind, über DirectAccess auf interne Netzwerkressourcen zugreifen, ohne sich über eine VPN-Verbindung einzuloggen. Clientcomputer, die keines dieser Betriebssysteme verwenden, können per VPN eine Verbindung zum internen Netzwerk herstellen.
- **Erleichterte Verwaltung.** Die Remoteverwaltung von DirectAccess-Clientcomputern im Internet ist mithilfe von RAS-Administratoren über DirectAccess möglich, selbst wenn die Clientcomputer sich nicht im internen Unternehmensnetzwerk befinden. Clientcomputer, die nicht den Unternehmensanforderungen entsprechen, können automatisch über Verwaltungsserver gewartet werden. Sowohl DirectAccess als auch VPN werden über dieselbe Konsole und mit denselben

Assistenten verwaltet. Außerdem können einer oder mehrere DirectAccess-Server über eine einzelne Remotezugriffs-Verwaltungskonsole verwaltet werden.

## Für dieses Szenario erforderliche Rollen und Features

Die folgende Tabelle enthält die für dieses Szenario erforderlichen Rollen und Features:

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Remotezugriffs-Rolle	<p>Die Rolle wird über die Server-Manager-Konsole oder Windows PowerShell installiert bzw. deinstalliert. Diese Rolle umfasst DirectAccess sowie die Routing- und RAS-Dienste. Die Remotezugriffs-Rolle besteht aus zwei Komponenten:</p> <ol style="list-style-type: none"> <li>1. DirectAccess und RRAS-VPN. DirectAccess und VPN werden in der Remote Zugriffs-Verwaltungskonsole verwaltet.</li> <li>2. RRAS-Routing. RRAS-Routing Features werden in der Legacy-Routing-und Remote Zugriffs Konsole verwaltet.</li> </ol> <p>Die RAS-Serverrolle ist von den folgenden Serverrollen/-features abhängig:</p> <ul style="list-style-type: none"> <li>-Internetinformationsdienste (IIS)-Webserver: dieses Feature ist erforderlich, um den Netzwerkadressen Server auf dem DirectAccess-Server und den Standard Webtest zu konfigurieren.</li> <li>-Interne Windows-Datenbank. Wird für die lokale Kontoführung auf dem DirectAccess-Server verwendet.</li> </ul>
Feature "Tools für die Remotezugriffsverwaltung"	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"> <li>-Sie wird bei der Installation der Remote Zugriffs Rolle standardmäßig auf einem DirectAccess-Server installiert und unterstützt die Benutzeroberfläche der Remote Verwaltungskonsole und Windows PowerShell-Cmdlets.</li> <li>-Es kann optional auf einem Server installiert werden, auf dem die DirectAccess-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.</li> </ul> <p>Das Feature "Tools für die Remotezugriffsverwaltung" besteht aus den folgenden Komponenten:</p> <ul style="list-style-type: none"> <li>-Remote Zugriff grafische Benutzeroberfläche (GUI)</li> <li>-Remote Zugriffs Modul für Windows PowerShell</li> </ul> <p>Abhängigkeiten umfassen:</p> <ul style="list-style-type: none"> <li>-Gruppenrichtlinien-Verwaltungskonsole</li> <li>-RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li> <li>-Windows PowerShell 3,0</li> <li>-Tools und Infrastruktur für die grafische Verwaltung</li> </ul>

## Hardwareanforderungen

Für dieses Szenario müssen die folgenden Hardwareanforderungen erfüllt werden:

- Serveranforderungen:

- Ein Computer, der die Hardwareanforderungen für Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 erfüllt.
- Auf dem Server muss mindestens ein Netzwerkadapter installiert, aktiviert und mit dem internen Netzwerk verbunden sein. Werden zwei Adapter verwendet, sollte ein Adapter mit dem internen Unternehmensnetzwerk und der andere mit dem externen Netzwerk (Internet oder privates Netzwerk) verbunden sein.
- Falls Teredo als IPv4- bis IPv6-Übergangsprotokoll benötigt wird, benötigt der externe Adapter des Servers zwei aufeinanderfolgenden öffentlichen IPv4-Adressen. Wenn nur eine IP-Adresse verfügbar ist, kann nur IP-HTTPS als Übergangsprotokoll verwendet werden.
- Mindestens ein Domänencontroller. DirectAccess-Server und DirectAccess-Clients müssen Domänenmitglieder sein.
- Eine Zertifizierungsstelle ist erforderlich, wenn Sie keine selbstsignierten Zertifikate für IP-HTTPS oder den Netzwerkadressenserver verwenden möchten, oder wenn Sie Clientzertifikate zur Client-IPsec-Authentifizierung verwenden möchten. Alternativ können Sie die Zertifikate von einer öffentlichen Zertifizierungsstelle anfordern.
- Befindet sich der Netzwerkadressenserver nicht auf dem DirectAccess-Server, ist ein separater Webserver für die Ausführung erforderlich.

- Clientanforderungen:

- Auf einem Client Computer muss Windows 10, Windows 8 oder Windows 7 ausgeführt werden.

**NOTE**

Die folgenden Betriebssysteme können als DirectAccess-Clients verwendet werden: Windows 10, Windows Server 2012 R2, Windows Server 2012, Windows 8 Enterprise, Windows 7 Enterprise oder Windows 7 Ultimate.

- Anforderungen an Infrastruktur und Verwaltungsserver:

- Während der Remoteverwaltung von DirectAccess-Clientcomputern initiieren die Clients die Kommunikation mit Verwaltungsservern, z. B. Domänencontrollern, System Center-Konfigurationsservern und Inhaltsregistrierungsstellen (HRA)-Servern, für Dienste, darunter Windows- und Antivirus-Updates sowie Network Access Protection (NAP)-Clientkompatibilität. Die erforderlichen Server sollten bereitgestellt werden, bevor mit der Bereitstellung des Remotezugriffs begonnen wird.
- Falls der Remotezugriff Client-NAP-Kompatibilität erfordert, sollten die NPS- und HRS-Server bereitgestellt werden, bevor mit der Bereitstellung des Remotezugriffs begonnen wird.
- Falls ein VPN aktiviert ist, ist ein DHCP-Server erforderlich, um die IP-Adressen automatisch den VPN-Clients zuzuweisen, sofern kein statischen IP-Adresspool genutzt wird.

## Software Anforderungen

Für dieses Szenario gelten eine Reihe von Anforderungen:

- Serveranforderungen:

- Der DirectAccess-Server muss Domänenmitglied sein. Der Server kann an der Schwelle zum

internen Netzwerks oder geschützt durch eine Edgefirewall oder ein anderes Gerät bereitgestellt werden.

- Wird der DirectAccess-Server durch eine Edgefirewall oder ein NAT-Gerät geschützt, muss das Gerät so konfiguriert sein, dass ein- und ausgehender Datenverkehr für den DirectAccess-Server zugelassen wird.
  - Die Person, die den Remotezugriff auf dem Server einrichtet, muss lokale Administratorberechtigungen für den Server und Benutzerberechtigungen für die Domäne besitzen. Zusätzlich benötigt der Administrator Berechtigungen für die Gruppenrichtlinien, die bei der DirectAccess-Bereitstellung verwendet werden. Um die Features nutzen zu können, die die DirectAccess-Bereitstellung auf mobile Computer beschränken, ist die Berechtigung zum Erstellen von WMI-Filtern für den Domänencontroller erforderlich.
- RAS-Client-Anforderungen:
    - DirectAccess-Clients müssen Domänenmitglieder sein. Domänen, die Clients beinhalten, können zur selben Gesamtstruktur gehören wie der DirectAccess-Server, oder sie können eine bidirektionale Vertrauensstellung mit der DirectAccess-Serverstruktur oder der Domäne innehaben.
    - Eine Active Directory-Sicherheitsgruppe wird benötigt, um die Computer aufzunehmen, die als DirectAccess-Clients konfiguriert werden. Wird beim Konfigurieren der DirectAccess-Clienteinstellungen keine Sicherheitsgruppe angegeben, wird das Client-Gruppenrichtlinienobjekt standardmäßig auf alle Laptopcomputer in der Sicherheitsgruppe "%quot;Domänencomputer%quot;" angewendet.

**NOTE**

Es wird empfohlen, dass Sie eine Sicherheitsgruppe für jede Domäne erstellen, die DirectAccess-Clientcomputer enthält.

**IMPORTANT**

Wenn Sie Teredo in der DirectAccess-Bereitstellung aktiviert haben und Zugriff auf Windows 7-Clients bereitstellen möchten, müssen Sie sicherstellen, dass die Clients auf Windows 7 mit SP1 aktualisiert werden. Clients, die Windows 7 RTM verwenden, können keine Verbindung über Teredo herstellen. Diese Clients können jedoch weiterhin eine Verbindung zum Unternehmensnetzwerk über IP-HTTPS herstellen.

## Siehe auch

Die folgende Tabelle enthält Links zu zusätzlichen Ressourcen.

ART DES INHALTS	VERWEISE
Bereitstellung	<a href="#">DirectAccess-Bereitstellungs Pfade in Windows Server</a> <a href="#">Bereitstellen eines einzelnen DirectAccess-Servers mit dem Assistenten für die ersten Schritte</a>
Tools und Einstellungen	<a href="#">PowerShell-Cmdlets für den Remote Zugriff</a>

ART DES INHALTS	VERWEISE
<b>Communityressourcen</b>	<a href="#">Leitfaden zum DirectAccess-Lebensfaden</a> <a href="#">DirectAccess-wiki-Einträge</a>
<b>Verwandte Technologien</b>	<a href="#">Funktionsweise von IPv6</a>

# Planen einer erweiterten DirectAccess-Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema werden die Planungsschritte aufgelistet, die für die Bereitstellung eines einzelnen DirectAccess-Servers mit Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 mit allen grundlegenden und erweiterten Features erforderlich sind. Die Planungsphase umfasst folgende Themen.

- [Schritt 1: Planen der erweiterten DirectAccess-Infrastruktur](#)

In dieser Phase planen Sie Ihre Netzwerk- und Servertopologie, die Firewall-Einstellungen, die Zertifikatanforderungen, das DNS (Domain Name System), das Active Directory, die DirectAccess-Verwaltungsserver und den DirectAccess-Netzwerkadressenserver.

- [Schritt 2: Planen von erweiterten DirectAccess-bereit Stellungen](#)

In dieser Phase planen Sie die Client- und Serverbereitstellung, einschließlich der DirectAccess-Infrastruktur und der Anwendungsserver.

## Nächster Schritt

Wenn Sie diese Planungsschritte abgeschlossen haben, können Sie mit der Bereitstellung des Servers beginnen. Anweisungen hierzu finden Sie unter [Installieren und Konfigurieren von Advanced DirectAccess](#).

# Schritt 1 Planen der erweiterten DirectAccess-Infrastruktur

09.04.2020 • 83 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt bei der Planung einer erweiterten DirectAccess-Bereitstellung auf einem einzelnen Server ist die Planung der Infrastruktur, welche für diese Bereitstellung erforderlich ist. In diesem Thema werden die Schritte zur Planung der Infrastruktur beschrieben. Diese Planungsaufgaben müssen nicht in einer bestimmten Reihenfolge durchgeführt werden.

AUFGABE	BESCHREIBUNG
<a href="#">1.1 Planen der Netzwerktopologie und-Einstellungen</a>	Entscheiden Sie über den Standort des DirectAccess-Servers (Edge oder hinter einem NAT-Gerät oder einer Firewall), und planen Sie IP-Adressenvergabe, Routing und Tunnelerzwingung.
<a href="#">1.2 Planen der Firewallanforderungen</a>	Planen Sie, wie DirectAccess-Verkehr über Edge-Firewalls zugelassen wird.
<a href="#">1.3 Planen der Zertifikat Anforderungen</a>	Entscheiden Sie, ob Sie Kerberos oder Zertifikate für die Clientauthentifizierung verwenden möchten, und planen Sie Websitezertifikate. IP-HTTPS ist ein Übergangsprotokoll, das von DirectAccess-Clients zum Tunneln von IPv6-Datenverkehr über IPv4-Netzwerke verwendet wird. Entscheiden Sie, ob die Authentifizierung zum IP-HTTPS-Server über ein Zertifikat erfolgen soll, das durch eine Zertifizierungsstelle (CA) ausgegeben wird, oder durch ein selbstsigniertes Zertifikat, das automatisch durch den DirectAccess-Server ausgestellt wird.
<a href="#">1.4 Planen der DNS-Anforderungen</a>	Planen Sie DNS-Einstellungen (Domain Name System) für die DirectAccess-Server, die Infrastrukturserver, die Optionen für die lokale Namensauflösung und die Clientkonnektivität.
<a href="#">1.5 Planen des Netzwerkadressen Servers</a>	Der Netzwerkadressenserver wird von DirectAccess-Clients verwendet, um festzustellen, ob sie sich im internen Netzwerk befinden. Entscheiden Sie, ob die Netzwerkadressenserver-Website in Ihrer Organisation platziert werden soll (auf dem DirectAccess-Server oder einem anderen Server), und planen Sie die Zertifikatanforderungen, wenn sich der Netzwerkadressenserver auf dem DirectAccess-Server befindet.
<a href="#">1.6 Planen der Verwaltungs Server</a>	Sie können DirectAccess-Clientcomputer, die sich außerhalb des Unternehmensnetzwerk befinden, remote im Internet verwalten. Berücksichtigen Sie bei der Planung Verwaltungsserver (beispielsweise Updateserver), die für die Verwaltung von Remotedclients verwendet werden.

AUFGABE	BESCHREIBUNG
1,7 Plan Active Directory Domain Services	Planen Sie Ihre Domänencontroller, Ihre Active Directory-Anforderungen, Clientauthentifizierung und mehrere Domänen.
1,8 planen Gruppenrichtlinie Objekte	Entscheiden Sie, welche Gruppenrichtlinienobjekte in Ihrer Organisation erforderlich sind und wie diese erstellt oder bearbeitet werden.

## 1.1 Planen der Netzwerktopologie und -einstellungen

In diesem Abschnitt wird erklärt, wie Sie Ihr Netzwerk planen, einschließlich:

- [1.1.1 Planen von Netzwerkadapters und IP-Adressierung](#)
- [1.1.2 Planen der IPv6-Intranet-Konnektivität](#)
- [1.1.3 Planen der Tunnel Erzwingung](#)

### 1.1.1 Planen von Netzwerkadapters und IP-Adressierung

1. Identifizieren Sie die Netzwerkadaptertopologie, die Sie verwenden möchten. DirectAccess kann mit einer der folgenden Topologien eingerichtet werden:

- **Zwei Netzwerkadapter.** Der DirectAccess-Server kann am Rand installiert werden, wenn ein Netzwerkadapter mit dem Internet und der andere mit dem internen Netzwerk verbundenen ist. Alternativ kann er auch hinter einem NAT-Gerät, einer Firewall oder einem Routergerät installiert werden, wobei ein Netzwerkadapter mit einem Perimeternetzwerk und der andere mit dem internen Netzwerk verbunden ist.
- **Ein Netzwerkadapter.** Der DirectAccess-Server wird hinter einem NAT-Gerät installiert, und der einzige Netzwerkadapter wird mit dem internen Netzwerk verbunden.

2. Identifizieren Sie Ihre IP-Adressierungsanforderungen:

DirectAccess verwendet IPv6 mit IPsec, um eine sichere Verbindung zwischen DirectAccess-Clientcomputern und dem internen Unternehmensnetzwerk herzustellen. Jedoch erfordert DirectAccess nicht unbedingt Konnektivität mit dem IPv6-Internet oder nativen IPv6-Support auf internen Netzwerken. Stattdessen konfiguriert und verwendet es automatisch IPv6-Übergangstechnologien, um IPv6-Datenverkehr durch das IPv4-Internet (durch die Verwendung von 6to4, Teredo oder IP-HTTPS) und durch Ihr nur-IPv4-Intranet (durch die Verwendung von NAT64 oder ISATAP) zu tunneln. Eine Übersicht über diese Übergangstechnologien finden Sie in folgenden Ressourcen:

- [IPv6-Übergangs Technologien](#)
- [IP-HTTPS-tunnelingprotokollspezifikation](#)

3. Konfigurieren Sie erforderliche Adapter und Adressen entsprechend folgender Tabelle. Für Bereitstellungen, die einen einzigen Netzwerkadapter verwenden und hinter einem NAT-Gerät eingerichtet sind, konfigurieren Sie die IP-Adressen, indem Sie nur die Spalte **INTERNER NETZWERKADAPTER** verwenden.

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGE N

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv4-Internet und IPv4-Intranet	<p>Konfigurieren Sie zwei statische, aufeinander folgende öffentliche IPv4-Adressen mit den entsprechenden Subnetzmasken (nur für Teredo erforderlich).</p> <p>Konfigurieren Sie zudem die IPv4-Adresse des Standardgateways der Internetfirewall oder des lokalen Routers Ihres Internetdienstanbieters (Internet Service Provider, ISP). <b>Hinweis:</b> Der DirectAccess-Server benötigt zwei aufeinander folgende öffentliche IPv4-Adressen, damit er als Teredo-Server fungieren kann und Windows-basierte Clients den DirectAccess-Server verwenden können, um den Typ des NAT-Geräts zu erkennen, hinter dem Sie sich befinden.</p>	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>: Eine IPv4-Intranetadresse mit der entsprechenden Subnetzmaske.</li> <li>: Das Verbindungs spezifische DNS-Suffix des Intranetnamespaces. Zudem sollte ein DNS-Server auf der internen Schnittstelle konfiguriert werden. <b>Vorsicht:</b> Konfigurieren Sie kein Standard Gateway auf Intranetschnittstellen.</li> </ul>	<p>Gehen Sie wie folgt vor, um den DirectAccess-Server so zu konfigurieren, dass er alle Subnetze auf dem internen IPv4-Netzwerk erreicht:</p> <ul style="list-style-type: none"> <li>-Listen Sie die IPv4-Adressräume für alle Speicherorte im Intranet auf.</li> <li>-Verwenden Sie den Befehl <b>Route Add-p</b> oder <b>Netsh Interface IPv4 Add Route</b>, um die IPv4-Adressbereiche als statische Routen in der IPv4-Routing Tabelle des DirectAccess-Servers hinzuzufügen.</li> </ul>

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv6-Internet und IPv6-Intranet	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>-Verwenden Sie die Adress Konfiguration, die von Ihrem ISP bereitgestellt wird.</li> <li>-Verwenden Sie den Befehl <b>Route Print</b>, um sicherzustellen, dass eine IPv6-Standard Route vorhanden ist, und verweist auf den ISP-Router in der IPv6-Routing Tabelle.</li> <li>: Bestimmen Sie, ob der ISP- und der Intranetrouter die in RFC 4191 beschriebenen standardmäßigen Routereinstellungen verwenden, und verwenden Sie eine höhere Standardeinstellung als ihre lokalen Intranetrouter. Wenn beide Fälle zutreffen, ist keine weitere Konfiguration für die Standardroute erforderlich. Die höhere Präferenz für den ISP-Router stellt sicher, dass die aktive IPv6-Standardroute des DirectAccess-Servers auf das IPv6-Internet zeigt.</li> </ul> <p>Wenn Sie über eine systemeigene IPv6-Infrastruktur verfügen, kann die Internetschnittstelle außerdem auch die Domänencontroller im Intranet erreichen, da der DirectAccess-Server ein IPv6-Router ist. Fügen Sie in diesem Fall Paketfilter zum Domänencontroller im Perimeternetzwerk hinzu, die Konnektivität zur IPv6-Adresse der Internetschnittstelle des DirectAccess-Servers verhindern.</p>	<p>Konfigurieren Sie Folgendes:</p> <p>Wenn Sie nicht die Standardeinstellungen verwenden, können Sie Ihre Intranetschnittstellen mit dem folgenden Befehl konfigurieren:<b>Netsh Interface IPv6 Set interfaceindex ignoredefaultroutes = aktiviert</b>.</p> <p>Dieser Befehl stellt sicher, dass der IPv6-Routingtabelle keine weiteren Standardrouten hinzugefügt werden, die auf Intranetrouter zeigen. Sie können den Schnittstellenindex der Intranetschnittstellen mit folgendem Befehl abrufen: <b>netsh interface ipv6 show interface</b>.</p>	<p>Wenn Sie ein IPv6-Intranet haben, führen Sie folgende Schritte aus, um den DirectAccess-Server so zu konfigurieren, dass er alle IPv6-Speicherorte erreicht:</p> <ul style="list-style-type: none"> <li>-Auflisten der IPv6-Adressräume für alle Speicherorte im Intranet.</li> <li>-Verwenden Sie den Befehl <b>Netsh Interface IPv6 Add Route</b>, um die IPv6-Adressbereiche als statische Routen in der IPv6-Routing Tabelle des DirectAccess-Servers hinzuzufügen.</li> </ul>

	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv4-Internet und IPv6-Intranet	<p>Der DirectAccess-Server leitet den Datenverkehr für die Standard-IPv6-Route mit dem Microsoft-IP6-zu-IP4-Adapter an ein IP6-zu-IP4-Relay im IPv4-Internet weiter. Sie können einen DirectAccess-Server für die IPv4-Adresse des Microsoft-IP6-zu-IP4-Adapters mit folgendem Befehl konfigurieren:</p> <pre>netsh interface ipv6  6to4 set relay name=  &lt;ipaddress&gt;  state=enabled</pre> <p>.</p>		

#### NOTE

- Wenn dem DirectAccess-Client eine öffentliche IPv4-Adresse zugewiesen wurde, verwendet diese die IP6-zu-IP4-Übergangstechnologie für die Verbindung mit dem Internet. Wenn diesem eine private IPv4-Adresse zugewiesen wurde, wird Teredo verwendet. Wenn der DirectAccess-Client weder mit IP6-zu-IP4 noch mit Teredo eine Verbindung mit dem DirectAccess-Server herstellen kann, wird IP-HTTPS verwendet.
- Um Teredo zu verwenden, müssen Sie zwei aufeinander folgende IP-Adressen auf dem nach außen verfügbaren Netzwerkadapter konfigurieren.
- Sie können Teredo nicht verwenden, wenn der DirectAccess-Server nur einen Netzwerkadapter hat.
- Systemeigene IPv6-Clientcomputer können über eine systemeigene IPv6 eine Verbindung zum DirectAccess-Server herstellen, und es ist keine Übergangstechnologie erforderlich.

### 1.1.2 Planen von IPv6-Intranetkonnektivität

Für die Verwaltung von Remote-DirectAccess-Clients ist IPv6 erforderlich. IPv6 ermöglicht DirectAccess-Verwaltungsservern, für die Remote-Verwaltung eine Verbindung zu DirectAccess-Clients, die sich im Internet befinden, herzustellen.

#### NOTE

- Es ist nicht erforderlich, IPv6 auf Ihrem Netzwerk zu verwenden, um Verbindungen zu unterstützen, die durch DirectAccess-Clientcomputer zu IPv4-Ressourcen auf Ihrem Organisationsnetzwerk initiiert werden. Für diese Zwecke wird NAT64/DNS64 verwendet.
- Falls Sie keine Remote-DirectAccess-Clients verwalten, müssen Sie IPv6 nicht bereitstellen.
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) wird in DirectAccess-Bereitstellungen nicht unterstützt.
- Wenn Sie IPv6 verwenden, können Sie IPv6-Host-(AAAA)-Ressourceneintragsabfragen für DNS64 aktivieren, indem Sie folgenden Windows PowerShell-Befehl verwenden: `Set-NetDnsTransitionConfiguration -OnlySendAQuery $false`.

### 1.1.3 Planen der Tunnelerzwingung

Mit IPv6 und der Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) trennen DirectAccess-Clients ihren Intranet- und Internetdatenverkehr wie folgt:

- DNS-Namensabfragen nach vollqualifizierten Domänennamen (FQDNs) im Intranet und der gesamte Intranetdatenverkehr werden über die Tunnel zum DirectAccess-Server oder direkt mit den Intranetservfern ausgetauscht. Der Intranetdatenverkehr von DirectAccess-Clients ist IPv6-Datenverkehr.

- DNS-Namensabfragen nach FQDNs, die einer Ausnahmeregel entsprechen oder nicht zum Intranetnamespace gehören, sowie der gesamte Datenverkehr mit Internetservern werden über die physische Schnittstelle ausgetauscht, die mit dem Internet verbunden ist. Der Internetdatenverkehr von DirectAccess-Clients ist typischerweise IPv4-Datenverkehr.

Im Gegensatz hierzu wird bei einigen RAS-VPN-Implementierungen (Remote Access Virtual Private Network), einschließlich des VPN-Clients, der gesamte Datenverkehr (Intranet und Internet) standardmäßig über die RAS-VPN-Verbindung gesendet. Der Internetdatenverkehr für den Zugriff auf IPv4-Internetressourcen wird vom VPN-Server an IPv4-Webproxyserver im Intranet weitergeleitet. Es ist möglich, den Intranet- und Internetdatenverkehr für RAS-VPN-Clients durch getrennte Tunnel zu separieren. Dies beinhaltet die Konfiguration der IP-Routingtabelle auf den VPN-Clients, sodass der Datenverkehr an Intranetspeicherorte über die VPN-Verbindung und der Datenverkehr an alle anderen Speicherorte über die physische Schnittstelle, die mit dem Internet verbundenen ist, gesendet wird.

Durch Erzwingen von Tunneln können Sie DirectAccess-Clients so konfigurieren, dass der gesamte Datenverkehr durch die Tunnel zum DirectAccess-Server gesendet wird. Wenn die Tunnelerzungung konfiguriert ist, erkennen DirectAccess-Clients, dass sie im Internet sind, und entfernen ihre IPv4-Standardroute. Abgesehen vom lokalen Subnetzdatenverkehr sendet der DirectAccess-Client ausschließlich IPv6-Daten, die durch Tunnel zum DirectAccess-Server gesendet werden.

#### **IMPORTANT**

Wenn Sie Tunnelerzungung verwenden oder diese in Zukunft hinzufügen möchten, sollten Sie eine Zwei-Tunnel-Konfiguration bereitstellen. Aufgrund von Sicherheitsüberlegungen wird die Tunnelerzungung in einer Ein-Tunnel-Konfiguration nicht unterstützt.

Das Aktivieren des Erzwingens von Tunneln hat folgende Auswirkungen:

- DirectAccess-Clients bauen IPv6-Verbindungen zum DirectAccess-Server nur mithilfe von IP-HTTPS (Internet Protocol over Secure Hypertext Transfer Protocol) über das IPv4-Internet auf.
- Die einzigen Speicherorte, auf die ein DirectAccess-Client standardmäßig über IPv4 zugreifen kann, sind die in seinem lokalen Subnetz. Bei allen anderen Daten, die von Anwendungen und Diensten auf dem DirectAccess-Client gesendet werden, handelt es sich um über die DirectAccess-Verbindung gesendete IPv6-Daten. Daher können mit Nur-IPv4-Anwendungen auf dem DirectAccess-Client keine Internetressourcen (außer die im lokalen Subnetz) erreicht werden.

#### **IMPORTANT**

Für die Tunnelerzungung über DNS64 und NAT64 muss IPv6-Internetkonnektivität implementiert sein. Eine Möglichkeit dafür ist, das IP-HTTPS-Präfix global routingfähig zu machen, sodass ipv6.msftncsi.com über IPv6 erreichbar ist, und die Antwort vom Internetserver zu den IP-HTTPS-Clients über den DirectAccess-Server zurückgegeben werden kann.

Da dies in den meisten Fällen nicht möglich ist, ist die beste Möglichkeit, virtuelle NCSI-Server innerhalb des Unternehmensnetzwerks zu erstellen, folgende:

1. Fügen Sie einen NRPT-Eintrag für ipv6.msftncsi.com hinzu, und lösen Sie ihn anhand von DNS64 zu einer internen Website auf (dies kann eine IPv4-Website sein).
2. Fügen Sie einen NRPT-Eintrag für dns.msftncsi.com hinzu, und lösen Sie ihn anhand eines Unternehmens-DNS-Servers auf, um den IPv6-Host-(AAAA)-Ressourceneintrag fd3e:4f5a:5b81::1 zurückzugeben. (Die Verwendung von DNS64, um nur Host-(A)-Ressourceneintragsabfragen für diesen FQDN zu senden, funktioniert möglicherweise nicht, da dies in Nur-IPv4-Bereitstellungen konfiguriert ist. Es sollte also so konfiguriert werden, dass direkt anhand von Unternehmens-DNS aufgelöst wird.)

## 1.2 Planen der Firewallanforderungen

Wenn sich der DirectAccess-Server hinter einer Edge-Firewall befindet, sind folgende Ausnahmen für RAS-Datenverkehr erforderlich, wenn sich der DirectAccess-Server auf dem IPv4-Internet befindet:

- Teredo-Datenverkehr-UDP (User Datagram Protocol)-Zielport 3544 eingehend und UDP-Quellport 3544 ausgehend.
- IPv6-zu-IPv4-Datenverkehr-IP-Protokoll 41 eingehend und ausgehend.
- IP-HTTPS-TCP (Transmission Control Protocol)-Zielport 443 und TCP-Quellport 443 ausgehend.
- Wenn Sie den Remotezugriff mit einem einzigen Netzwerkadapter bereitstellen und den Netzwerkadressenserver auf dem DirectAccess-Server installieren, sollte TCP-Port 62000 ebenfalls ausgenommen werden.

### NOTE

Diese Ausnahme erfolgt auch dem DirectAccess-Server, und alle anderen Ausnahmen befinden sich auf der Edge-Firewall.

Bei Teredo- und IP6-zu-IP4-Datenverkehr sollten diese Ausnahmen für beide aufeinander folgenden öffentlichen IPv4-Adressen mit Internetzugriff auf dem DirectAccess-Server angewendet werden. Für IP-HTTPS müssen die Ausnahmen auf der Adresse angewendet werden, die auf dem öffentlichen DNS-Server registriert ist.

Die folgenden Ausnahmen sind für RAS-Datenverkehr erforderlich, wenn sich der DirectAccess-Server auf dem IPv6-Internet befindet:

- IP-Protokoll-ID 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend
- ICMPv6-Datenverkehr eingehend und ausgehend (nur wenn Teredo verwendet wird)

Wenden Sie bei zusätzlichen Firewalls die folgenden internen Netzwerkfirewallausnahmen für RAS-Datenverkehr an:

- ISATAP-Protokoll 41 eingehend und ausgehend
- TCP/UDP für den gesamten IPv4/- und Pv6-Datenverkehr
- ICMP für den gesamten IPv4- und IPv6 Datenverkehr (nur wenn Teredo verwendet wird)

## 1.3 Planen der Zertifikatanforderungen

Es gibt drei Szenarien, die Zertifikate erfordern, wenn Sie einen einzigen DirectAccess-Server bereitstellen:

- [1.3.1 Planen von Computer Zertifikaten für IPsec-Authentifizierung](#)

Zertifikatanforderungen für IPsec beinhalten ein Computerzertifikat, das von DirectAccess-Clientcomputern verwendet wird, wenn diese die IPsec-Verbindung zwischen dem Client und dem DirectAccess-Server herstellen, und einem Computerzertifikat, das von DirectAccess-Servern für das Einrichten von IPsec-Verbindungen mit DirectAccess-Clients verwendet wird.

Für DirectAccess in Windows Server 2012 ist die Verwendung dieser IPsec-Zertifikate nicht obligatorisch. Als Alternative kann der DirectAccess-Server als Kerberos-Proxy fungieren, damit die IPsec-Authentifizierung ohne erforderliche Zertifikate durchgeführt werden kann. Wenn das Kerberos-Protokoll verwendet wird, funktioniert dies über SSL, und der Kerberos-Proxy verwendet das Zertifikat, das für IP-HTTPS zu diesem Zwecke konfiguriert wurde. Einige Unternehmensszenarien (einschließlich Bereitstellung

für mehrere Standorte und Einmalkennwort-Clientauthentifizierung) erfordern die Verwendung der Zertifikatauthentifizierung, und nicht das Kerberos-Protokoll.

- [1.3.2 Planen von Zertifikaten für IP-HTTPS](#)

Wenn Sie Remotezugriff konfigurieren, wird der DirectAccess-Server automatisch für das Handeln als IP-HTTPS-Listener konfiguriert. Die IP-HTTPS-Website erfordert ein Websitezertifikat, und Clientcomputer müssen in der Lage sein, die CRL-Website (Certificate Revocation List, Zertifikatsperrlisten) für das Zertifikat zu kontaktieren.

- [1.3.3 Planen von Website Zertifikaten für den Netzwerkadressen Server](#)

Der Netzwerkadressenserver ist eine Website, die erkennt, ob sich Clientcomputer im Unternehmensnetzwerk befinden. Der Netzwerkadressenserver erfordert ein Websitezertifikat. DirectAccess-Clients müssen die CRL-Website für das Zertifikat kontaktieren können.

In der folgenden Tabelle werden die Zertifizierungsstellenanforderungen für jedes Szenario zusammengefasst.

IPSEC-AUTHENTIFIZIERUNG	IP-HTTPS-SERVER	NETZWERKADRESSEN SERVER
Eine interne Zertifizierungsstelle ist erforderlich, um Computer Zertifikate an den DirectAccess-Server und Clients für die IPSec-Authentifizierung auszugeben, wenn Sie nicht den Kerberos-Proxy für die Authentifizierung verwenden.	Interne Zertifizierungsstelle:  Sie können eine interne Zertifizierungsstelle für die Ausgabe des IP-HTTPS-Zertifikats verwenden; Sie müssen jedoch sicherstellen, dass der Sperrlisten-Verteilungspunkt extern verfügbar ist.	Interne Zertifizierungsstelle:  Sie können eine interne Zertifizierungsstelle für die Ausgabe des Netzwerkadressenserver-Websitezertifikats verwenden. Stellen Sie sicher, dass der Sperrlisten-Verteilungspunkt eine hohe Verfügbarkeit vom internen Netzwerk aus hat.
	Selbstsigniertes Zertifikat:  Sie können ein selbstsigniertes Zertifikat für den IP-HTTPS-Server verwenden; Sie müssen jedoch sicherstellen, dass der Sperrlisten-Verteilungspunkt extern verfügbar ist.  Ein selbstsigniertes Zertifikat kann nicht in Bereitstellungen für mehrere Standorte verwendet werden.	Selbstsigniertes Zertifikat:  Sie können ein selbstsigniertes Zertifikat für die Netzwerkadressenserver-Website verwenden.  Ein selbstsigniertes Zertifikat kann nicht in Bereitstellungen für mehrere Standorte verwendet werden.
	<b>Empfohlen</b>  Öffentliche Zertifizierungsstelle:  Es wird empfohlen, eine öffentliche Zertifizierungsstelle für die Ausgabe des IP-HTTPS-Zertifikats zu verwenden. Dadurch wird sichergestellt, dass der Sperrlisten-Verteilungspunkt extern verfügbar ist.	

### 1.3.1 Planen von Computerzertifikaten für IPsec-Authentifizierung

Wenn Sie zertifikatbasierte IPsec-Authentifizierung verwenden, müssen der DirectAccess-Server und die Clients ein Computerzertifikat erhalten können. Die einfachste Möglichkeit für die Installation der Zertifikate ist die Konfiguration der gruppenrichtlinienbasierten automatischen Registrierung für Computerzertifikate. Dadurch wird sichergestellt, dass alle Domänenmitglieder ein Zertifikat von einer Unternehmenszertifizierungsstelle erhalten. Wenn Sie keine Unternehmens Zertifizierungsstelle in Ihrer Organisation eingerichtet haben, finden Sie weitere

Informationen unter [Active Directory Certificate Services](#).

Für dieses Zertifikat gelten die folgenden Anforderungen:

- Das Zertifikat sollte eine Clientauthentifizierungs-EKU (Extended Key Usage, Erweiterte Schlüsselverwendung) haben.
- Das Clientzertifikat und das Serverzertifikat sollten zum selben Stammzertifikat gebunden sein. Das Stammzertifikat muss in den DirectAccess-Konfigurationseinstellungen ausgewählt sein.

### 1.3.2 Planen von Zertifikaten für IP-HTTPS

Der DirectAccess-Server fungiert als IP-HTTPS-Listener, und Sie müssen manuell ein HTTPS-Websitezertifikat auf dem Server installieren. Beachten Sie Folgendes bei der Planung:

- Die Verwendung einer öffentlichen Zertifizierungsstelle ist empfohlen, sodass Zertifikatsperrlisten bereits verfügbar sind.
- Geben Sie im Feld **Antragsteller** die IPv4-Adresse des Internetadapters des DirectAccess-Servers oder die FQDN der IP-HTTPS-URL an (die ConnectTo-Adresse). Falls sich der DirectAccess-Server hinter einem NAT-Gerät befindet, sollte der öffentliche Name oder die Adresse des NAT-Geräts angegeben werden.
- Der allgemeine Name des Zertifikats sollte dem Namen der IP-HTTPS-Website entsprechen.
- Geben Sie im Feld **Erweiterte Schlüsselverwendung** die Serverauthentifizierungs-Objektkennung (OID) an.
- Geben Sie im Feld **Sperrlisten-Verteilungspunkte** einen Zertifikatsperrlisten-Verteilungspunkt an, auf den mit dem Internet verbundene DirectAccess-Clients zugreifen können.
- Das IP-HTTPS-Zertifikat muss einen privaten Schlüssel enthalten.
- Das IP-HTTPS-Zertifikat muss direkt in den persönlichen Speicher importiert werden.
- Die Namen von IP-HTTPS-Zertifikaten können Platzhalter enthalten.

Falls Sie IP-HTTPS nicht auf einem Standardport verwenden werden, müssen Sie folgende Schritte auf dem DirectAccess-Server ausführen:

1. Entfernen Sie die vorhandene Zertifikatbindung für 0.0.0.0:443, und ersetzen Sie diese mit einer Zertifikatbindung für den ausgewählten Port. Für dieses Beispiel wird Port 44500 verwendet. Zeigen Sie vor dem Löschen der Zertifikatbindung **appid** an und kopieren Sie es.

- a. Geben Sie Folgendes ein, um die Zertifikatbindung zu löschen:

```
netsh http delete ssl ipport=0.0.0.0:443
```

- b. Geben Sie Folgendes ein, um eine neue Zertifikatbindung hinzuzufügen:

```
netsh http add ssl ipport=0.0.0.0:44500 certhash=<use the thumbprint from the DirectAccess server SSL cert> appid=<use the appid from the binding that was deleted>
```

2. Geben Sie Folgendes ein, um die IP-HTTPS-URL auf dem Server zu ändern:

```
Netsh int http set int url=https://<DirectAccess server name (for example server.contoso.com)>:44500/IPHTTPS
```

```
Net stop iphlpsvc & net start iphlpsvc
```

3. Ändern Sie die URL-Reservierung für kdcproxy.

- Geben Sie Folgendes ein, um die vorhandene URL-Reservierung zu löschen:

```
netsh http del urlacl url=https://+:443/KdcProxy/
```

- Geben Sie Folgendes ein, um eine neue URL-Reservierung hinzuzufügen:

```
netsh http add urlacl url=https://+:44500/KdcProxy/ sddl=D:(A;;GX;;;NS)
```

4. Fügen Sie die Einstellungen hinzu, um das Abhören von kpssvc auf dem Nicht-Standardport zu erzwingen.

Geben Sie Folgendes ein, um den Registrierungsschlüssel hinzuzufügen:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings /v HttpsUrlGroup /t REG_MULTI_SZ /d +:44500 /f
```

5. Geben Sie Folgendes ein, um den kdcproxy-Dienst auf dem Domänencontroller zu starten:

```
net stop kpssvc & net start kpssvc
```

Falls Sie IP-HTTPS nicht auf einem Standardport verwenden werden, müssen Sie folgende Schritte auf dem Domänencontroller ausführen:

1. Ändern Sie die IP-HTTPS-Einstellung im Client-Gruppenrichtlinienobjekt.

- Öffnen Sie den Gruppenrichtlinien-Editor.
- Navigieren Sie zu Computerkonfiguration=>Richtlinien=>Administrative Vorlagen=> Netzwerk=>TCPIP-Einstellungen=>IPv6-Übergangstechnologien.
- Öffnen Sie die IP-HTTPS-Statuseinstellung und ändern Sie die URL zu **https://<DirectAccess-Servername (z. B. server.contoso.com)>:44500/IPHTTPS**.
- Klicken Sie auf **Übernehmen**.

2. Ändern Sie die Kerberos-Proxy-Client-Einstellung im Client-Gruppenrichtlinienobjekt.

- Navigieren Sie im Gruppenrichtlinien-Editor zu Computerkonfiguration=>Richtlinien=>Administrative Vorlagen=> System=>Kerberos => Geben Sie die KDC-Proxyserver für Kerberos-Clients an.
- Öffnen Sie die IP-HTTPS-Statuseinstellung und ändern Sie die URL zu **https://<DirectAccess-Servername (z. B. server.contoso.com)>:44500/IPHTTPS**.
- Klicken Sie auf **Übernehmen**.

3. Ändern Sie die Client-IPsec-Richtlinieneinstellungen so, dass ComputerKerb und UserKerb verwendet werden.

- Navigieren Sie im Gruppenrichtlinien-Editor zu Computerkonfiguration=>Richtlinien=> Windows-Einstellungen=> Sicherheitseinstellungen=> Windows-Firewall mit erweiterter Sicherheit.
- Klicken Sie auf **Verbindungssicherheitsregeln**, und doppelklicken Sie dann auf IPsec-Regel.

- c. Klicken Sie auf der Registerkarte **Authentifizierung** auf **Erweitert**.
- d. Für Auth1: Entfernen Sie die vorhandene Authentifizierungsmethode, und ersetzen Sie diese mit ComputerKerb. Für Auth2: Entfernen Sie die vorhandene Authentifizierungsmethode, und ersetzen Sie diese mit „UserKerb“.
- e. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Führen Sie **gpupdate /force** auf den Clientcomputern und dem DirectAccess-Server aus, um den manuellen Prozess für die Verwendung eines IP-HTTPS-Nicht-Standardports abzuschließen.

### 1.3.3 Planen von Websitezertifikaten für den Netzwerkadressenserver

Beachten Sie Folgendes bei der Planung der Netzwerkadressenserver-Website:

- Im Feld **Antragsteller** muss die IP-Adresse der Intranetschnittstelle des Netzwerkadressenservers oder der FQDN der Netzwerkadressen-URL angegeben sein.
- Verwenden Sie im Feld **Erweiterte Schlüsselverwendung** die Serverauthentifizierungs-OID.
- Verwenden Sie im Feld **Sperrlisten-Verteilungspunkte** einen Zertifikatsperrlisten-Verteilungspunkt, auf den mit dem Intranet verbundene DirectAccess-Clients zugreifen können. Der Zertifikatsperrlisten-Verteilungspunkt sollte nicht von außerhalb des internen Netzwerks zugänglich sein.
- Wenn Sie zu einem späteren Zeitpunkt eine Bereitstellung für mehrere Standorte oder im Cluster planen, sollte der Name des Zertifikats nicht dem internen Namen eines DirectAccess-Servers entsprechen, der zur Bereitstellung hinzugefügt wird.

#### NOTE

Stellen Sie sicher, dass die Zertifikate für IP-HTTPS und den Netzwerkadressenserver einen **Antragstellename** haben. Wenn das Zertifikat keinen **Antragstellename**, aber einen **Alternativen Antragstellennamen** hat, wird es nicht vom RAS-Assistenten akzeptiert.

## 1.4 Planen der DNS-Anforderungen

In diesem Abschnitt werden die DNS-Anforderungen für DirectAccess-Clientanfragen und Infrastrukturserver in einer RAS-Bereitstellung erklärt. Der Abschnitt hat die folgenden Unterabschnitte:

- [1.4.1 Planen der DNS-Serveranforderungen](#)
- [1.4.2 Planen der lokalen Namensaauflösung](#)

### DirectAccess-Client Anforderungen

DNS wird verwendet, um Anfragen von DirectAccess-Clientcomputern aufzulösen, die sich nicht auf dem internen (oder Unternehmens-)Netzwerk befinden. DirectAccess-Clients versuchen, eine Verbindung zum DirectAccess-Netzwerkadressenserver herzustellen, um zu bestimmen, ob sie sich im Internet oder auf dem internen Netzwerk befinden.

- Bei erfolgreicher Verbindung werden die Clients als im internen Netzwerk befindlich identifiziert, DirectAccess wird nicht verwendet, und Clientanfragen werden mithilfe des DNS-Servers aufgelöst, welcher auf dem Netzwerkadapter des Clientcomputers konfiguriert ist.
- Wenn keine Verbindung hergestellt werden kann, wird davon ausgegangen, dass sich die Clients im Internet befinden, und DirectAccess-Clients verwenden die Richtlinientabelle für die Namensaauflösung (Name Resolution Policy Table, NRPT) verwenden, um zu bestimmen, welcher DNS-Server für die Auflösung der Namensanfragen verwendet werden soll.

Sie können angeben, dass Clients DirectAccess-DNS64 oder einen anderen internen DNS-Server für die Auflösung verwenden. Wenn Sie eine Namensauflösung durchführen, wird die NRPT von DirectAccess-Clients verwendet, um festzulegen, wie eine Anfrage behandelt werden soll. Clients fordern einen voll qualifizierten Namen oder einen Namen mit einer einzelnen Bezeichnung an, z. b. <https://internal>. Wenn ein Name mit einer einzelnen Bezeichnung gefordert ist, wird ein DNS-Suffix angehängt, um einen FQDN zu bilden. Wenn die DNS-Abfrage einem Eintrag in der NRPT entspricht, und DNS64 oder ein DNS-Server auf dem internen Netzwerk für den Eintrag angegeben wurde, wird die Abfrage für die Namensauflösung mithilfe des angegebenen Server gesendet. Wenn eine Übereinstimmung vorhanden ist, aber kein DNS-Server angegeben wurde, weist dies auf eine Ausnahmeregel hin, und die normale Namensauflösung wird verwendet.

#### **NOTE**

Wenn ein neues Suffix zur NRPT in der Remotezugriffs-Verwaltungskonsole hinzugefügt wird, können die Standard-DNS-Server für das Suffix automatisch erkannt werden, wenn Sie auf **Erkennen** klicken.

Die automatische Erkennung funktioniert wie folgt:

- Wenn das Unternehmensnetzwerk IPv4-basiert ist oder IPv4 und IPv6 verwendet, ist die Standardadresse die DNS64-Adresse des internen Adapters auf dem DirectAccess-Server.
- Wenn das Unternehmensnetzwerk IPv6-basiert ist, ist die Standardadresse die IPv6-Adresse der DNS-Server auf dem Unternehmensnetzwerk.

#### **Infrastruktur Server**

- **Netzwerkadressen Server**

DirectAccess-Clients versuchen, den Netzwerkadressenserver zu erreichen, um zu bestimmen, ob sie sich auf dem internen Netzwerk befinden. Clients im internen Netzwerk müssen in der Lage sein, den Namen des Netzwerkadressenservers aufzulösen, befinden sie sich jedoch im Internet, dürfen sie den Namen nicht auflösen. Um dies zu gewährleisten, wird der FQDN des Netzwerkadressenservers standardmäßig als Ausnahmeregel zum NRPT hinzugefügt. Außerdem werden bei der Konfiguration von RAS folgende Regeln automatisch erstellt:

- Eine DNS-Suffixregel für die Stammdomäne oder den Domänennamen des DirectAccess-Servers und die IPv6-Adressen, die der DNS64-Adresse entsprechen. In Unternehmensnetzwerken mit ausschließlich IPv6 sind die Intranet-DNS-Server auf dem DirectAccess-Server konfiguriert. Wenn der DirectAccess-Server z. B. Mitglied der Domäne corp.contoso.com ist, wird für das DNS-Suffix .corp.contoso.com eine Regel erstellt.
- Eine Ausnahmeregel für den FQDN des Netzwerkadressenservers. Wenn die Netzwerkadressen Server-URL z. b. <https://nls.corp.contoso.com> ist, wird eine Ausnahme Regel für den voll qualifizierten Namen (NLS.Corp.contoso.com) erstellt.

- **IP-HTTPS-Server**

Der DirectAccess-Server fungiert als IP-HTTPS-Listener und verwendet das Serverzertifikat zur Authentifizierung der IP-HTTPS-Clients. Der IP-HTTPS-Name muss von den DirectAccess-Clients aufgelöst werden können, die öffentliche DNS-Server verwenden.

- **CRL-Sperr Überprüfung**

DirectAccess verwendet Zertifikatsperrüberprüfungen für die IP-HTTPS-Verbindung zwischen den DirectAccess-Clients und dem DirectAccess-Server und für die HTTPS-basierte Verbindung zwischen dem DirectAccess-Client und dem Netzwerkadressenserver. In beiden Fällen müssen DirectAccess-Clients in der Lage sein, auf den Zertifikatsperrlisten-Verteilungspunkt zuzugreifen und ihn aufzulösen.

- **ISATAP**

ISATAP ermöglicht Unternehmenscomputern, eine IPv6-Adresse zu erhalten, und es kapselt IPv6-Pakete innerhalb eines IPv4-Headers. Es kann vom DirectAccess-Server verwendet werden, um IPv6-Konnektivität mit ISATAP-Hosts im gesamten Intranet bereitzustellen. In einer nicht systemeigenen IPv6-Netzwerkumgebung konfiguriert sich der DirectAccess-Server automatisch als ISATAP-Router.

Da ISATAP nicht mehr in DirectAccess unterstützt wird, müssen Sie sicherstellen, dass Ihre DNS-Server so konfiguriert sind, dass sie nicht auf ISATAP-Abfragen reagieren. In der Standardeinstellung blockiert der DNS-Serverdienst die Namensauflösung für den ISATAP-Namen über die globale DNS-Abfragesperrliste. Entfernen Sie nicht den ISATAP-Namen aus den globalen Abfragesperrlisten.

- **Konnektivitätsverifier**

RAS erstellt einen Standard-Webtest, der von DirectAccess-Clientcomputern dazu verwendet wird, die Konnektivität zum internen Netzwerk zu prüfen. Damit der Test wie erwartet funktioniert, müssen folgende Namen manuell in dem DNS registriert werden:

- **DirectAccess-WebProbe Host:** sollte in die interne IPv4-Adresse des DirectAccess-Servers oder die IPv6-Adresse in einer reinen IPv6-Umgebung aufgelöst werden.
- **DirectAccess-corpconnectivityhost:** sollte in die lokale Host Adresse (Loopback) aufgelöst werden. Die folgenden Host-(A)- und (AAAA)-Ressourceneinträge sollten erstellt werden: ein Host-(A)-Ressourceneintrag mit dem Wert 127.0.0.1 und der Host-(AAAA)-Ressourceneintrag mit dem aus dem NAT64-Präfix und den letzten 32-Bit als 127.0.0.1 ermittelten Wert. Das NAT64-Präfix kann durch Ausführen des Windows PowerShell-Befehls `get-netnattransitionconfiguration` abgerufen werden.

**NOTE**

Dies gilt nur in einer IPv4-Umgebung. In einer Umgebung mit IPv4 plus IPv6 oder in einer reinen IPv6-Umgebung sollte nur ein Host-(AAAA)-Ressourceneintrag mit der Loopback-IP-Adresse ::1 erstellt werden.

Mithilfe anderer Webadressen über HTTP oder `ping` können Sie zusätzliche Verbindungsprüfer erstellen. Für jeden Verbindungsprüfer muss ein DNS-Eintrag vorhanden sein.

#### 1.4.1 Planen der DNS-Serveranforderungen

Nachfolgend sind die DNS-Anforderungen für eine DirectAccess-Bereitstellung aufgeführt.

- Für DirectAccess-Clients müssen Sie einen DNS-Server verwenden, auf dem Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder ein anderer DNS-Server ausgeführt wird, der IPv6 unterstützt.

**NOTE**

Es wird nicht empfohlen, DNS-Server zu verwenden, auf denen Windows Server 2003 ausgeführt wird, wenn Sie DirectAccess bereitstellen. Windows Server 2003-DNS-Server unterstützen zwar IPv6-Datensätze, doch Windows Server 2003 wird nicht mehr von Microsoft unterstützt. Darüber hinaus sollten Sie DirectAccess nicht bereitstellen, wenn auf Ihren Domänencontrollern Windows Server 2003 aufgrund eines Problems mit dem Dateireplikationsdienst ausgeführt wird. Weitere Informationen finden Sie unter [DirectAccess: nicht unterstützte Konfigurationen](#).

- Verwenden Sie einen DNS-Server, der dynamische Updates unterstützt. Sie können DNS-Server verwenden, die keine dynamischen Updates unterstützen, es ist dann jedoch erforderlich, dass Sie Einträge auf diesen Servern manuell aktualisieren.
- Der FQDN für die über das Internet erreichbaren Sperrlisten-Verteilungspunkte müssen über Internet-DNS-

Server auflösbar sein. Wenn sich beispielsweise der URL-<https://crl.contoso.com/crl/corp-DC1-CA.crl> im Feld **CRL-Verteilungs Punkte** des IP-HTTPS-Zertifikats des DirectAccess-Servers befindet, müssen Sie sicherstellen, dass der voll qualifizierte Name crld.contoso.com mithilfe von Internet-DNS-Servern aufgelöst werden kann.

#### 1.4.2 Planen der lokalen Namensauflösung

Beachten Sie folgende Punkte, wenn Sie eine lokale Namensauflösung planen:

##### NRPT

In folgenden Fällen müssen Sie eventuell zusätzliche NRPT-Regeln erstellen:

- Falls Sie weitere DNS-Suffixe für den Intranetnamespace hinzufügen müssen.
- Wenn der vollqualifizierter Domänenname (FQDN) der Zertifikatsperllisten-Verteilungspunkte auf dem Intranetnamespace beruhen, müssen Sie Ausnahmeregeln für die FQDNs der Zertifikatsperllisten-Verteilungspunkte hinzufügen.
- Wenn Sie über eine Split-Brain-DNS-Umgebung verfügen, müssen Sie Ausnahmeregeln für die Namen von Ressourcen hinzufügen, für die DirectAccess-Clients im Internet auf die Internetversion anstatt auf die Intranetversion zugreifen sollen.
- Wenn Sie Datenverkehr über Ihre Intranet-Webproxyserver zu einer externen Website weiterleiten, ist die externe Website nur über das Internet verfügbar und verwendet die Adressen des Webproxyservers, um die eingehenden Anfragen zuzulassen. Fügen Sie in diesem Fall eine Ausnahmeregel für den FQDN der externen Website hinzu, und geben Sie an, dass die Regel den Intranet-Webproxyserver und nicht die IPv6-Adressen des Intranet-DNS-Server verwenden soll.

Wenn Sie beispielsweise die externe Website test.contoso.com testen, kann dieser Name nicht über Internet-DNS-Server aufgelöst werden. Der Webproxyserver von Contoso kann den Namen jedoch auflösen und Anforderungen an die Website an den externen Webserver weiterleiten. Um den Sitezugriff durch Benutzer zu verhindern, die sich nicht im Contoso-Intranet befinden, lässt die externe Website nur Anforderungen von der IPv4-Internetadresse des Contoso-Webproxys zu. Da Intranetbenutzer den Contoso-Webproxy verwenden, können sie auf die Website zugreifen. Dies gilt jedoch nicht für DirectAccess-Benutzer, da diese den Contoso-Webproxy nicht verwenden. Wenn eine NRPT-Ausnahmeregel für test.contoso.com konfiguriert wird, die den Contoso-Webproxy verwendet, werden Webseitenanforderungen für test.contoso.com über das IPv4-Internet zum Intranet-Webproxyserver weitergeleitet.

#### Namen mit einer einzelnen Bezeichnung

Namen mit einer einzelnen Bezeichnung, wie z. B. <https://paycheck>, werden manchmal für Intranetserver verwendet. Wenn ein einteiliger Name erforderlich ist und eine DNS-Suffixsuchliste konfiguriert wird, werden die DNS-Suffixe in der Liste an den einteiligen Namen angehängt. Wenn z. B. ein Benutzer auf einem Computer, der Mitglied der Corp.contoso.com-Domänen Typen ist, im Webbrowser <https://paycheck>, lautet der als Name erstellte FQDN Paycheck.Corp.contoso.com. Standardmäßig basiert das angehängte Suffix auf dem primären DNS-Suffix des Clientcomputers.

##### NOTE

In einem zusammenhanglosen Namespace-Szenario, in dem ein oder mehrere Domänencomputer ein DNS-Suffix haben, das nicht der Active Directory-Domäne entspricht, zu dem die Computer gehören, müssen Sie sicherstellen, dass die Suchliste alle erforderlichen Suffixe enthält. Der RAS-Assistent wird den Active Directory-DNS-Namen standardmäßig als primäres DNS-Suffix auf dem Client konfigurieren. Stellen Sie sicher, dass Sie das DNS-Suffix hinzufügen, das von den Clients für die Namensauflösung verwendet wird.

Wenn mehrere Domänen und Windows Internet Name Service (WINS) in der Organisation bereitgestellt werden

und Sie sich remote verbinden, können Einzelnamen wie folgt aufgelöst werden:

- Stellen Sie eine WINS-Forward-Lookupzone im DNS bereit. Wenn versucht wird, computername.dns.zone1.corp.contoso.com aufzulösen, wird die Anfrage zum WINS-Server geleitet, der nur computername verwendet. Der Client denkt, dass er einen regulären DNS-Host-(A)-Ressourceneintrag ausgibt, obwohl es sich eigentlich um eine NetBIOS-Anfrage handelt. Weitere Informationen finden Sie unter „Verwalten einer Forward-Lookupzone“.
- Fügen Sie ein DNS-Suffix, zum Beispiel dns.zone1.corp.contoso.com, zum Standarddomänenrichtlinien-Gruppenrichtlinienobjekt hinzu.

## Split-Brain-DNS

Wird sowohl für Internet- als auch für Intranet-Namensauflösung die gleiche DNS-Domäne verwendet, wird dies als „Split-Brain-DNS“ bezeichnet.

Bei Split-Brain-DNS-bereit Stellungen müssen Sie die vollständig im Internet und im Intranet duplizierten voll qualifizierten Domänen Namen auflisten und entscheiden, welche Ressourcen der DirectAccess-Client erreichen soll: die Intranet- oder die Internet Version. Für alle Namen, die einer Ressource entsprechen, für die der DirectAccess-Client auf die Internetversion zugreifen soll, müssen Sie der NRPT den entsprechenden FQDN als Ausnahmeregel für die DirectAccess-Clients hinzufügen.

Wenn in einer Split-Brain-DNS-Umgebung beide Versionen der Ressource verfügbar sein sollen, konfigurieren Sie die Intranetressourcen mit alternativen Namen, bei denen es sich nicht um Duplikate der Namen handelt, die im Internet verwendet werden, und weisen Sie die Benutzer an, im Intranet den alternativen Namen zu verwenden. So können Sie beispielsweise für das Intranet den alternativen Namen [www.internal.contoso.com](http://www.internal.contoso.com) anstelle von [www.contoso.com](http://www.contoso.com) konfigurieren.

In einer Umgebung ohne Split-Brain-DNS unterscheidet sich der Internetnamespace vom Intranetnamespace. Die Contoso Corporation verwendet z. B. im Internet {1}contoso.com{2} und im Intranet {3}corp.contoso.com{4}. Da alle Intranetressourcen das DNS-Suffix corp.contoso.com verwenden, leitet die NRPT-Regel für corp.contoso.com alle DNS-Namensabfragen für Intranetressourcen an Intranet-DNS-Server weiter. DNS-Namensabfragen für Namen mit dem Suffix contoso.com entsprechen nicht der corp.contoso.com-Intranetnamespace-Regel in der NRPT und werden daher an Internet-DNS-Server gesendet. Bei einer Bereitstellung ohne Split-Brain-DNS ist für die NRPT keine zusätzliche Konfiguration erforderlich, da keine Doppelung der FQDNs für Intranet- und Internetressourcen auftritt. DirectAccess-Clients können sowohl auf die Internet- als auch auf die Intranetressourcen ihrer Organisation zugreifen.

## Lokales Namensauflösungsverhalten für DirectAccess-Clients

Wenn ein Name nicht mit DNS aufgelöst werden kann, um den Namen im lokalen Subnetz aufzulösen, kann der DNS-Client Dienst in Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows 8 und Windows 7 die lokale Namensauflösung verwenden, wobei die Protokolle Link-Local Multicast Name Resolution (LLMNR) und NetBIOS über TCP/IP verwendet werden.

Die lokale Namensauflösung ist in der Regel für Peer-zu-Peer-Verbindungen erforderlich, wenn sich der Computer in privaten Netzwerken befindet, z. B. in einem Heimnetzwerk mit einem einzelnen Subnetz. Wenn der DNS-Clientdienst eine lokale Namensauflösung für Intranetservernamen ausführt, und der Computer mit einem freigegebenen Subnetz im Internet verbunden ist, können böswillige Benutzer über TCP/IP-Nachrichten LLMNR und NetBIOS erfassen, um Intranetservernamen zu ermitteln. Auf der DNS-Seite des Assistenten zum Einrichten des Infrastrukturervers konfigurieren Sie das lokale Namensauflösungsverhalten anhand der von den Intranet-DNS-Servern empfangenen Antworttypen. Die folgenden Optionen sind verfügbar:

- **Verwenden der lokalen Namensauflösung, wenn der Name nicht im DNS vorhanden ist.** Diese Option ist die sicherste, da der DirectAccess-Client nur für die Servernamen eine lokale Namensauflösung ausführt, die nicht von den Intranet-DNS-Servern aufgelöst werden können. Wenn die Intranet-DNS-Server erreicht werden können, werden die Namen der Intranetserver aufgelöst. Wenn die Intranet-DNS-Server

nicht erreicht werden können, oder wenn andere DNS-Fehler auftreten, werden die Intranetservernamen nicht über die lokale Namensauflösung ins Subnetz durchgelassen.

- **Verwenden der lokalen Namensauflösung, wenn der Name nicht im DNS vorhanden ist oder DNS-Server nicht erreichbar sind, wenn der Clientcomputer sich auf einem privaten Netzwerk befindet (empfohlen)**. Diese Option ist wird empfohlen, da sie die Verwendung der lokalen Namensauflösung in einem privaten Netzwerk gestattet, wenn die Intranet-DNS-Server nicht erreichbar sind.
- **Verwenden der lokalen Namensauflösung für alle Arten von DNS-Auflösungsfehlern (am wenigsten sicher)**. Dies ist die unsicherste Option, da die Namen von Intranet-Netzwerkservern über die lokale Namensauflösung zum lokalen Subnetz durchgelassen werden können.

## 1.5 Planen des Netzwerkadressenservers

Der Netzwerkadressenserver ist eine Website, die erkennt, ob sich DirectAccess-Clients im Unternehmensnetzwerk befinden. Clients im Unternehmensnetzwerk verwenden kein DirectAccess, um interne Ressourcen zu erreichen, stattdessen stellen Sie direkt eine Verbindung her.

Der Netzwerkadressenserver kann auf dem DirectAccess-Server oder auf einem anderen Server in der Organisation installiert werden. Wenn Sie den Netzwerkadressenserver auf dem DirectAccess-Server hosten, wird die Website automatisch erstellt, wenn Sie die RAS-Serverrolle installieren. Wenn Sie den Netzwerkadressenserver auf einem anderen Server in Ihrer Organisation hosten, auf dem ein Windows-Betriebssystem läuft, müssen Sie sicherstellen, dass Internet Information Services (IIS) auf diesem Server installiert ist und dass die Website erstellt wird. DirectAccess konfiguriert keine Einstellungen auf einem Remote-Netzwerkadressenserver.

Stellen Sie sicher, dass die Netzwerkadressenserver-Website folgende Anforderungen erfüllt:

- Ist eine Website mit einem HTTPS-Serverzertifikat.
- DirectAccess-Clientcomputer müssen der Zertifizierungsstelle vertrauen, die das Serverzertifikat zur Netzwerkadressenserver-Website ausgegeben hat.
- DirectAccess-Clientcomputer auf dem internen Netzwerk müssen in der Lage sein, den Namen der Netzwerkadressenserver-Website aufzulösen.
- Die Netzwerkadressenserver-Website muss eine hohe Verfügbarkeit für Computer auf dem internen Netzwerk haben.
- Der Netzwerkadressenserver darf nicht für DirectAccess-Clientcomputer auf dem internen Netzwerk erreichbar sein.
- Das Serverzertifikat muss anhand einer Zertifikatsperlliste überprüft werden.

### 1.5.1 Planen von Zertifikaten für den Netzwerkadressenserver

Beachten Sie Folgendes, wenn Sie das Websitezertifikat für den Netzwerkadressenserver abrufen:

1. Im Feld **Antragsteller** muss eine IP-Adresse der Intranetschnittstelle des Netzwerkadressenservers oder der FQDN der Netzwerkadressen-URL angegeben sein.
2. Verwenden Sie im Feld **Erweiterte Schlüsselverwendung** die Serverauthentifizierungs-OID.
3. Verwenden Sie im Feld **Sperrlisten-Verteilungspunkte** einen Zertifikatsperllisten-Verteilungspunkt, auf den mit dem Intranet verbundene DirectAccess-Clients zugreifen können. Der Zertifikatsperllisten-Verteilungspunkt sollte nicht von außerhalb des internen Netzwerks zugänglich sein.

### 1.5.2 Planen von DNS für den Netzwerkadressenserver

DirectAccess-Clients versuchen, den Netzwerkadressenserver zu erreichen, um zu bestimmen, ob sie sich auf dem

internen Netzwerk befinden. Clients im internen Netzwerk müssen in der Lage sein, den Namen des Netzwerkadressenservers aufzulösen, befinden sie sich jedoch im Internet, dürfen sie den Namen nicht auflösen. Um dies zu gewährleisten, wird der FQDN des Netzwerkadressenservers standardmäßig als Ausnahmeregel zum NRPT hinzugefügt.

## 1.6 Planen der Verwaltungsserver

DirectAccess-Clients initiieren die Kommunikation mit Verwaltungsservern, welche Dienste wie Windows Update und Antivirus-Updates zur Verfügung stellen. DirectAccess-Clients verwenden zudem das Kerberos-Protokoll für den Kontakt zu Domänencontroller, um diese zu authentifizieren, bevor sie auf das interne Netzwerk zugreifen. Während der Remoteverwaltung von DirectAccess-Clients kommunizieren Verwaltungsserver mit Clientcomputern, um Verwaltungsfunktionen wie zum Beispiel Software- oder Hardware-Bestandsbewertungen durchzuführen. Der Remotezugriff kann automatisch bestimmte Verwaltungsserver erkennen, zum Beispiel:

- Domänen Controller: die automatische Ermittlung von Domänen Controllern wird für alle Domänen in derselben Gesamtstruktur wie der DirectAccess-Server und die Client Computer durchgeführt.
- Microsoft Endpoint Configuration Manager-Server: die automatische Ermittlung von Configuration Manager Servern wird für alle Domänen in derselben Gesamtstruktur wie der DirectAccess-Server und die Client Computer durchgeführt.

Domänen Controller und Configuration Manager Server werden automatisch erkannt, wenn DirectAccess erstmalig konfiguriert wird. Erkannte Domänen Controller werden nicht in der-Konsole angezeigt, aber die Einstellungen können mithilfe des Windows PowerShell-Cmdlets **Get-damgmtserver-Type all** abgerufen werden. Wenn Domänen Controller oder Configuration Manager Server geändert werden, wird durch Klicken auf **Verwaltungs Server aktualisieren** in der Remote Zugriffs-Verwaltungskonsole die Management Server Liste aktualisiert.

### Verwaltungs Serveranforderungen

- Verwaltungsserver müssen über den ersten (Infrastruktur)-Tunnel erreichbar sein. Wenn Sie Remotezugriff konfigurieren, werden diese beim Hinzufügen von Servern zur Verwaltungsserverliste automatisch über diesen Tunnel erreichbar gemacht.
- Verwaltungsserver, die Verbindungen zu DirectAccess-Clients initiieren, müssen IPv6 vollständig unterstützen, durch eine systemeigene IPv6-Adresse oder die Verwendung einer durch ISATAP zugewiesenen Adresse.

## 1.7 Planen der Active Directory-Domänendienste

In diesem Abschnitt wird erklärt, wie DirectAccess Active Directory-Domänendienste (AD DS) verwendet. Er ist in folgende Unterabschnitte gegliedert:

- [1.7.1 Planen der Client Authentifizierung](#)
- [1.7.2 Planen mehrerer Domänen](#)

DirectAccess verwendet AD DS und Active Directory Gruppenrichtlinien Objekte (Group Policy Objects, GPOs) wie folgt:

- **Authentifizierung**

AD DS wird für die Authentifizierung verwendet. Der Infrastrukturtunnel verwendet NTLMv2-Authentifizierung für das Computerkonto, das eine Verbindung zum DirectAccess-Server herstellt, und das Konto muss in einer Active Directory-Domäne aufgelistet sein. Der Intranettunnel verwendet für den Benutzer die Kerberos-Authentifizierung, um einen zweiten Tunnel zu erstellen.

- **Gruppenrichtlinie Objekte**

DirectAccess sammelt Konfigurationseinstellungen in Gruppenrichtlinienobjekten, die auf DirectAccess-Server, Clients und interne Anwendungsserver angewendet werden.

- **Sicherheitsgruppen**

DirectAccess verwendet Sicherheitsgruppen, um DirectAccess-Clientcomputer zu sammeln und zu identifizieren. Die Gruppenrichtlinien werden auf die erforderlichen Sicherheitsgruppen angewendet.

- **Erweiterte IPSec-Richtlinien**

DirectAccess kann IPsec-Authentifizierung und -Verschlüsselung zwischen Clients und dem DirectAccess-Server verwenden. Sie können die IPsec-Authentifizierung und -Verschlüsselung vom Client zu den angegebenen internen Anwendungsservern erweitern. Fügen Sie dazu die erforderlichen Anwendungsserver zu einer Sicherheitsgruppe hinzu.

## AD DS-Anforderungen

Wenn Sie AD DS für eine DirectAccess-Bereitstellung planen, müssen Sie folgende Anforderungen berücksichtigen:

- Es muss mindestens ein Domänen Controller mit dem Betriebssystem Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008 installiert werden.

Wenn sich der Domänencontroller in einem Umkreisnetzwerk befindet (und deshalb von einem Netzwerkadapter mit Internetzugriff des DirectAccess-Servers aus erreichbar ist), müssen Sie verhindern, dass der DirectAccess-Server den Domänencontroller erreicht, indem Sie dem Domänencontroller Paketfilter hinzufügen, damit die Konnektivität zur IP-Adresse des Internetadapters unterbunden wird.

- Der DirectAccess-Server muss Domänenmitglied sein.
- DirectAccess-Clients müssen Domänenmitglieder sein. Clients können folgenden Domänen angehören:
  - Domänen, die zur gleichen Gesamtstruktur wie der DirectAccess-Server gehören.
  - Domänen mit bidirektonaler Vertrauensstellung zur DirectAccess-Serverdomäne.
  - Domänen in einer Gesamtstruktur mit bidirektonaler Vertrauensstellung zu der Gesamtstruktur, der die DirectAccess-Domäne angehört.

### NOTE

- Der DirectAccess-Server kann nicht als Domänencontroller verwendet werden.
- Der für DirectAccess verwendete Active Directory-Domänencontroller darf nicht von einem externen Internetadapter des DirectAccess-Servers aus erreichbar sein (der Adapter darf sich nicht im Domänenprofil der Windows-Firewall befinden).

### 1.7.1 Planen der Clientauthentifizierung

Mit DirectAccess können Sie für die IPsec-Computerauthentifizierung zwischen der Verwendung von Zertifikaten oder eines integrierten Kerberos-Proxy, der die Computer über Benutzernamen und Kennwörter authentifiziert, wählen.

Wenn Sie sich entscheiden, AD DS-Anmeldedaten für die Authentifizierung zu verwenden, nutzt DirectAccess einen Sicherheitstunnel, der Computer (Kerberos) als erste Authentifizierung und Benutzer (Kerberos) als zweite Authentifizierung verwendet. Wenn Sie diesen Authentifizierungsmodus verwenden, nutzt DirectAccess einen einzigen Sicherheitstunnel, der Zugriff auf den DNS-Server, den Domänencontroller, und zu anderen Servern auf dem internen Netzwerk bietet.

Wenn Sie sich für die zweistufige Authentifizierung oder Netzwerzkugriffsschutz entscheiden, verwendet DirectAccess zwei Sicherheitstunnel. Der Remotezugriffs-Setup-Assistent konfiguriert die

Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit, die beim Aushandeln der IPsec-Sicherheitszuordnungen für die Tunnel zum DirectAccess-Server die Verwendung der folgenden Typen von Anmeldeinformationen angeben:

- Für den Infrastrukturtunnel erfolgt die erste Authentifizierung über die Anmeldeinformationen Computer (Kerberos) und die zweite über Benutzer (Kerberos).
- Für den Intranettunnel erfolgt die erste Authentifizierung über die Anmeldeinformationen Computerzertifikat und die zweite über Benutzer (Kerberos).

Wenn DirectAccess den Zugriff auf Clients mit Windows 7 oder in einer Bereitstellung mit mehreren Standorten zulässt, werden zwei Sicherheitstunnel verwendet. Der Remotezugriffs-Setup-Assistent konfiguriert die Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit, die beim Aushandeln der IPsec-Sicherheitszuordnungen für die Tunnel zum DirectAccess-Server die Verwendung der folgenden Typen von Anmeldeinformationen angeben:

- Für den Infrastrukturtunnel erfolgt die erste Authentifizierung über die Anmeldeinformationen Computerzertifikat und die zweite über NTLMv2. Bei NTLMv2-Anmeldeinformationen wird die Verwendung von AuthIP (Authenticated Internet Protocol) erzwungen und Zugriff auf einen DNS-Server und einen Domänencontroller bereitgestellt, bevor der DirectAccess-Client für den Intranettunnel Kerberos-Anmeldeinformationen verwenden kann.
- Für den Intranettunnel erfolgt die erste Authentifizierung über die Anmeldeinformationen Computerzertifikat und die zweite über Benutzer (Kerberos).

### 1.7.2 Planen mehrerer Domänen

Die Liste der Verwaltungsserver sollte die Domänencontroller von allen Domänen umfassen, welche Sicherheitsgruppen enthalten, die DirectAccess-Clientcomputer beinhalten. Es sollten alle Domänen enthalten sein, die Benutzerkonten umfassen, welche möglicherweise Computer nutzen, die als DirectAccess-Clients konfiguriert sind. Dadurch wird sichergestellt, dass Benutzer, die sich nicht in derselben Domäne wie der von ihnen genutzte Clientcomputer befinden, mit einem Domänencontroller in der Benutzerdomäne authentifiziert werden. Dies erfolgt automatisch, wenn sich Domänen in derselben Struktur befinden.

#### NOTE

Im Falle von Computern in Sicherheitsgruppen, welche für Clientcomputer oder Anwendungsserver in unterschiedlichen Strukturen verwendet werden, werden die Domänencontroller dieser Strukturen nicht automatisch erkannt. Sie können die Aufgabe **Verwaltungsserver aktualisieren** in der Remotezugriffs-Verwaltungskonsole ausführen, um diese Domänencontroller zu finden.

Wenn möglich sollten allgemeine Domänennamensuffixe während der Remotezugriffs-Bereitstellung zur Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) hinzugefügt werden. Wenn es zum Beispiel zwei Domänen gibt, domain1.corp.contoso.com und domain2.corp.contoso.com, können Sie, anstatt zwei Einträge zur NRPT hinzuzufügen, auch einen allgemeinen DNS-Suffix-Eintrag hinzufügen, bei dem das Domänennamensuffix corp.contoso.com ist. Dies geschieht automatisch für Domänen in demselben Stamm. Domänen, die sich nicht im selben Stamm befinden, müssen manuell hinzugefügt werden.

Wenn Windows Internet Name Service (WINS) in einer Umgebung mit mehreren Domänen bereitgestellt wird, müssen Sie eine WINS-Forward-Lookupzone in DNS bereitstellen. Weitere Informationen finden Sie weiter oben in diesem Dokument unter Name der **einzelnen Bezeichnungen** im Abschnitt "1.4.2 Planen der lokalen Namensauflösung".

## 1.8 Planen von Gruppenrichtlinienobjekten

In diesem Abschnitt wird die Rolle der Gruppenrichtlinienobjekte (GPOs) in der Remotezugriffsinfrastruktur erklärt.

Der Abschnitt ist in folgende Unterabschnitte gegliedert:

- [1.8.1 konfigurieren automatisch erstellter Gruppenrichtlinien Objekte](#)
- [1.8.2 konfigurieren manuell erstellter Gruppenrichtlinien Objekte](#)
- [1.8.3 Verwalten von Gruppenrichtlinien Objekten in einer Umgebung mit mehreren Domänen Controllern](#)
- [1.8.4 Verwalten von Remote Zugriffs-Gruppenrichtlinien Objekten mit eingeschränkten Berechtigungen](#)
- [1.8.5 wiederherstellen aus einem gelöschten GPO](#)

DirectAccess-Einstellungen, die bei der Konfiguration des Remotezugriffs konfiguriert werden, werden in GPOs gesammelt. Die folgenden Arten von Gruppenrichtlinienobjekten werden mit DirectAccess-Einstellungen aufgefüllt und wie folgt verteilt:

- **DirectAccess-Client-GPO**

Dieses Gruppenrichtlinienobjekt enthält die Client-Einstellungen, einschließlich der Einstellungen für die IPv6-Übergangstechnologie, der Einträge in der Richtlinientabelle für die Namensauflösung und der Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit. Das Gruppenrichtlinienobjekt wird auf die für die Clientcomputer angegebenen Sicherheitsgruppen angewendet.

- **DirectAccess-Server-Gruppenrichtlinien Objekt**

Dieses Gruppenrichtlinienobjekt enthält die DirectAccess-Konfigurationseinstellungen, die auf den als DirectAccess-Server konfigurierten Server in Ihrer Bereitstellung angewendet werden. Außerdem enthält es die Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit.

- **Anwendungsserver-Gruppenrichtlinien Objekt**

Dieses Gruppenrichtlinienobjekt enthält Einstellungen ausgewählter Anwendungsserver, auf die Sie die Authentifizierung und Verschlüsselung der DirectAccess-Clients erweitern können. Wenn die Authentifizierung und die Verschlüsselung nicht erweitert werden, wird dieses Gruppenrichtlinienobjekt nicht verwendet.

Es gibt zwei Möglichkeiten, Gruppenrichtlinienobjekte zu konfigurieren:

- **Automatisch:** Sie können angeben, dass Sie automatisch erstellt werden. Für jedes Gruppenrichtlinienobjekt wird ein Standardname angegeben.
- **Manuell:** Sie können GPOs verwenden, die vom Active Directory-Administrator vordefiniert wurden.

**NOTE**

Es können keine anderen Gruppenrichtlinienobjekte mehr konfiguriert werden, nachdem DirectAccess auf die Verwendung bestimmter Gruppenrichtlinienobjekte konfiguriert wurde.

Unabhängig davon, ob Sie automatisch oder manuell konfigurierte Gruppenrichtlinienobjekte verwenden, müssen Sie für die Erkennung langsamer Verbindungen eine Richtlinie hinzufügen, wenn die Clients 3G-Netzwerke verwenden. Der Pfad für **Richtlinie: Konfigurieren der Erkennung langsamer Verbindungen für die Gruppenrichtlinie** lautet: Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Gruppenrichtlinie.

**Caution**

Verwenden Sie das folgende Verfahren, um alle Remote Zugriffs-Gruppenrichtlinien Objekte zu sichern, bevor Sie DirectAccess-Cmdlets ausführen: [Sichern und Wiederherstellen der Remote Zugriffs Konfiguration](#).

Wenn die korrekten Berechtigungen für das Verknüpfen von Gruppenrichtlinienobjekten, die in den folgenden Abschnitten aufgeführt sind, fehlen, wird eine Warnung angezeigt. Der Remotezugriffsvorgang wird fortgesetzt,

Verknüpfungen werden jedoch nicht erstellt. Wenn diese Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, selbst wenn die Berechtigungen zu einem späteren Zeitpunkt hinzugefügt werden. Stattdessen muss der Administrator die Links manuell erstellen.

### **1.8.1 Konfigurieren automatisch erstellter Gruppenrichtlinienobjekte**

Beachten Sie beim Verwenden automatisch erstellter Gruppenrichtlinienobjekte Folgendes:

Automatisch erstellte Gruppenrichtlinienobjekte werden entsprechend des Speicherorts und Verknüpfungszielparameters wie folgt angewendet:

- Bei Gruppenrichtlinienobjekten des DirectAccess-Servers zeigen der Speicherortparameter und der Verknüpfungsparameter auf die Domäne, die den DirectAccess-Server enthält.
- Beim Erstellen der Gruppenrichtlinienobjekte für Client und Anwendungsserver wird der Speicherort auf eine Domäne festgelegt, auf der das Gruppenrichtlinienobjekt erstellt wird. Der Gruppenrichtlinienobjektname wird in jeder Domäne nachgeschlagen und mit DirectAccess-Einstellungen aufgefüllt, falls vorhanden. Das Verknüpfungsziel wird auf den Stamm der Domäne festgelegt, in der das Gruppenrichtlinienobjekt erstellt wurde. Für jede Domäne, die Clientcomputer oder Anwendungsserver enthält, wird ein Gruppenrichtlinienobjekt erstellt, und das Gruppenrichtlinienobjekt wird mit dem Stamm der entsprechenden Domäne verknüpft.

Beim Verwenden automatisch erstellter Gruppenrichtlinienobjekte benötigt der DirectAccess-Administrator zum Anwenden der DirectAccess-Einstellungen folgende Berechtigungen:

- Schreibberechtigungen für die Gruppenrichtlinienobjekte für jede Domäne
- Verknüpfungsberechtigungen für alle ausgewählten Clientdomänenstämme
- Verknüpfungsberechtigungen für die Server-Gruppenrichtlinien-Domänenstämme

Außerdem werden noch die folgenden Berechtigungen benötigt:

- Erstellen, Bearbeiten, Löschen und Ändern von Sicherheitsberechtigungen sind für die Gruppenrichtlinienobjekte erforderlich.
- Es wird empfohlen, dass der Remotezugriffsadministrator über Leserechte für Gruppenrichtlinienobjekte für jede Domäne verfügt. So kann der Remotezugriff prüfen, dass beim Erstellen von Gruppenrichtlinienobjekten keine Gruppenrichtlinienobjekte mit doppelten Namen vorhanden sind.

### **1.8.2 Konfigurieren manuell erstellter Gruppenrichtlinienobjekte**

Beachten Sie beim Verwenden manuell erstellter Gruppenrichtlinienobjekte Folgendes:

- Die Gruppenrichtlinienobjekte sollten vorhanden sein, bevor Sie den Remotezugriffs-Setup-Assistenten ausführen.
- Der Remotezugriffsadministrator muss in den manuell erstellten Gruppenrichtlinienobjekten über uneingeschränkte Berechtigungen für manuell erstellte Gruppenrichtlinienobjekte verfügen (Bearbeiten, Löschen, Ändern der Sicherheit).
- In der gesamten Domäne erfolgt eine Suche nach einer Verknüpfung zum Gruppenrichtlinienobjekt. Wenn das Gruppenrichtlinienobjekt in der Domäne nicht verknüpft ist, wird im Domänenstamm automatisch eine Verknüpfung erstellt. Wenn die zum Erstellen der Verknüpfung erforderlichen Berechtigungen nicht verfügbar sind, wird eine Warnung ausgegeben.

### **1.8.3 Verwalten von Gruppenrichtlinienobjekten in einer Umgebung mit mehreren Domänencontrollern**

Jedes Gruppenrichtlinienobjekt wird von einem bestimmten Domänencontroller wie folgt verwaltet:

- Das Server-Gruppenrichtlinienobjekt wird von einem der Domänencontroller im Active Directory-Standort verwaltet, der dem Server zugeordnet ist. Wenn die Domänencontroller an diesem Standort

schreibgeschützt sind, wird das Server-Gruppenrichtlinienobjekt vom Domänencontroller mit Schreibzugriff verwaltet, der am nächsten beim DirectAccess-Server liegt.

- Client- und Anwendungsserver-Gruppenrichtlinienobjekte werden vom Domänencontroller verwaltet, der als primärer Domänencontroller (PDC) ausgeführt wird.

Berücksichtigen Sie Folgendes, wenn Sie die Gruppenrichtlinienobjekt-Einstellungen manuell ändern möchten:

- Führen Sie für das Server-Gruppenrichtlinienobjekt von einer Eingabeaufforderung mit erhöhten Rechten auf dem DirectAccess-Server `nltest /dsgetdc: /writable` aus, um festzulegen, welcher Domänencontroller dem DirectAccess-Server zugeordnet ist.
- Wenn Sie Änderungen mit Windows PowerShell-Cmdlets für Netzwerke oder von der Gruppenrichtlinien-Verwaltungskonsole aus vornehmen, wird standardmäßig der Domänencontroller, der als PDC fungiert, verwendet.

Wenn Sie Einstellungen an einem Domänencontroller ändern, bei dem es sich nicht um den dem DirectAccess-Server zugeordneten Domänencontroller (für das Server-Gruppenrichtlinienobjekt) oder um den PDC (Für Client- und Anwendungsserver-Gruppenrichtlinienobjekte) handelt, müssen Sie zusätzlich Folgendes berücksichtigen:

- Stellen Sie vor dem Ändern der Einstellungen sicher, dass der Domänencontroller mit einem aktuellen Gruppenrichtlinienobjekt repliziert wurde, und sichern Sie Ihre Gruppenrichtlinienobjekt-Einstellungen. Weitere Informationen finden Sie unter [Sichern und Wiederherstellen der Remote Zugriffs Konfiguration](#). Falls das Gruppenrichtlinienobjekt nicht aktualisiert wurde, können Zusammenführungskonflikte bei der Replikation auftreten, die zu einer beschädigten Remotezugriffskonfiguration führen können.
- Nach dem Ändern der Einstellungen müssen Sie warten, bis die Änderungen auf den Domänencontrollern repliziert wurden, die den Gruppenrichtlinienobjekten zugeordnet sind. Nehmen Sie keine weiteren Änderungen über die Remotezugriffs-Verwaltungskonsole oder Remotezugriffs-PowerShell-Cmdlets vor, bis die Replikation abgeschlossen ist. Falls ein Gruppenrichtlinienobjekt auf zwei Domänencontrollern bearbeitet wurde, bevor die Replikation abgeschlossen ist, können Zusammenführungskonflikte auftreten, die zu einer beschädigten Remotezugriffskonfiguration führen können.

Alternativ können Sie die Standardeinstellung auch über das Dialogfeld **Domänencontroller ändern** in der Gruppenrichtlinien-Verwaltungskonsole oder über das Windows PowerShell-Cmdlet **Open-NetGPO** ändern, sodass die Änderungen den Domänencontroller verwenden, den Sie angeben.

- Klicken Sie dazu in der Gruppenrichtlinien-Verwaltungskonsole mit der rechten Maustaste auf den Domänen- oder Standortcontainer, und klicken Sie dann auf **Domänencontroller ändern**.
- Für Windows PowerShell geben Sie den Parameter **DomainController** für das Cmdlet **Open-NetGPO** ein. Um zum Beispiel die privaten und öffentlichen Profile in Windows Firewall auf einem Gruppenrichtlinienobjekt namens `domain1\DA_Server_GPO_Europe` über einen Domänencontroller namens `europe-dc.corp.contoso.com` zu aktivieren, geben Sie Folgendes ein:

```
$gpoSession = Open-NetGPO -PolicyStore "domain1\DA_Server_GPO_Europe" -DomainController "europe-dc.corp.contoso.com"
Set-NetFirewallProfile -GpoSession $gpoSession -Name @("Private","Public") -Enabled True
Save-NetGPO -GpoSession $gpoSession
```

#### 1.8.4 Verwalten der Gruppenrichtlinienobjekte für den Remotezugriff mit eingeschränkten Berechtigungen

Um eine Remotezugriffsbereitstellung zu verwalten, benötigt der Remotezugriffsadministrator uneingeschränkte Berechtigungen für die Gruppenrichtlinienobjekte (Lesen, Bearbeiten, Löschen, Ändern der Sicherheit) für die in dieser Bereitstellung verwendeten Gruppenrichtlinienobjekte. Dies liegt daran, dass die Remotezugriffs-Verwaltungskonsole und die PowerShell-Module für den Remotezugriff die Konfiguration von den Remotezugriffs-Gruppenrichtlinienobjekten lesen und darauf schreiben (dies gilt für Client-, Server- und Anwendungsserver-

Gruppenrichtlinienobjekte).

In vielen Organisationen ist der Domänenadministrator, der sich um Gruppenrichtlinienobjekt-Vorgänge kümmert, nicht identisch mit dem Remotezugriffsadministrator, der für die Remotezugriffskonfiguration verantwortlich ist. Diese Organisationen haben möglicherweise Richtlinien, die verhindern, dass der Remotezugriffsadministrator uneingeschränkte Berechtigungen für die Gruppenrichtlinienobjekte in der Domäne hat. Der Domänenadministrator muss möglicherweise auch die Richtlinienkonfiguration überprüfen, bevor diese auf einen Computer in der Domäne angewendet wird.

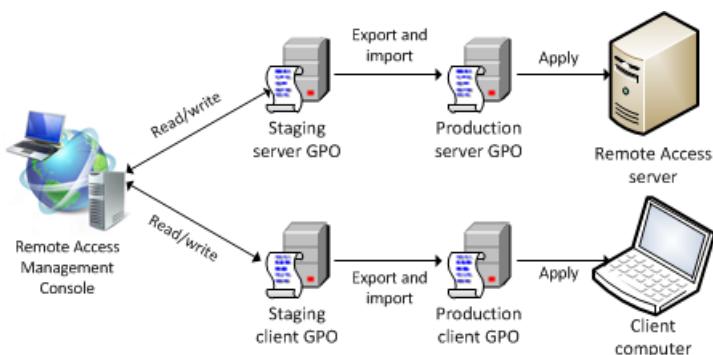
Um diesen Anforderungen zu entsprechen, sollte der Domänenadministrator zwei Kopien jedes Gruppenrichtlinienobjekts erstellen: Bereitstellung und Produktion. Der Remotezugriffsadministrator erhält uneingeschränkte Berechtigungen für die Bereitstellungs-Gruppenrichtlinienobjekte. Der Remotezugriffsadministrator gibt die Bereitstellungs-Gruppenrichtlinienobjekte in der Remotezugriffs-Verwaltungskonsole und in Windows PowerShell-Cmdlets an, welche die Gruppenrichtlinienobjekte für die Remotezugriffsbereitstellung verwendeten. Dadurch kann der Remotezugriffsadministrator die Remotezugriffskonfiguration wie und wann erforderlich lesen und bearbeiten.

Der Domänenadministrator muss sicherstellen, dass die Bereitstellungs-Gruppenrichtlinienobjekte nicht mit einem Verwaltungsbereich in der Domäne verknüpft sind und der Remotezugriffsadministrator keine Gruppenrichtlinienobjekt-Verknüpfungsberechtigungen in der Domäne hat. Dadurch wird sichergestellt, dass Änderungen, die durch den Remotezugriffsadministrator an den Bereitstellungs-Gruppenrichtlinienobjekten vorgenommen wurden, keine Auswirkungen auf die Computer in der Domäne haben.

Der Domänenadministrator verknüpft die Produktions-Gruppenrichtlinienobjekte mit dem erforderlichen Verwaltungsbereich und wendet den entsprechenden Sicherheitsfilter an. Dadurch wird sichergestellt, dass die Änderungen an diesen Gruppenrichtlinienobjekten auf die Computer in der Domäne angewendet werden (Clientcomputer, DirectAccess-Server und Anwendungsserver). Der Remotezugriffsadministrator erhält keine Berechtigungen für die Produktions-Gruppenrichtlinienobjekte.

Wenn Änderungen an den Bereitstellungs-Gruppenrichtlinienobjekten vorgenommen werden, kann der Domänenadministrator die Richtlinienkonfiguration in diesen Gruppenrichtlinienobjekten überprüfen, um sicherzustellen, dass diese die Sicherheitsanforderungen in der Organisation erfüllen. Der Domänenadministrator exportiert dann über die Sicherungsfunktion die Einstellungen von den Bereitstellungs-Gruppenrichtlinienobjekten und importiert die Einstellungen zu den entsprechenden Produktions-Gruppenrichtlinienobjekten, die dann auf die Computer in der Domäne angewendet werden.

Im folgenden Diagramm wird diese Konfiguration gezeigt.



### 1.8.5 Wiederherstellen eines gelöschten Gruppenrichtlinienobjekts

Wenn ein Gruppenrichtlinienobjekt eines Clients, eines DirectAccess-Servers, oder eines Anwendungsservers versehentlich gelöscht wurde und keine Sicherung verfügbar ist, müssen Sie die Konfigurationseinstellungen entfernen und sie neu konfigurieren. Wenn eine Sicherung verfügbar ist, können Sie das Gruppenrichtlinienobjekt aus der Sicherung wiederherstellen.

In der Remote Zugriffs-Verwaltungskonsole wird die folgende Fehlermeldung angezeigt: **GPO (GPO-Name) wurde nicht gefunden**. Führen Sie folgende Schritte aus, um die Konfigurationseinstellungen zu entfernen:

1. Führen Sie das Windows PowerShell-Cmdlet **Uninstall-remoteaccess** aus.
2. Öffnen Sie die Remotezugriffs-Verwaltungskonsole.
3. In der angezeigten Fehlermeldung werden Sie darauf hingewiesen, dass das Gruppenrichtlinienobjekt nicht gefunden werden konnte. Klicken Sie auf **Konfigurationseinstellungen entfernen**. Nach Abschluss des Vorgangs wird der Server in einem nicht konfigurierten Zustand wiederhergestellt.

## Nächste Schritte

- [Schritt 2: Planen von DirectAccess-Bereitstellungen](#)

# Schritt 2 Planen von erweiterten DirectAccess-bereit Stellungen

09.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nach der Planung der DirectAccess-Infrastruktur besteht der nächste Schritt der Bereitstellung des erweiterten DirectAccess auf einem einzelnen Server mit IPv4 und IPv6 darin, die Einstellungen für den Remotezugriffs-Setup-Assistenten vorzunehmen.

AUFGABE	BESCHREIBUNG
<a href="#">2,1 Planen der Client Bereitstellung</a>	Planen Sie die Methode zum Verbinden der Clientcomputer mithilfe von DirectAccess. Entscheiden Sie, welche verwalteten Computer als DirectAccess-Clients konfiguriert werden, und planen Sie die Bereitstellung von NCA (Network Connectivity Assistant) oder DCA (DirectAccess Connectivity Assistant) auf den Clientcomputern.
<a href="#">2,2 Planen der DirectAccess-Server Bereitstellung</a>	Planen Sie die Bereitstellung des DirectAccess-Servers.
<a href="#">2,3 Planen der Infrastruktur Server</a>	Planen Sie die Infrastrukturserver für Ihre DirectAccess-Bereitstellung, dazu gehört der DirectAccess-Netzwerkadressenserver, die DNS-Server (Domain Name System) und die DirectAccess-Verwaltungsserver.
<a href="#">2,4 Planen von Anwendungsservern</a>	Planen Sie die IPv4- und IPv6-Anwendungsserver, und ziehen Sie die optionale Möglichkeit in Betracht, eine obligatorische End-to-End-Authentifizierung zwischen DirectAccess-Clientcomputern und internen Anwendungsservern einzurichten.
<a href="#">2,5 Planen von DirectAccess und VPN-Clients von Drittanbietern</a>	Bei der Bereitstellung von DirectAccess mit VPN-Clients von Drittanbietern kann es erforderlich sein, die folgenden Registrierungswerte festzulegen, um die nahtlose gleichzeitige Verwendung der beiden Remotezugriffslösungen zu aktivieren.

## 2.1 Planen der Clientbereitstellung

Bei der Planung Ihrer Clientbereitstellung müssen drei Entscheidungen getroffen werden:

1. Soll DirectAccess für alle oder nur für mobile Computer verfügbar sein?

Bei der Konfiguration der DirectAccess-Clients im DirectAccess-Client-Setup-Assistenten können Sie auswählen, dass nur mobile Computer in den angegebenen Sicherheitsgruppen eine Verbindung über DirectAccess aufbauen können. Wenn Sie nur den Zugriff für mobile Computer zulassen, konfiguriert der Remotezugriff automatisch einen WMI-Filter, um sicherzustellen, dass das Gruppenrichtlinienobjekt des DirectAccess-Clients nur auf mobile Computer in den angegebenen Sicherheitsgruppen angewendet wird. Der Remotezugriffsadministrator benötigt Sicherheitsberechtigungen zum Erstellen oder Bearbeiten, damit er WMI-Filter für das Gruppenrichtlinienobjekt erstellen oder bearbeiten kann, um diese Einstellung zu aktivieren.

## 2. In welchen Sicherheitsgruppen sollen die DirectAccess-Clientcomputer enthalten sein?

Die DirectAccess-Cienteinstellungen befinden sich in dem Gruppenrichtlinienobjekt des DirectAccess-Clients. Das Gruppenrichtlinienobjekt wird auf Computer angewendet, die in den Sicherheitsgruppen enthalten sind, die Sie in dem DirectAccess-Client-Setup-Assistenten angegeben haben. Sie können angeben, dass Sicherheitsgruppen in einer beliebigen unterstützten Domäne enthalten sein sollen. Weitere Informationen finden Sie im Abschnitt [1.7 Plan Active Directory Domain Services](#).

Bevor Sie DirectAccess konfigurieren, sollten Sie die Sicherheitsgruppen erstellen. Nach Abschluss der DirectAccess-Bereitstellung können Sie Computer zur Sicherheitsgruppe hinzufügen, wenn Sie jedoch Clientcomputer hinzufügen, die sich in einer anderen Domäne befinden wie die Sicherheitsgruppe, dann wird das Client-Gruppenrichtlinienobjekt nicht auf diese Clients angewendet. Wenn Sie beispielsweise SG1 in Domäne A für DirectAccess-Clients erstellen und später Clients von Domäne B zu dieser Gruppe hinzufügen, wird das Client-Gruppenrichtlinienobjekt nicht auf Clients von Domäne B angewendet. Sie können dieses Problem vermeiden, indem Sie eine neue Client-Sicherheitsgruppe für jede Domäne erstellen, die die DirectAccess-Clientcomputer enthält. Alternativ dazu können Sie auch das Windwows PowerShell-Cmdlet **Add-DAClient** mit dem Namen des neuen Gruppenrichtlinienobjekts für die neue Domäne ausführen, wenn Sie keine neue Sicherheitsgruppe erstellen möchten.

## 3. Welche Einstellungen müssen für den Netzwerkkonkennitivitäts-Assistenten konfiguriert werden?

Der Netzwerkkonkennitivitäts-Assistent wird auf Clientcomputern ausgeführt, er stellt zusätzliche Informationen zur DirectAccess-Verbindung mit Endbenutzern bereit. Im DirectAccess-Client-Setup-Assistenten können Sie Folgendes konfigurieren:

- **Konnektivitätsverifier**

Ein Standardwebtest wird erstellt, den Clients verwenden, um die Verbindung zum internen Netzwerk zu prüfen. Der Standardname lautet:

`https://directaccess-WebProbeHost.<domain_name>`

Der Name sollte manuell im DNS registriert werden. Mithilfe anderer Webadressen über HTTP oder **ping** können Sie weitere Verbindungsprüfer erstellen. Für jeden Verbindungsprüfer muss ein DNS-Eintrag vorhanden sein.

- **Eine Helpdesk-e-Mail-Adresse**

Wenn Endbenutzer Probleme mit der DirectAccess-Verbindung haben, können Sie eine E-Mail mit Diagnoseinformationen an den DirectAccess-Administrator senden, um das Problem zu beheben.

- **Ein DirectAccess-Verbindungs Name**

Geben Sie einen DirectAccess-Verbindungsnamen an, damit Endbenutzer die DirectAccess-Verbindung auf ihren Computern leichter identifizieren können.

- **DirectAccess-Clients die Verwendung der lokalen Namensauflösung gestatten**

Clients benötigen eine Methode, um Namen lokal aufzulösen. Wenn Sie zulassen, dass DirectAccess-Clients die lokale Namensauflösung verwenden, können Endbenutzer zum Auflösen von Namen lokale DNS-Server verwenden. Wenn Endbenutzer die Verwendung lokaler DNS-Server zur Namensauflösung auswählen, sendet DirectAccess keine Anforderungen zum Auflösen einzelner Bezeichnungsnamen an den internen Unternehmens-DNS-Server. Stattdessen verwendet er die lokale Namensauflösung, indem er die Multicastnamensauflösung für lokale Verbindungen (Link-Local Multicast Name Resolution, LLNMR) und NetBIOS über TCP/IP-Protokolle verwendet.

## 2.2 Planen der DirectAcess-Serverbereitstellung

Berücksichtigen Sie folgende Entscheidungen bei der Bereitstellung Ihres DirectAccess-Servers:

- **Netzwerktopologie**

Bei der Bereitstellung eines DirectAccess-Servers sind mehrere Topologien verfügbar:

- **Zwei Netzwerkadapter.** Mit zwei Netzwerkadapters kann DirectAccess so konfiguriert werden, dass ein Netzwerkadapter direkt mit dem Internet und der andere mit dem internen Netzwerk verbunden ist. Alternativ kann der Server hinter einem Edgegerät installiert werden, wie z. B. einer Firewall oder einem Router. In dieser Konfiguration ist ein Netzwerkadapter direkt mit dem Umkreisnetzwerk und der andere mit dem internen Netzwerk verbunden.
- **Ein Netzwerkadapter.** In dieser Konfiguration ist der Server hinter einem Edgegerät wie z. B. einer Firewall oder einem Router installiert. Der Netzwerkadapter ist mit dem internen Netzwerk verbunden.

Weitere Informationen zum Auswählen der Topologie für Ihre Bereitstellung finden Sie unter [1,1 Planen der Netzwerktopologie und-Einstellungen](#).

- **ConnectTo-Adresse**

Clientcomputer verwenden die ConnectTo-Adresse, um eine Verbindung zum DirectAccess-Server herzustellen. Die von Ihnen gewählte Adresse muss mit dem Antragstellernamen des IP-HTTPS-Zertifikats übereinstimmen, das Sie für die IP-HTTPS-Verbindung bereitstellen. Außerdem muss sie im öffentlichen DNS verfügbar sein.

- **Leistungsverlauf für Netzwerkadapter**

Der Setup-Assistent für den Remotezugriffsserver erkennt automatisch die Netzwerkadapter, die auf dem DirectAccess-Server konfiguriert sind. Vergewissern Sie sich, dass die richtigen Adapter ausgewählt sind.

- **IP-HTTPS-Zertifikat**

Der Setup-Assistent für den Remotezugriffsserver erkennt automatisch ein Zertifikat, das für die IP-HTTPS-Verbindung geeignet ist. Der Antragstellername von Ihnen gewählten Zertifikats muss mit der ConnectTo-Adresse übereinstimmen. Wenn Sie selbstsignierte Zertifikate verwenden, können Sie die Verwendung eines Zertifikats auswählen, das automatisch vom Remotezugriffsserver erstellt wird.

- **IPv6-Präfixe**

Wenn der Setup-Assistent für den Remotezugriffsserver erkennt, dass IPv6 auf den Netzwerkadapters bereitgestellt wurde, füllt er automatisch IPv6-Präfixe für das interne Netzwerk auf. Ein IPv6-Präfix zum Zuweisen für die DirectAccess-Clientcomputer und ein IPv6-Präfix zum Zuweisen für die VPN-Clientcomputer. Wenn die automatisch generierten Präfixe nicht mit Ihrer systemeigenen IPv6-Infrastruktur übereinstimmen, müssen Sie sie manuell ändern. Weitere Informationen finden Sie unter [1,1 Planen der Netzwerktopologie und-Einstellungen](#).

- **Authentifizierung**

Entscheiden Sie, wie DirectAccess-Clients sich mit dem DirectAccess-Server authentifizieren sollen:

- **Benutzauthentifizierung.** Sie können für Benutzer die zweistufige oder die Authentifizierung mit Active Directory-Anmeldeinformationen aktivieren. Weitere Informationen zum Authentifizieren mit zweistufiger Authentifizierung finden Sie unter Bereitstellen des [Remote Zugriffs mit OTP-Authentifizierung](#).
- **Computerauthentifizierung.** Sie können die Computerauthentifizierung so konfigurieren, dass sie im Auftrag des Clients Zertifikate oder den DirectAccess-Server als Kerberos-Proxy verwendet. Weitere Informationen finden Sie unter [1,3 Planen der Zertifikat Anforderungen](#).

- **Windows 7-Clients.** Standardmäßig können Client Computer, auf denen Windows 7 ausgeführt wird, keine Verbindung mit einer DirectAccess-Bereitstellung von Windows Server 2012 R2 oder Windows Server 2012 herstellen. Wenn Sie über Clients in Ihrer Organisation verfügen, auf denen Windows 7 ausgeführt wird, und Sie den Remote Zugriff auf interne Ressourcen benötigen, können Sie eine Verbindung herstellen. Clientcomputer, die auf interne Ressourcen zugreifen sollen, müssen Mitglied einer Sicherheitsgruppe sein, die Sie im DirectAccess-Client-Setup-Assistenten angeben.

**NOTE**

Wenn Sie zulassen, dass Clients, auf denen Windows 7 ausgeführt wird, eine Verbindung mithilfe von DirectAccess herstellen, muss die Computer Zertifikat Authentifizierung

- **VPN-Konfiguration**

Entscheiden Sie, ob ein VPN-Zugriff auf nicht DirectAccess-fähige Remoteclients bereitgestellt werden soll, bevor Sie DirectAccess konfigurieren. Sie sollten einen VPN-Zugriff bereitstellen, wenn Sie in Ihrer Organisation über Clientcomputer verfügen, die die DirectAccess-Konnektivität nicht unterstützen (da sie nicht verwaltet werden oder ein Betriebssystem einsetzen, bei dem DirectAccess nicht unterstützt wird). Mit dem Setup-Assistent für den Remotezugriffsserver können Sie konfigurieren, wie IP-Adressen zugewiesen werden (über DHCP oder einen Pool statischer Adressen) und wie VPN-Clients authentifiziert werden - mithilfe des Active Directory oder eines RADIUS-Servers (Remote Authentication Dial-Up Service).

## 2.3 Planen der Infrastrukturserver

Für DirectAccess sind drei Typen von Infrastrukturservern erforderlich:

- **DNS-Server.** Weitere Informationen finden Sie im Abschnitt [1.4 Planen von DNS-Anforderungen](#).
- **Netzwerkadressenserver.** Weitere Informationen finden Sie unter [1.5 Planen des Netzwerkadressenservers](#).
- **Verwaltungsserver.** Weitere Informationen finden Sie unter [1.6 Planen von Verwaltungsservern](#).

## 2.4 Planen der Anwendungsserver

Anwendungsserver sind Server im Unternehmensnetzwerk, die von Clientcomputern über eine DirectAccess-Verbindung zugänglich sind. Anwendungsserver werden identifiziert, indem Sie in einer Sicherheitsgruppe hinzugefügt werden. Das Gruppenrichtlinienobjekt des Anwendungsservers wird dann auf die Server in der Gruppe angewendet.

**NOTE**

Das Hinzufügen von Anwendungsservern zu einer Sicherheitsgruppe ist nur erforderlich, wenn Sie eine End-to-End-Authentifizierung und -Verschlüsselung benötigen.

Optional können Sie auch die End-to-End-Authentifizierung und -Verschlüsselung zwischen DirectAccess-Client und ausgewählten internen Anwendungsservern voraussetzen. Wenn Sie die End-to-End-Authentifizierung konfigurieren, verwenden DirectAccess-Clients eine IPsec-Transportrichtlinie. Bei der Verwendung dieser Richtlinie muss die Authentifizierung und der Schutz der IPsec-Sitzungen auf den angegebenen Anwendungsservern beendet werden. In diesem Fall leitet der Remotezugriffsserver die authentifizierten und geschützten IPsec-Sitzungen an die Anwendungsserver weiter.

Standardmäßig wird bei der Erweiterung der Authentifizierung auf Anwendungsserver die Datennutzlast zwischen DirectAccess-Client und Anwendungsserver verschlüsselt. Sie können auch auswählen, den Datenverkehr nicht zu

verschlüsseln und nur die Authentifizierung verwenden. Dies ist jedoch weniger sicher als die Verwendung der Authentifizierung und-Verschlüsselung und wird nur für Anwendungsserver unterstützt, auf denen die Betriebssysteme Windows Server 2008 R2 oder Windows Server 2012 ausgeführt werden.

## 2.5 Planen von DirectAccess und VPN-Clients von Drittanbietern

Einige VPN-Clients von Drittanbietern erstellen im Ordner Netzwerkverbindungen keine Verbindungen. Dies kann dazu führen, dass DirectAccess keine Intranetkonnektivität erkennt, wenn die VPN-Verbindung hergestellt ist und eine Verbindung zum Intranet besteht. Diese Bedingung tritt auf, wenn VPN-Clients von Drittanbietern ihre Schnittstellen registrieren, indem sie diese als (NDIS) ENDPOINT-Typen (Network Device Interface Specification) definieren. Sie können die gleichzeitige Verwendung dieser VPN-Clienttypen aktivieren, indem Sie den folgenden Registrierungswert auf 1 festlegen.

HKEY\_LOCAL\_MACHINE

\system\currentcontrolset\services\nlasvc\parameters\showdomainendpointinterfaces  
(REG\_DWORD)

Einige VPN-Clients von Drittanbietern verwenden eine Konfiguration mit geteiltem Tunneln, sodass der VPN-Clientcomputer direkt auf das Internet zugreifen kann, ohne den Datenverkehr über die VPN-Verbindung an das Intranet senden zu müssen.

Bei Konfigurationen mit geteiltem Tunneln wird die Standardgateweyeinstellung für den VPN-Client in der Regel als nicht konfiguriert oder als nur Nullen (0.0.0.0) belassen. Sie können dieses Verhalten prüfen, indem Sie eine erfolgreiche VPN-Verbindung zum Intranet herstellen und das Ipconfig.exe-Befehlszeilentool verwenden, um die entsprechende Konfiguration anzuzeigen.

Wenn die VPN-Verbindung das Standardgateway als leer oder nur Nullen (0.0.0.0) anzeigt, ist Ihr VPN-Client entsprechend konfiguriert. Standardmäßig erkennt der DirectAccess-Client geteilte Tunnelkonfigurationen nicht. Um DirectAccess-Clients für eine Erkennung dieser VPN-Clientkonfigurationstypen zu konfigurieren, müssen Sie den folgenden Registrierungswert auf 1 festlegen.

HKEY\_LOCAL\_MACHINE \system\currentcontrolset\services\nlasvc\parameters\internet\  
enablengatewaylocationerkennungs (REG\_DWORD)

## Vorheriger Schritt

- [Schritt 1: Planen der DirectAccess-Infrastruktur](#)

# Installieren und Konfigurieren von DirectAccess (erweitert)

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In dieser Übersicht werden die Konfigurationsschritte aufgeführt, die zum Bereitstellen eines einzelnen DirectAccess-Servers mit Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 mit IPv4 und IPv6 ausgeführt werden müssen.

- [Schritt 1: Konfigurieren der erweiterten DirectAccess-Infrastruktur.](#)

In dieser Phase konfigurieren Sie die Netzwerk- und Servereinstellungen, Zertifikatanforderungen, DNS-Einstellungen (Domain Name System), die Bereitstellung des Netzwerkadressenservers, DirectAccess-Verwaltungsserver, Active Directory-Einstellungen und Gruppenrichtlinienobjekte.

- [Schritt 2: Konfigurieren Sie erweiterte DirectAccess-Server.](#)

In dieser Phase konfigurieren Sie die DirectAccess-Clientcomputer, Servereinstellungen, Infrastrukturserver und Anwendungsserver.

- [Schritt 3: Überprüfen Sie die erweiterte DirectAccess-Bereitstellung.](#)

Dieser Schritt beschreibt die Überprüfung der Bereitstellung.

Bevor Sie mit der Bereitstellung beginnen, müssen Sie die in [Planen einer erweiterten DirectAccess-Bereitstellung](#) erläuterten Planungsschritte prüfen.

# Schritt 1 Konfigurieren der erweiterten DirectAccess-Infrastruktur

09.04.2020 • 47 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2012 R2, Windows Server 2012

In diesem Thema wird die Konfiguration der Infrastruktur beschrieben, die für eine Bereitstellung des erweiterten Remotezugriffs erforderlich ist, die einen einzelnen DirectAccess-Server in einer gemischten IPv4- und IPv6-Umgebung verwendet. Bevor Sie mit den Bereitstellungs Schritten beginnen, stellen Sie sicher, dass Sie die in [Planen einer erweiterten DirectAccess-Bereitstellung](#) beschriebenen Planungsschritte abgeschlossen haben.

AUFGABE	BESCHREIBUNG
1.1 Konfigurieren der Servernetzwerkeinstellungen	Konfigurieren Sie die Servernetzwerkeinstellungen auf dem DirectAccess-Server.
1.2 Konfigurieren des Erzwingens von Tunneln	Konfigurieren Sie das Erzwingen von Tunneln.
1.3 Konfigurieren des Routings im Unternehmensnetzwerk	Konfigurieren Sie das Routing im Unternehmensnetzwerk.
1.4 Konfigurieren der Firewalls	Konfigurieren Sie bei Bedarf zusätzliche Firewalls.
1.5 Konfigurieren von Zertifizierungsstellen und Zertifikaten	Konfigurieren Sie bei Bedarf eine Zertifizierungsstelle und weitere für die Bereitstellung erforderliche Zertifikatsvorlagen.
1.6 Konfigurieren des DNS-Servers	Konfigurieren Sie die DNS-Einstellungen für den DirectAccess-Server.
1.7 Konfigurieren des Active Directory	Fügen Sie der Active Directory-Domäne Clientcomputer und DirectAccess-Server hinzu.
1.8 Konfigurieren der Gruppenrichtlinienobjekte	Konfigurieren Sie bei Bedarf Gruppenrichtlinienobjekte für die Bereitstellung.
1.9 Konfigurieren von Sicherheitsgruppen	Konfigurieren Sie Sicherheitsgruppen, die DirectAccess-Clientcomputer und weitere Sicherheitsgruppen enthalten, die für die Bereitstellung erforderlich sind.
1.10 Konfigurieren des Netzwerkadressenservers	Konfigurieren Sie den Netzwerkadressenserver, dazu gehört auch die Installation des Netzwerkadressenserver-Websitezertifikats.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## 1.1 Konfigurieren von Servernetzwerk Einstellungen

Für eine einzelne Serverbereitstellung in einer Umgebung mit IPv4 und IPv6 sind folgende Netzwerkschnittstelleneinstellungen erforderlich. Sämtliche IP-Adressen können im **Netzwerk- und Freigabecenter** von Windows mit der Option **Adapttereinstellungen ändern** konfiguriert werden.

### Edge-Topologie

- Zwei aufeinander folgende, öffentliche, statische IPv4- oder IPv6-Adressen mit Internetzugriff.

#### NOTE

Für Teredo sind zwei öffentliche Adressen erforderlich. Falls Sie Teredo nicht verwenden, können Sie eine einzelne, öffentliche, statische IPv4-Adresse konfigurieren.

- Eine einzelne, interne, statische IPv4- oder IPv6-Adresse

### Hinter einem NAT-Gerät (mit zwei Netzwerkadapters)

- Eine einzelne, interne, statische IPv4- oder IPv6-Adresse mit Internetzugriff
- Eine einzelne, interne, statische IPv4- oder IPv6-Adresse mit Netzwerkzugriff

### Hinter einem NAT-Gerät (mit einem Netzwerkadapter)

- Eine einzelne, interne, statische IPv4- oder IPv6-Adresse mit Netzwerkzugriff

#### NOTE

Wenn ein DirectAccess-Server mit zwei oder mehr Netzwerkadapters (davon einer im Domänenprofil und einer in einem öffentlichen oder privaten Profil klassifiziert) mit einer einzelnen NetzwerkadAPTERtopologie konfiguriert ist, wird Folgendes empfohlen:

- Vergewissern Sie sich, dass der zweite Netzwerkadapter und zusätzliche Netzwerkadapter im Domänenprofil klassifiziert sind.
- Wenn der zweite Netzwerkadapter nicht für das Domänen Profil konfiguriert werden kann, muss die DirectAccess IPSec-Richtlinie mithilfe des folgenden Windows PowerShell-Befehls manuell auf alle Profile festgelegt werden, nachdem DirectAccess konfiguriert wurde:

```
$gposession = Open-NetGPO "PolicyStore <Name of the server GPO>
Set-NetIPsecRule "DisplayName <Name of the IPsec policy> "GPOSession $gposession "Profile Any
Save-NetGPO "GPOSession $gposession
```

## 1,2 Konfigurieren der Tunnel Erzwingung

Das Erzwingen von Tunnels kann mithilfe des Remotezugriffs-Setup-Assistenten konfiguriert werden. Diese Option wird im Remoteclient-Konfigurationsassistenten als Kontrollkästchen angezeigt. Diese Einstellung hat nur Auswirkungen auf DirectAccess-Clients. Wenn VPN aktiviert ist, verwenden VPN-Clients standardmäßig das Erzwingen von Tunnels. Administratoren können die Einstellung für VPN-Clients über das Clientprofil ändern.

Durch Aktivierung des Kontrollkästchens zum Erzwingen von Tunneln wird Folgendes bewirkt:

- Aktivieren des Erzwingens von Tunnels für DirectAccess-Clients
- Hinzufügen eines **Any**-Eintrags in der Richtlinientabelle für die Namensauflösung für DirectAccess-Clients, dadurch wird der gesamte DNS-Datenverkehr an die internen Netzwerk-DNS-Server geleitet
- Konfigurieren Sie die DirectAccess-Clients so, dass sie immer die IP-HTTPS-Übergangstechnologie verwenden

Um Internetressourcen für DirectAccess-Clients verfügbar zu machen, die das Erzwingen von Tunnels verwenden, können Sie einen Proxyserver verwenden, der IPv6-basierte Anforderungen für Internetressourcen empfangen kann und sie in Anforderungen für IPv4-basierte Internetressourcen übersetzt. Zum Konfigurieren eines Proxyservers für Internetressourcen müssen Sie den Standardeintrag in der Richtlinientabelle für die Namensauflösung ändern, um den Proxyserver hinzuzufügen. Verwenden Sie dazu die PowerShell-Cmdlets für den Remotezugriff oder die DNS-PowerShell-Cmdlets. Verwenden Sie beispielsweise das PowerShell-Cmdlet für den Remotezugriff wie folgt:

```
Set-DAClientDNSConfiguration "DNSSuffix "." "ProxyServer <Name of the proxy server:port>
```

#### **NOTE**

Wenn DirectAccess und VPN auf dem gleichen Server aktiviert sind, das VPN sich im Modus zum Erzwingen von Tunnels befindet und der Server in einer Edgetopologie oder einer Topologie hinter einem NAT (mit zwei Netzwerkadaptersn, einer ist mit der Domäne und der andere mit einem privaten Netzwerk verbunden) bereitgestellt wird, kann der VPN-Internetdatenverkehr nicht über die externe Schnittstelle des DirectAccess-Servers weitergeleitet werden. Um dieses Szenario zu ermöglichen, muss der Remotezugriff auf dem Server hinter einer Firewall in einer einzelnen Netzwerkadaptertopologie bereitgestellt werden. Alternativ dazu können Organisationen einen separaten Proxyserver in dem internen Netzwerk verwenden, um den Internetdatenverkehr von den VPN-Clients weiterzuleiten.

#### **NOTE**

Wenn eine Organisation für das Zugreifen auf Internetressourcen einen Webproxy für DirectAccess-Clients verwendet und der Unternehmensproxy nicht fähig ist, interne Netzwerkressourcen zu verarbeiten, können die DirectAccess-Clients nicht auf die internen Ressourcen zugreifen, wenn sie sich außerhalb des Intranets befinden. In solch einem Szenario müssen Sie in der Richtlinientabelle für die Namensauflösung manuell Einträge für die internen Netzwerksuffixe erstellen, indem Sie die DNS-Seite des Infrastruktur-Assistenten verwenden, damit DirectAccess-Clients auf die internen Ressourcen zugreifen können. Wenden Sie auf die Suffixe in der Richtlinientabelle für die Namensauflösung keine Proxeinstellungen an. Die Suffixe sollten mit DNS-Server-Standardeinträgen aufgefüllt werden.

## 1.3 Konfigurieren des Routings im Unternehmensnetzwerk

Konfigurieren Sie das Routing im Unternehmensnetzwerk wie folgt:

- Wenn in der Organisation eine systemeigene IPv6-Adresse bereitgestellt wird, fügen Sie ihr eine Route hinzu, damit die Router im internen Netzwerk den IPv6-Datenverkehr zurück über den DirectAccess-Server leiten.
- Konfigurieren Sie die IPv4-und IPv6-Routen der Organisation manuell auf den DirectAccess-Servern. Fügen Sie eine öffentliche Route hinzu, sodass der gesamte Datenverkehr mit Organisations-IPv6-Präfix (/48) an das interne Netzwerk weitergeleitet wird. Fügen Sie für IPv4-Datenverkehr explizite Routen hinzu, damit IPv4-Datenverkehr an das interne Netzwerk weitergeleitet wird.

## 1.4 Konfigurieren von Firewalls

Wenden Sie bei zusätzlichen Firewalls in der Bereitstellung die folgenden Firewallausnahmen mit Internetzugriff für Remotezugriff-Datenverkehr an, wenn der DirectAccess-Server sich im IPv4-Internet befindet:

- Teredo-Datenverkehr "UDP-Zielport 3544 (User Datagram Protocol) eingehend und UDP-Quellport 3544 ausgehend.
- IPv6-zu-IPv4-Datenverkehr "IP-Protokoll 41 eingehend und ausgehend.
- IP-HTTPS "TCP (Transmission Control Protocol)-Zielport 443 und TCP-Quellport 443 ausgehend. Wenn der

DirectAccess-Server nur einen Netzwerkadapter hat und der Netzwerkadressenserver sich auf dem DirectAccess-Server befindet, wird auch TCP-Port 62000 benötigt.

**NOTE**

Diese Ausnahme muss auf dem DirectAccess-Server konfiguriert werden, während alle anderen Ausnahmen auf der Edge-Firewall konfiguriert werden müssen.

**NOTE**

Bei Teredo- und IP6-zu-IP4-Datenverkehr sollten diese Ausnahmen für beide aufeinander folgenden öffentlichen IPv4-Adressen mit Internetzugriff auf dem DirectAccess-Server angewendet werden. Bei IP-HTTPS müssen die Ausnahmen nur auf die Adresse angewendet werden, die zur Auflösung des öffentlichen Namens des Servers dient.

Wenden Sie bei zusätzlichen Firewalls die folgenden Firewallausnahmen mit Internetzugriff für Remotezugriff-Datenverkehr an, wenn der DirectAccess-Server sich im IPv6-Internet befindet:

- IP-Protokoll 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend.
- Internet Control Message Protocol für IPv6 (ICMPv6) eingehender und ausgehender Datenverkehr (nur für Teredo-Implementierungen).

Wenden Sie bei zusätzlichen Firewalls die folgenden internen Netzwerkfirewallausnahmen für RAS-Datenverkehr an:

- ISATAP "Protokoll 41 eingehend und ausgehend
- TCP/UDP für den gesamten IPv4/IPv6-Datenverkehr
- ICMP für den gesamten IPv4/IPv6-Datenverkehr

## 1,5 Konfigurieren von Zertifizierungsstellen und Zertifikaten

Der Remote Zugriff in Windows Server 2012 ermöglicht Ihnen die Auswahl zwischen der Verwendung von Zertifikaten für die Computer Authentifizierung oder der Verwendung eines integrierten Kerberos-Proxys, der mithilfe von Benutzernamen und Kenn Wörtern authentifiziert wird. Außerdem müssen Sie ein IP-HTTPS-Zertifikat auf dem DirectAccess-Server konfigurieren.

Weitere Informationen finden Sie unter [Active Directory Certificate Services](#).

### 1.5.1 Konfigurieren der IPsec-Authentifizierung

Auf dem DirectAccess-Server und allen DirectAccess-Clients, die die IPsec-Authentifizierung verwenden sollen, ist ein Computerzertifikat erforderlich. Das Zertifikat muss von einer internen Zertifizierungsstelle ausgestellt werden, und DirectAccess-Server und -Clients müssen der Zertifikatskette vertrauen, die die Stamm- und Zwischenzertifikate ausstellen.

So konfigurieren Sie die IPsec-Authentifizierung

1. Entscheiden Sie in der internen Zertifizierungsstelle, ob Sie die Zertifikat Vorlage des Computers verwenden möchten, oder wenn Sie eine neue Zertifikat Vorlage erstellen möchten, wie unter [Erstellen von Zertifikat Vorlagen](#)beschrieben.

#### **NOTE**

Wenn Sie eine neue Vorlage erstellen, muss sie für die Client-Authentifizierung konfiguriert werden.

2. Stellen Sie die Zertifikatvorlage bei Bedarf bereit. Weitere Informationen finden Sie unter Bereitstellen von [Zertifikat Vorlagen](#).
3. Konfigurieren Sie die Zertifikatvorlage bei Bedarf für die automatische Registrierung. Weitere Informationen finden Sie unter [Konfigurieren](#) der automatischen Zertifikat Registrierung.

### **1.5.2 Konfigurieren von Zertifikat Vorlagen**

Wenn Sie zur Ausstellung von Zertifikaten eine interne Zertifizierungsstelle verwenden, müssen Sie für das IP-HTTPS-Zertifikat und das Netzwerkadressenserver-Websitezertifikat eine Zertifikatvorlage konfigurieren.

So konfigurieren Sie eine Zertifikatvorlage

1. Erstellen Sie in der internen Zertifizierungsstelle eine Zertifikat Vorlage, wie unter [Erstellen von Zertifikat Vorlagen](#) beschrieben.
2. Stellen Sie die Zertifikatvorlage wie unter [Deploying Certificate Templates](#) beschrieben bereit.

### **1.5.3 Konfigurieren des IP-HTTPS-Zertifikats**

Für den Remotezugriff ist zum Authentifizieren von IP-HTTPS-Verbindungen mit dem DirectAccess-Server ein IP-HTTPS-Zertifikat erforderlich. Für die IP-HTTPS-Authentifizierung sind drei Zertifikatoptionen verfügbar:

#### **Öffentliches Zertifikat**

Ein öffentliches Zertifikat wird durch einen Drittanbieter bereitgestellt. Wenn der Antragstellername des Zertifikats keine Platzhalterzeichen enthält, muss er die URL des extern auflösbaren vollqualifizierten Domänenamens (FQDN) sein, die nur für IP-HTTPS-Verbindungen zum DirectAccess-Server verwendet wird.

#### **Privates Zertifikat**

Wenn Sie ein privates Zertifikat verwenden, sind folgende Elemente erforderlich, falls sie noch nicht vorhanden sind:

- Ein Websitezertifikat für die IP-HTTPS-Authentifizierung. Beim Zertifikatantragsteller sollte es sich um einen extern auflösbaren FQDN handeln, der über das Internet erreichbar ist. Das Zertifikat basiert auf der Zertifikat Vorlage, die Sie anhand der Anweisungen in 1.5.2 Konfigurieren von Zertifikat Vorlagen erstellt haben.
- Ein Zertifikatsperllisten-Verteilungspunkt, der über einen öffentlich auflösbaren FQDN erreichbar ist.

#### **Selbst signiertes Zertifikat**

Wenn Sie ein selbstsigniertes Zertifikat verwenden, sind folgende Elemente erforderlich, falls sie noch nicht vorhanden sind:

- Ein Websitezertifikat für die IP-HTTPS-Authentifizierung. Beim Zertifikatantragsteller sollte es sich um einen extern auflösbaren FQDN handeln, der über das Internet erreichbar ist.
- Ein Zertifikatsperllisten-Verteilungspunkt, der über einen öffentlich auflösbaren FQDN erreichbar ist.

#### **NOTE**

Selbstsignierte Zertifikate können nicht in Bereitstellungen für mehrere Standorte verwendet werden.

Stellen Sie sicher, dass das für die IP-HTTPS-Authentifizierung verwendete Websitezertifikat die folgenden Anforderungen erfüllt:

- Der allgemeine Name des Zertifikats sollte dem Namen der IP-HTTPS-Website entsprechen.
- Geben Sie im Feld **Betreff** den voll qualifizierten Namen für die IP-HTTPS-URL an.
- Geben Sie im Feld **Erweiterte Schlüsselverwendung** die Serverauthentifizierungs-Objektkennung (OID) an.
- Geben Sie im Feld **Sperrlisten-Verteilungspunkte** einen Zertifikatsperrlisten-Verteilungspunkt an, auf den mit dem Internet verbundene DirectAccess-Clients zugreifen können.
- Das IP-HTTPS-Zertifikat muss einen privaten Schlüssel enthalten.
- Das IP-HTTPS-Zertifikat muss direkt in den persönlichen Speicher importiert werden.
- Die Namen von IP-HTTPS-Zertifikaten können Platzhalter enthalten.

**So installieren Sie das IP-HTTPS-Zertifikat von einer internen Zertifizierungsstelle**

1. Auf dem DirectAccess-Server: Geben Sie auf dem **Start** BildschirmMMC. exeein, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-ins hinzufügen oder entfernen** auf **Zertifikate, Hinzufügen, Computerkonto, Weiter, Lokaler Computer, Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
6. Klicken Sie zweimal auf **Weiter**.
7. Aktivieren Sie auf der Seite **Zertifikate anfordern** das Kontrollkästchen für die zuvor erstellte Zertifikat Vorlage (Weitere Informationen finden Sie unter 1.5.2 Konfigurieren von Zertifikat Vorlagen). Klicken Sie bei Bedarf auf **Es werden zusätzliche Informationen für diese Zertifikatsregistrierung benötigt**.
8. Klicken Sie im Dialogfeld **Zertifikateigenschaften** auf der Registerkarte **Antragsteller** im Bereich **Antragstellename** unter **Typ** auf **Allgemeiner Name**.
9. Geben Sie im Feld **Wert** die IPv4-Adresse des externen Adapters des DirectAccess-Servers oder die FQDN der IP-HTTPS-URL an und klicken Sie anschließend auf **Hinzufügen**.
10. Wählen Sie unter **Alternativer Name** für **Typ** die Option **DNS** aus.
11. Geben Sie im Feld **Wert** die IPv4-Adresse des externen Adapters des DirectAccess-Servers oder die FQDN der IP-HTTPS-URL an und klicken Sie anschließend auf **Hinzufügen**.
12. Auf der Registerkarte **Allgemein** unter **Anzeigename** können Sie einen Namen für das Zertifikat eingeben, sodass Sie es schneller identifizieren können.
13. Klicken Sie auf der Registerkarte **Erweiterungen** auf den Pfeil neben dem Feld **Erweiterte Schlüsselverwendung** und vergewissern Sie sich, dass in der Liste **Ausgewählte Optionen Serverauthentifizierung** angezeigt wird.
14. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
15. Überprüfen Sie im Detailbereich des Zertifikat-Snap-Ins, dass das neue Zertifikat mit der Option **Beabsichtigte Zwecke** registriert wurde.

# 1,6 Konfigurieren des DNS-Servers

Sie müssen einen DNS-Eintrag für die Netzwerkadressenserver-Website für das interne Netzwerk in Ihrer Bereitstellung manuell konfigurieren.

## So erstellen Sie den Netzwerkadressen Server

1. Auf dem internen Netzwerk-DNS-Server: Geben Sie auf dem **Start Bildschirm dnsmgmt. mscein**, und drücken Sie dann die EINGABETASTE.
2. Erweitern Sie im linken Bereich der **DNS-Manager**-Konsole die Forward-Lookupzone für Ihre Domäne. Klicken Sie mit der rechten Maustaste auf die Domäne, und anschließend auf **Neuer Host (A oder AAAA)**.
3. Gehen Sie im Dialogfeld **Neuer Host** im Feld **IP-Adresse** wie folgt vor:
  - Geben Sie in das Feld **Name (bei Nichtangabe wird übergeordnete Domäne verwendet)** den DNS-Namen für die Netzwerkadressenserver-Website (mit diesem Namen verbinden sich die DirectAccess-Clients mit dem Netzwerkadressenserver) ein.
  - Geben Sie die IPv4- oder IPv6-Adresse des Netzwerkadressenservers ein, klicken Sie dann auf **Host hinzufügen** und anschließend auf **OK**.
4. Vorgehensweise im Dialogfeld **Neuer Host**:
  - Geben Sie in das Feld **Name (bei Nichtangabe wird übergeordnete Domäne verwendet)** den DNS-Namen des Webtests ein (der Name für Standard-Webtests lautet **directaccess-webprobehost**).
  - Geben Sie in das Feld **IP-Adresse** die IPv4- oder IPv6-Adresse des Webtests ein und klicken Sie dann auf **Host hinzufügen**.
  - Wiederholen Sie diesen Vorgang für **directaccess-corpconnectivityhost** und manuell erstellte Verbindungsprüfer.
5. Klicken Sie im Dialogfeld **DNS** auf **OK** und dann auf **Fertig**.

## Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address  
<network_location_server_IPv4_address>  
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address  
<network_location_server_IPv6_address>
```

Außerdem müssen Sie die DNS-Einträge für folgende Elemente konfigurieren:

- **Der IP-HTTPS-Server**

DirectAccess-Clients müssen in der Lage sein, den DNS-Namen des DirectAccess-Servers aus dem Internet aufzulösen.

- **CRL-Sperr Überprüfung**

DirectAccess verwendet Zertifikatsperrüberprüfungen für die IP-HTTPS-Verbindung zwischen den DirectAccess-Clients und dem DirectAccess-Server und für die HTTPS-basierte Verbindung zwischen dem DirectAccess-Client und dem Netzwerkadressenserver. In beiden Fällen müssen DirectAccess-Clients in der Lage sein, auf den Zertifikatsperrlisten-Verteilungspunkt zuzugreifen und ihn aufzulösen.

- ISATAP

Intrasite Automatic Tunnel Addressing Protocol (ISATAP) verwendet Tunnel, damit DirectAccess-Clients über das IPv4-Internet eine Verbindung zum DirectAccess-Server aufbauen können, dabei werden die IPv6-Pakete innerhalb eines IPv4-Headers zu kapseln. Es kann vom Remotezugriff verwendet werden, um IPv6-Konnektivität mit ISATAP-Hosts im gesamten Intranet bereitzustellen. In einer nicht systemeigenen IPv6-Netzwerkumgebung konfiguriert sich der DirectAccess-Server automatisch als ISATAP-Router. Auflösungsunterstützung für den ISATAP-Namen ist nicht erforderlich.

## 1.7 Konfigurieren von Active Directory

Der DirectAccess-Server und alle DirectAccess-Clientcomputer müssen zu einer Active Directory-Domäne zusammengeführt werden. DirectAccess-Clientcomputer müssen Mitglied folgender Domänenarten sein:

- Domänen, die zur gleichen Gesamtstruktur wie der DirectAccess-Server gehören.
- Domänen, die zu Gesamtstrukturen mit einer bidirektionalen Vertrauensstellung zur DirectAccess-Servergesamtstruktur gehören.
- Domänen mit bidirektonaler Vertrauensstellung zur DirectAccess-Serverdomäne.

### So fügen Sie den DirectAccess-Server einer Domäne hinzu

1. Klicken Sie im Server-Manager auf **Lokaler Server**. Klicken Sie im Detailbereich auf den Link neben **Computername**.
2. Klicken Sie im Dialogfeld **Systemeigenschaften** auf die Registerkarte **Computername** und klicken Sie dann auf **Ändern**.
3. Geben Sie unter **Computernamen** den Namen des Computers ein, falls Sie beim Beitritt des Servers zur Domäne auch den Computernamen ändern. Klicken Sie unter **Mitglied von** auf **Domäne**, und geben Sie dann den Namen der Domäne ein, für die der Beitritt des Servers durchgeführt werden soll (z. B. corp.contoso.com), und klicken Sie dann auf **OK**.
4. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, der über die Berechtigung zum Durchführen des Beitritts von Computern zur Domäne verfügt. Klicken Sie anschließend auf **OK**.
5. Klicken Sie, wenn das Begrüßungsdialogfeld für die Domäne angezeigt wird, auf **OK**.
6. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
7. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
8. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.

### So fügen Sie Clientcomputer zur Domäne hinzu

1. Geben Sie auf dem **Start** Bildschirm **Explorer** ein, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie mit der rechten Maustaste auf das Computersymbol und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Seite **System** auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie im Dialogfeld **Systemeigenschaften** auf der Registerkarte **Computername** auf **Ändern**.
5. Geben Sie unter **Computername** den Namen des Computers ein, falls Sie beim Beitritt des Servers zur Domäne auch den Computernamen ändern. Klicken Sie unter **Mitglied von** auf **Domäne**, und geben Sie dann den Namen der Domäne ein, für die der Beitritt des Servers durchgeführt werden soll (z. B. corp.contoso.com), und klicken Sie dann auf **OK**.
6. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den

Benutzernamen und das Kennwort eines Benutzers ein, der über die Berechtigung zum Durchführen des Beitritts von Computern zur Domäne verfügt. Klicken Sie anschließend auf **OK**.

7. Klicken Sie, wenn das Begrüßungsdialogfeld für die Domäne angezeigt wird, auf **OK**.
8. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
9. Klicken Sie im Dialogfeld **Systemeigenschaften** auf **Schließen**.
10. Klicken Sie auf **Jetzt neu starten**, wenn Sie aufgefordert werden, den Computer neu zu starten.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

##### **NOTE**

Bei der Eingabe des folgenden **Add-Computer**-Befehls müssen Sie die Domänenanmeldeinformationen angeben.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

## 1.8 Konfigurieren von GPOs

Zum Bereitstellen des Remote Zugriffs sind mindestens zwei Gruppenrichtlinie Objekte erforderlich:

- Eins enthält die Einstellungen für den DirectAccess-Server
- Eins enthält die Einstellungen für DirectAccess-Clientcomputer

Wenn Sie den Remote Zugriff konfigurieren, erstellt der Assistent automatisch die erforderlichen Gruppenrichtlinie Objekte. Wenn Ihre Organisation jedoch eine Benennungskonvention erzwingt, können Sie einen Namen in das Gruppenrichtlinienobjekt-Dialogfeld der Remotezugriffs-Verwaltungskonsole eingeben. Weitere Informationen finden Sie unter [2.7. Zusammenfassung der Konfiguration und alternative Gruppenrichtlinienobjekte](#). Das Gruppenrichtlinienobjekt wird beim Erstellen der Berechtigungen erstellt. Wenn Sie nicht über die erforderlichen Berechtigungen zum Erstellen von Gruppenrichtlinienobjekten verfügen, müssen sie vor der Konfiguration des Remotezugriffs erstellt werden.

Informationen zum Erstellen von Gruppenrichtlinie Objekten finden Sie unter [Erstellen und Bearbeiten eines Gruppenrichtlinie Objekts](#).

## **IMPORTANT**

Administratoren können die DirectAccess-Gruppenrichtlinie Objekte manuell mit einer Organisationseinheit verknüpfen, indem Sie die folgenden Schritte ausführen:

1. Verknüpfen Sie die erstellten Gruppenrichtlinienobjekte mit den entsprechenden Organisationseinheiten, bevor Sie DirectAccess konfigurieren.
2. Wenn Sie DirectAccess konfigurieren, sollten Sie eine Sicherheitsgruppe für die Clientcomputer angeben.
3. Der Remote Zugriffs Administrator verfügt möglicherweise über Berechtigungen zum Verknüpfen der Gruppenrichtlinie Objekte mit der Domäne. In beiden Fällen werden die Gruppenrichtlinienobjekte automatisch konfiguriert. Wenn die Gruppenrichtlinienobjekte bereits mit einer Organisationseinheit verknüpft sind, werden die Verknüpfungen nicht entfernt und die die Gruppenrichtlinienobjekte werden nicht mit der Domäne verknüpft. Für ein Server-Gruppenrichtlinienobjekt muss die Organisationseinheit das Servercomputerobjekt enthalten, andernfalls wird das Gruppenrichtlinienobjekt mit dem Domänenstamm verknüpft.
4. Wenn Sie vor dem Ausführen des DirectAccess-Assistenten keine Verknüpfung zur Organisationseinheit hergestellt haben, kann der Domänen Administrator nach Abschluss der Konfiguration die DirectAccess-Gruppenrichtlinie Objekte mit den erforderlichen Organisationseinheiten verknüpfen. Die Verknüpfung zur Domäne kann entfernt werden. Weitere Informationen finden Sie unter [Verknüpfen eines Gruppenrichtlinie Objekts](#).

## **NOTE**

Wenn ein Gruppenrichtlinie Objekt manuell erstellt wurde, ist es möglich, dass das Gruppenrichtlinie Objekt während der DirectAccess-Konfiguration nicht verfügbar ist. Das Gruppenrichtlinie Objekt wurde möglicherweise nicht auf den nächstgelegenen Domänen Controller des Verwaltungs Computers repliziert. In diesem Fall kann der Administrator warten, bis die Replikation abgeschlossen ist oder er kann die Replikation erzwingen.

### **1.8.1 Konfigurieren der Gruppenrichtlinienobjekte für den Remotezugriff mit eingeschränkten Berechtigungen**

In einer Bereitstellung, die Bereitstellungs- und Produktions-Gruppenrichtlinienobjekte verwendet, sollte der Domänenadministrator folgende Schritte ausführen:

1. Abrufen der Liste der erforderlichen Gruppenrichtlinienobjekte für die Remotezugriffsbereitstellung aus dem Remotezugriffsadministrator. Weitere Informationen finden Sie unter [1.8 Planen von Gruppenrichtlinienobjekten](#).
2. Erstellen eines Gruppenrichtlinienobjektpaars mit unterschiedlichen Namen für jedes vom Remotezugriffsadministrator angeforderte Gruppenrichtlinienobjekt. Das erste wird als Bereitstellungsgruppenrichtlinienobjekt verwendet und das zweite als Produktionsgruppenrichtlinienobjekt  
Informationen zum Erstellen von Gruppenrichtlinie Objekten finden Sie unter [Erstellen und Bearbeiten eines Gruppenrichtlinie Objekts](#).
3. Informationen zum Verknüpfen der Produktionsgruppen Richtlinien Objekte finden Sie unter [Verknüpfen eines Gruppenrichtlinie Objekts](#).
4. Erteilen Sie dem Remotezugriffsadministrator Berechtigungen zum **Ändern von Einstellungen, Löschen und Ändern von Sicherheitseinstellungen** für alle Bereitstellungsgruppenrichtlinienobjekte. Weitere Informationen finden Sie unter [Delegieren von Berechtigungen für eine Gruppe oder einen Benutzer in einem Gruppenrichtlinie Objekt](#).
5. Verweigern Sie die Remote Zugriffs Administrator-Berechtigungen zum Verknüpfen von Gruppenrichtlinien Objekten in allen Domänen (oder vergewissern Sie sich, dass der Remote Zugriffs Administrator nicht über diese Berechtigungen verfügt). Weitere Informationen finden Sie unter [Delegieren von Berechtigungen zum Verknüpfen von Gruppenrichtlinie Objekten](#).

Beim Konfigurieren des Remotezugriffs sollten Remotezugriffsadministratoren immer nur die

Bereitstellungsgruppenrichtlinienobjekte angeben (nicht die Produktionsgruppenrichtlinienobjekte). Das gilt für die Erstkonfiguration des Remotezugriffs und für das Ausführen zusätzlicher Konfigurationsschritte, für die zusätzliche Gruppenrichtlinienobjekte erforderlich sind; z. B. beim Hinzufügen von Einstiegspunkten in einer Bereitstellung mit mehreren Standorten oder beim Aktivieren von Clientcomputern auf zusätzlichen Domänen.

Nachdem Remotezugriffsadministrator die Änderungen an der Remotezugriffskonfiguration abgeschlossen hat, sollte der Domänenadministrator die Einstellungen in den Bereitstellungsgruppenrichtlinienobjekten überprüfen und das folgende Verfahren verwenden, um die Einstellungen in die Produktionsgruppenrichtlinienobjekte zu kopieren.

#### TIP

Führen Sie folgendes Verfahren nach jeder Änderung an der Konfiguration des Remotezugriffs durch.

**So kopieren Sie die Einstellungen in die Produktionsgruppenrichtlinienobjekte**

1. Vergewissern Sie sich, dass alle Bereitstellungsgruppenrichtlinienobjekte in der Remotezugriffsbereitstellung mit allen Domänencontrollern der Domäne repliziert wurden. Dieser Schritt ist nötig, um sicherzustellen, dass die aktuellste Konfiguration in die Produktionsgruppenrichtlinienobjekte importiert wird. Weitere Informationen finden Sie unter Überprüfen des Gruppenrichtlinieninfrastrukturstatus.
2. Exportieren der Einstellung durch Sichern aller Bereitstellungsgruppenrichtlinienobjekte in der Remotezugriffsbereitstellung. Weitere Informationen finden Sie unter Sichern eines Gruppenrichtlinienobjekts.
3. Ändern Sie die Sicherheitsfilter für jedes Produktionsgruppenrichtlinienobjekt, damit die Sicherheitsfilter mit denen des entsprechenden Bereitstellungsgruppenrichtlinienobjekts übereinstimmen. Weitere Informationen finden Sie unter Filtern mithilfe von Sicherheitsgruppen.

#### NOTE

Dieser Schritt ist nötig, da die **Importeinstellungen** den Sicherheitsfilter des Quellgruppenrichtlinienobjekts nicht kopieren.

4. Importieren Sie für jedes Produktionsgruppenrichtlinienobjekt die Einstellungen aus der Sicherung des entsprechenden Bereitstellungsrichtlinienobjekts wie folgt:
  - a. Erweitern Sie in der Gruppenrichtlinien-Verwaltungskonsole (GPMC) den Knoten Gruppenrichtlinie Objekte in der Gesamtstruktur und Domäne, in der das Produktions Gruppenrichtlinie Objekt enthalten ist, in das die Einstellungen importiert werden.
  - b. Klicken Sie mit der rechten Maustaste auf Gruppenrichtlinienobjekt und dann auf **Importeinstellungen**.
  - c. Klicken Sie dann im **Importeinstellungs-Assistent** auf der Seite **Willkommen** auf **Weiter**.
  - d. Klicken Sie auf der Seite **Gruppenrichtlinienobjekt sichern** auf **Sichern**.
  - e. Geben Sie im Dialogfeld **Gruppenrichtlinienobjekt sichern** im Feld **Standort** den Pfad an, unter dem Sie die Gruppenrichtlinienobjektsicherungen speichern möchten oder klicken Sie auf **Durchsuchen**, um nach dem Ordner zu suchen.
  - f. Geben Sie in das Feld **Beschreibung** eine Beschreibung für das Produktionsgruppenrichtlinienobjekt ein und klicken Sie dann auf **Sichern**.
  - g. Klicken Sie auf **OK**, sobald die Sicherung abgeschlossen ist und anschließend auf der Seite **Gruppenrichtlinienobjekt sichern** auf **Weiter**.

- h. Geben Sie auf der Seite **Sicherungsspeicherort** in das Feld **Sicherungsordner** den Pfad für den Speicherort an, an dem die Sicherung des entsprechenden Bereitstellungsgruppenrichtlinienobjekts in Schritt 2 gespeichert wurde oder klicken Sie auf **Durchsuchen**, um nach dem Ordner zu suchen und klicken Sie anschließend auf **Weiter**.
  - i. Aktivieren Sie auf der Seite **Quellgruppenrichtlinienobjekt** das Kontrollkästchen **Für jedes Gruppenrichtlinienobjekt nur die neueste Version anzeigen**, um ältere Sicherungen auszublenden, wählen Sie anschließend das entsprechende Bereitstellungsgruppenrichtlinienobjekt aus. Klicken Sie auf **Einstellungen anzeigen**, um die Remotezugriffseinstellungen zu überprüfen, bevor sie auf das Produktionsgruppenrichtlinienobjekt angewendet werden, klicken Sie danach auf **Weiter**.
  - j. Klicken Sie auf der Seite **Sicherung wird überprüft** auf **Weiter** und anschließend auf **Fertig stellen**.

#### **Befehle in Windows PowerShell**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

- So sichern Sie das stagingclientgpo "DirectAccess-Client Einstellungen-Staging" in der Domäne "Corp.contoso.com" im Sicherungsordner "c:\Backups":

```
$backup = Backup-GPO "Name 'DirectAccess Client Settings - Staging' "Domain 'corp.contoso.com' "Path 'C:\Backups\'
```

- So zeigen Sie die Sicherheits Filterung des stagingclientgpo "DirectAccess-Client Einstellungen-Staging" in der Domäne "Corp.contoso.com" an:

```
Get-GPPermission "Name 'DirectAccess Client Settings - Staging' "Domain 'corp.contoso.com' "All | ?{ $_.Permission -eq 'GpoApply'}
```

- Fügen Sie dem Sicherheitsfilter des Produktions Client-Gruppenrichtlinien Objekts "DirectAccess-Client Einstellungen" Produktion "in der Domäne" Corp.contoso.com "die Sicherheitsgruppe" Corp. c-so. com\DirectAccess-Clients "hinzufügt:

```
Set-GPPermission "Name 'DirectAccess Client Settings - Production' "Domain 'corp.contoso.com' "PermissionLevel GpoApply "TargetName 'corp.contoso.com\DirectAccess clients' "TargetType Group
```

- So importieren Sie die Einstellungen aus der Sicherung in das Produktions Client-Gruppenrichtlinien Objekt "DirectAccess-Client Einstellungen" Produktion "in der Domäne" Corp.contoso.com ":

```
Import-GPO "BackupId $backup.Id "Path $backup.BackupDirectory "TargetName 'DirectAccess Client Settings - Production' "Domain 'corp.contoso.com'
```

## 1,9 Konfigurieren von Sicherheitsgruppen

Die DirectAccess-Einstellungen, die auf dem Client Computer Gruppenrichtlinie Objekt enthalten sind, werden nur auf Computer angewendet, die Mitglieder der Sicherheitsgruppe sind, die Sie beim Konfigurieren des Remote Zugriffs angeben. Außerdem müssen Sie eine Sicherheitsgruppe für diese Server erstellen, wenn Sie zum Verwalten Ihrer Anwendungsserver Sicherheitsgruppen verwenden.

## So erstellen Sie eine Sicherheitsgruppe für DirectAccess-Clients

1. Geben Sie auf dem **Start BildschirmDSA**. mscein, und drücken Sie dann die EINGABETASTE. Erweitern Sie in der Konsole **Active Directory-Benutzer und -Computers** im linken Bereich die Domäne, die die Sicherheitsgruppe enthält, klicken Sie mit der rechten Maustaste auf **Benutzer**, zeigen Sie auf **Neu** und klicken Sie dann auf **Gruppe**.
2. Geben Sie im Dialogfeld **Neues Objekt - Gruppe** unter **Gruppenname** den Namen für die Sicherheitsgruppe ein.
3. Klicken Sie unter **Gruppenbereich** auf **Global**, unter **Gruppentyp** auf **Sicherheit** und anschließend auf **OK**.
4. Doppelklicken Sie auf die Sicherheitsgruppe der DirectAccess-Clientcomputer und dann im Dialogfeld **Eigenschaften** auf die Registerkarte **Mitglieder**.
5. Auf der Registerkarte **Mitglieder** klicken Sie auf **Hinzufügen**.
6. Wählen Sie im Dialogfeld zum **Auswählen von Benutzern, Kontakten Computern oder Dienstkonten** die Clientcomputer aus, für die DirectAccess aktiviert werden soll, und klicken Sie anschließend auf **OK**.

### Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

## 1.10 Konfigurieren des Netzwerkadressen Servers

Der Netzwerkadressenserver sollte ein Server mit hoher Verfügbarkeit sein, der über ein gültiges SSL-Zertifikat verfügt, dem die DirectAccess-Clients vertrauen. Für das Netzwerkadressenserver-Zertifikat sind zwei Zertifikatoptionen verfügbar:

- **Privates Zertifikat**

Dieses Zertifikat basiert auf der Zertifikat Vorlage, die Sie anhand der Anweisungen in [1.5.2 Konfigurieren von Zertifikat Vorlagen](#) erstellt haben.

- **Selbst signiertes Zertifikat**

**NOTE**

Selbstsignierte Zertifikate können nicht in Bereitstellungen für mehrere Standorte verwendet werden.

Folgendes ist für alle Zertifikattypen erforderlich, falls noch nicht vorhanden:

- Ein Websitezertifikat für den Netzwerkadressenserver. Der Zertifikatantragsteller sollte die URL des Netzwerkadressenservers sein.
- Ein Sperrlisten-Verteilungspunkt mit hoher Verfügbarkeit aus dem internen Netzwerk.

#### **NOTE**

Wenn sich die Netzwerkadressenserver-Website auf dem DirectAccess-Server befindet, wird bei der Konfiguration des Remotezugriffs automatisch eine Website erstellt. Diese Website ist an das von Ihnen angegebene Serverzertifikat gebunden.

#### **So installieren Sie das Netzwerkadressenserver-Zertifikat von einer internen Zertifizierungsstelle**

1. Auf dem Server, auf dem die Netzwerkadressen Server-Website gehostet wird: Geben Sie auf dem **Start BildschirmMMC** ein, und drücken Sie dann die **EINGABETASTE**.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-ins hinzufügen oder entfernen** auf **Zertifikate, Hinzufügen, Computerkonto, Weiter, Lokaler Computer, Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
6. Klicken Sie zweimal auf **Weiter**.
7. Aktivieren Sie auf der Seite **Zertifikate anfordern** das Kontrollkästchen für die Zertifikat Vorlage, die Sie erstellt haben, indem Sie die Anweisungen unter 1.5.2 Konfigurieren von Zertifikat Vorlagen befolgen.  
Klicken Sie bei Bedarf auf **Es werden zusätzliche Informationen für diese Zertifikatsregistrierung benötigt**.
8. Klicken Sie im Dialogfeld **Zertifikateigenschaften** auf der Registerkarte **Antragsteller** im Bereich **Antragstellernname** unter **Typ** auf **Allgemeiner Name**.
9. Geben Sie in das Feld **Wert** den FQDN der Netzwerkadressenserver-Website ein und klicken Sie dann auf **Hinzufügen**.
10. Wählen Sie unter **Alternativer Name** für **Typ** die Option **DNS** aus.
11. Geben Sie in das Feld **Wert** den FQDN der Netzwerkadressenserver-Website ein und klicken Sie dann auf **Hinzufügen**.
12. Auf der Registerkarte **Allgemein** unter **Anzeigename** können Sie einen Namen für das Zertifikat eingeben, sodass Sie es schneller identifizieren können.
13. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
14. Überprüfen Sie im Detailbereich des Zertifikat-Snap-in, dass das neue Zertifikat unter **Serverauthentifizierung** mit der Option **Beabsichtigte Zwecke** registriert wurde.

#### **So konfigurieren Sie den Netzwerkadressenserver**

1. Richten Sie eine Website auf einem Server mit hoher Verfügbarkeit ein. Für die Website sind keine Inhalte erforderlich, für einen Test sollten Sie jedoch eine Standardseite definieren, die eine Meldung anzeigt, wenn Clients eine Verbindung zu der Website aufbauen.

#### **NOTE**

Dieser Schritt ist nicht nötig, wenn die Netzwerkadressenserver-Website auf einem DirectAccess-Server gehostet wird.

2. Binden Sie ein HTTPS-Serverzertifikat an die Website. Der allgemeine Name des Zertifikats sollte mit dem Namen der Netzwerkadressenserver-Website übereinstimmen. Vergewissern Sie sich, dass die

DirectAccess-Clients der ausstellenden Zertifizierungsstelle vertrauen.

**NOTE**

Dieser Schritt ist nicht nötig, wenn die Netzwerkadressenserver-Website auf einem DirectAccess-Server gehostet wird.

3. Richten Sie eine CRL-Website mit hoher Verfügbarkeit aus dem internen Netzwerk ein.

Auf die Sperrlisten-Verteilungspunkte wurde folgendermaßen zugegriffen:

- Webserver mithilfe einer HTTP-basierten URL, z. b.: <https://crl.corp.contoso.com/crl/corp-APP1-CA.crl>
- Dateiserver, auf die über einen UNC-Pfad (Universal Naming Convention) zugegriffen wird, z. b. \\crl.Corp.contoso.com\crl\corp-App1-ca.crl

Wenn der interne Sperrlisten-Verteilungspunkt nur über IPv6 erreichbar ist, müssen Sie eine Windows-Firewall mit erweiterter Sicherheit konfigurieren, und in der Verbindungssicherheitsregel den IPsec-Schutz aus der IPv6-Adresse Ihres Intranets zu den IPv6-Adressen Ihrer Sperrlisten-Verteilungspunkte ausschließen.

4. Vergewissern Sie sich, dass die DirectAccess-Clients im internen Netzwerk den Namen des Netzwerkadressenservers auflösen können. Vergewissern Sie sich, dass der Name nicht von DirectAccess-Clients im Internet aufgelöst werden kann.

## Nächster Schritt

- [Schritt 2: Konfigurieren erweiterter DirectAccess-Server](#)

# Schritt 2 Konfigurieren von erweiterten DirectAccess-Servern

09.04.2020 • 21 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird die Konfiguration der Client- und Servereinstellungen erläutert, die für eine erweiterte Remotezugriffsbereitstellung erforderlich sind, die einen einzelnen Remotezugriffsserver in einer gemischten IPv4- und IPv6-Umgebung verwendet. Bevor Sie mit den Bereitstellungs Schritten beginnen, stellen Sie sicher, dass Sie die in [Planen einer erweiterten DirectAccess-Bereitstellung](#)beschriebenen Planungsschritte abgeschlossen haben.

AUFGABE	BESCHREIBUNG
2.1. Installieren der Remotezugriffsrolle	Installieren Sie die Remotezugriffsrolle.
2.2. Konfigurieren des Bereitstellungstypen	Konfigurieren Sie den Bereitstellungstypen als DirectAccess und VPN, nur DirectAccess, oder nur VPN
<a href="#">Planen einer erweiterten DirectAccess-Bereitstellung</a>	Konfigurieren Sie den Remotezugriffsserver mit den Sicherheitsgruppen, die die DirectAccess-Clients enthalten.
2.4. Konfigurieren des Remotezugriffsservers	Konfigurieren Sie die Einstellungen des Remotezugriffsservers.
2.5. Konfigurieren des Infrastrukturserver	Konfigurieren Sie die Infrastrukturserver, die in der Organisation eingesetzt werden.
2.6. Konfigurieren von Anwendungsservern	Konfigurieren Sie die Anwendungsserver so, dass für die Anmeldung eine Authentifizierung und Verschlüsselung vorausgesetzt wird.
2.7. Zusammenfassung der Konfiguration und alternative Gruppenrichtlinienobjekte	Zeigen Sie die Zusammenfassung der Remotezugriffskonfiguration an und ändern Sie bei Bedarf die Gruppenrichtlinienobjekte.
2.8. Konfiguration des Remotezugriffsservers mithilfe von Windows PowerShell	Konfigurieren Sie den Remote Zugriff mithilfe von Windows PowerShell.

## NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## 2.1. Installieren der Remotezugriffsrolle

Um den Remotezugriff bereitzustellen, müssen Sie die Remotezugriffsrolle auf einem Server in Ihrer Organisation installieren, der als Remotezugriffsserver fungiert.

### So installieren Sie die Remotezugriffsrolle

1. Klicken Sie auf dem Remote Zugriffs Server in der Server-Manager-Konsole im Dashboard auf Rollen und

## Features hinzufügen.

2. Klicken Sie dreimal auf **Weiter**, um zum Bildschirm **Serverrollen auswählen** zu gelangen.
3. Wählen Sie im Dialogfeld **Serverrollen auswählen** die Rolle **Remotezugriff** aus, klicken Sie bei Aufforderung auf **Features hinzufügen**, und klicken Sie dann auf **Weiter**.
4. Klicken Sie fünfmal auf **Weiter**.
5. Klicken Sie auf der Seite **Installationsauswahl bestätigen** auf **Installieren**.
6. Überprüfen Sie auf der Seite **Installationsstatus**, ob die Installation erfolgreich war, und klicken Sie dann auf **Schließen**.

## Windows PowerShell äquivalente Befehle

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

## 2.2. Konfigurieren des Bereitstellungstypen

Der Remotezugriff kann mithilfe der Remotezugriffs-Verwaltungskonsole auf drei verschiedene Arten bereitgestellt werden:

- DirectAccess und VPN
- Nur DirectAccess
- Nur VPN

In dieser Anleitung wird in den Beispielverfahren eine Nur-DirectAccess-Bereitstellung verwendet.

### So konfigurieren Sie den Bereitstellungstypen

1. Öffnen Sie auf dem Remote Zugriffs Server die Remote Zugriffs-Verwaltungskonsole: Geben Sie auf dem Start Bildschirm `ramgmtui.exe` ein, und drücken Sie dann die EINGABETASTE. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, bestätigen Sie, dass die angezeigte Aktion ausgeführt werden soll, und klicken Sie anschließend auf **Ja**.
2. Klicken Sie in der Remotezugriffs-Verwaltungskonsole im mittleren Bereich auf **Remotezugriffs-Setup-Assistenten ausführen**.
3. Klicken Sie im Dialogfeld **Remotezugriff konfigurieren** die entsprechende Bereitstellungsoption an (DirectAccess und VPN, nur DirectAccess oder nur VPN).

## 2.3. Konfigurieren von DirectAccess-Clients

Damit ein Clientcomputer zur Verwendung von DirectAccess bereitgestellt werden kann, muss er zur ausgewählten Sicherheitsgruppe gehören. Nachdem DirectAccess konfiguriert wurde, werden Clientcomputer in der Sicherheitsgruppe bereitgestellt, damit sie das DirectAccess-Gruppenrichtlinienobjekt empfangen. Sie können auch das Bereitstellungsszenario konfigurieren, darüber können Sie DirectAccess für den Clientzugriff und die Remoteverwaltung oder nur für die Remoteverwaltung konfigurieren.

### So konfigurieren Sie DirectAccess-Clients

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 1 Remoteclients** auf **Konfigurieren**.

2. Klicken Sie im DirectAccess-Client-Setup-Assistenten auf der Seite **Bereitstellungsszenario** auf das Bereitstellungsszenario, das Sie in Ihrer Organisation verwenden möchten (**Gesamtes DirectAccess** oder **Nur Remoteverwaltung**) und klicken Sie dann auf **Weiter**.
3. Klicken Sie auf der Seite **Gruppen auswählen** auf **Hinzufügen**.
4. Wählen Sie im Dialogfeld **Gruppen auswählen** die Sicherheitsgruppen aus, die Ihre DirectAccess-Clientcomputer enthalten.

**NOTE**

Wenn sich die Sicherheitsgruppe in einer anderen Gesamtstruktur als der RAS-Server befindet, klicken Sie nach Abschluss des Setup-Assistenten für den Remote Zugriff auf **Verwaltungs Server aktualisieren** im Bereich **Tasks**, um die Domänen Controller und Configuration Manager Server in der neuen Gesamtstruktur zu ermitteln.

5. Aktivieren Sie das Kontrollkästchen **DirectAccess ausschließlich für mobile Computer aktivieren**, damit bei Bedarf nur mobile Computer auf das interne Netzwerk zugreifen.
6. Aktivieren Sie das Kontrollkästchen **Tunnelerzwingung verwenden**, um den gesamten Client-Datenverkehr (an das interne Netzwerk und das Internet) bei Bedarf über den RAS-Server zu leiten.
7. Klicken Sie auf **Weiter**.
8. Vorgehensweise auf der Seite **Netzwerkkonnektivitäts-Assistent**:

- Fügen Sie in der Tabelle Ressourcen hinzu, die zum Ermitteln der Konnektivität zum internen Netzwerk verwendet wird. Wenn keine weiteren Ressourcen konfiguriert werden, wird automatisch ein Standardwebtest erstellt.

**Caution**

Wenn Sie die Webtestspeicherorte zum Ermitteln der Konnektivität zum Unternehmensnetzwerk konfigurieren, müssen Sie sich vergewissern, dass mindestens ein HTTP-basierter Test konfiguriert ist. Es reicht nicht aus, nur einen **ping**-Test zu konfigurieren. Diese Vorgehensweise kann zu einer ungenauen Ermittlung des Verbindungsstatus führen. Das liegt daran begründet, dass **ping** aus IPsec ausgeschlossen wird, folglich sorgt er nicht dafür, dass die IPsec-Tunnel ordnungsgemäß eingerichtet werden.

- Fügen Sie eine Helpdesk-E-Mail-Adresse hinzu, damit Benutzer Informationen absenden können, wenn bei ihnen Verbindungsprobleme auftreten.
- Geben Sie einen Anzeigenamen für die DirectAccess-Verbindung ein. Dieser Name wird in der Netzwerkliste angezeigt, wenn der Benutzer auf das Netzwerksymbol im Infobereich klickt.
- Aktivieren Sie bei Bedarf das Kontrollkästchen **DirectAccess-Clients ermöglichen, die lokale Namensauflösung zu verwenden**.

**NOTE**

Wenn die lokale Namensauflösung aktiviert ist, können Benutzer, bei denen den Netzwerkkonnektivitäts-Assistent ausgeführt wird, auswählen, Namen mithilfe von DNS-Servern aufzulösen, die auf dem DirectAccess-Clientcomputer konfiguriert sind.

9. Klicken Sie auf **Fertig stellen**.

## 2.4. Konfigurieren des Remotezugriffsservers

Um den Remotezugriff bereitzustellen, müssen Sie den Remotezugriffsserver mit korrekten Netzwerkadapters,

einer öffentlichen URL für den Remotezugriffsserver, zu dem Clientcomputer eine Verbindung aufbauen können (die ConnectTo-Adresse), einem IP-HTTPS-Zertifikat mit einem Antragsteller, der mit der ConnectTo-Adresse übereinstimmt, IPv6-Einstellungen und Clientcomputer-Authentifizierung konfigurieren.

#### So konfigurieren Sie den Remotezugriffsserver

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 2 RAS-Server** auf **Konfigurieren**.
2. Klicken Sie im Setup-Assistenten für den RAS-Server auf der Seite **Netzwerktopologie** auf die Bereitstellungstopologie, die in Ihrer Organisation verwendet wird. Geben Sie unter **Geben Sie den öffentlichen Namen oder die öffentliche IPv4-Adresse** an den öffentlichen Namen für die Bereitstellung ein (dieser Name stimmt mit dem Antragstellernamen des IP-HTTPS-Zertifikats überein, z. B. edge1.contoso.com), und klicken Sie dann auf **Weiter**.
3. Auf der Seite **Netzwerkadapter** erkennt der Assistent automatisch die Netzwerkadapter für die Netzwerke in Ihrer Bereitstellung. Falls der Assistent nicht die korrekten Netzwerkadapter erkennt, wählen Sie die korrekten Adapter manuell aus. Der Assistent erkennt außerdem automatisch das IP-HTTPS-Zertifikat, das auf dem öffentlichen Namen für die Bereitstellung basiert und im vorherigen Schritt des Assistenten festgelegt wurde. Wenn der Assistent das korrekte IP-HTTPS-Zertifikat nicht erkennt, klicken Sie auf **Durchsuchen**, um das korrekte Zertifikat manuell auszuwählen und klicken Sie dann auf **Weiter**.
4. Auf der Seite **Präfixkonfiguration** wird nur bei IPv6-Bereitstellung im internen Netzwerk angezeigt) erkennt der Assistent automatisch die IPv6-Einstellungen, die im internen Netzwerk eingesetzt werden. Wenn für Ihre Bereitstellung zusätzliche Präfixe erforderlich sind, konfigurieren Sie die IPv6-Präfixe für das interne Netzwerk, ein IPv6-Präfix zum Zuweisen für DirectAccess-Clientcomputer und ein IPv6-Präfix zum Zuweisen für VPN-Clientcomputer.

#### NOTE

Sie können mehrere interne IPv6-Präfixe angeben, indem Sie eine durch Semikolon getrennte Liste verwenden, z. B. 2001:db8:1::/48;2001:db8:2::/48.

#### 5. Vorgehensweise auf der Seite Authentifizierung:

- Klicken Sie unter **Benutzauthentifizierung** auf **Active Directory-Anmeldeinformationen**. Um eine Bereitstellung mit der zweistufigen Authentifizierung zu konfigurieren, klicken Sie auf **Zweistufige Authentifizierung**. Weitere Informationen finden Sie unter [Bereitstellen des Remotezugriffs mit OTP-Authentifizierung](#).
- In Bereitstellungen für mehrere Standorte oder die zweistufige Authentifizierung müssen Sie die Computerzertifikatauthentifizierung verwenden. Aktivieren Sie das Kontrollkästchen **Computerzertifikate verwenden**, um die Computerzertifikatauthentifizierung zu verwenden und das IPsec-Stammzertifikat auszuwählen.
- Aktivieren Sie das Kontrollkästchen **Windows 7-Client Computer Verbindungen über DirectAccess aktivieren**, damit Windows 7-Client Computer über DirectAccess eine Verbindung herstellen können.

#### NOTE

Für diesen Bereitstellungstypen müssen Sie ebenfalls die Computerzertifikatauthentifizierung verwenden.

#### 6. Klicken Sie auf **Fertig stellen**.

## 2,5. Konfigurieren des Infrastrukturservers

Um die Infrastrukturserver in einer Remotezugriffsbereitstellung zu konfigurieren, müssen Sie den Netzwerkadressenserver, die DNS-Einstellungen (einschließlich DNS-Suffixsuchliste) und die Verwaltungsserver konfigurieren, die nicht automatisch vom Remotezugriff erkannt werden.

### So konfigurieren Sie die Infrastrukturserver

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 3 Infrastrukturserver** auf **Konfigurieren**.
2. Klicken Sie im Assistenten zum Einrichten des Infrastrukturservers auf der Seite **Netzwerkadressenserver** auf die Option, die dem Speicherort des Netzwerkadressenservers in Ihrer Bereitstellung entspricht. Wenn der Netzwerkadressenserver auf einem Remotewebservice installiert ist, geben Sie die URL ein und klicken Sie dann auf **Überprüfen**, bevor Sie fortfahren. Wenn der Netzwerkadressenserver nicht auf einem Remotewebservice installiert ist, klicken Sie auf **Durchsuchen**, um das entsprechende Zertifikat zu suchen und klicken Sie dann auf **Weiter**.
3. Geben Sie auf der Seite **DNS** in der Tabelle alle zusätzlichen Namenssuffixe ein, die als NRPT-Ausnahmen (Name Resolution Policy Table, Richtlinientabelle für die Namensauflösung) angewendet werden. Wählen Sie die entsprechende Option für die lokale Namensauflösung, und klicken Sie dann auf **Weiter**.
4. Auf der Seite **DNS-Suffixsuchliste** erkennt der RAS-Server die Domänensuffixe in der Bereitstellung automatisch. Verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um Domänensuffixe aus der Liste der zu verwendenden Domänensuffixe zu entfernen oder ihr hinzuzufügen. Um ein neues Domänensuffix unter **Neues Suffix** hinzuzufügen, müssen Sie dass Suffix eingeben und anschließend auf **Hinzufügen** klicken. Klicken Sie auf **Weiter**.
5. Fügen Sie auf der Seite **Verwaltung** die Verwaltungsserver hinzu, die nicht automatisch erkannt wurden und klicken Sie dann auf **Weiter**. Der Remote Zugriff fügt automatisch Domänen Controller und Configuration Manager Server hinzu.

### NOTE

Obwohl die Server automatisch hinzugefügt werden, werden Sie nicht in der Liste angezeigt. Nachdem Sie die Konfiguration zum ersten Mal angewendet haben, werden die Configuration Manager-Server in der Liste angezeigt.

6. Klicken Sie auf **Fertig stellen**.

## 2,6. Konfigurieren von Anwendungsservern

Bei einer Remotezugriffsbereitstellung ist das Konfigurieren von Anwendungsservern eine optionale Aufgabe. Mit dem Remotezugriff können Sie für ausgewählte Anwendungsserver eine Authentifizierung voraussetzen, die durch die Aufnahme in eine Sicherheitsgruppe der Anwendungsserver bestimmt wird. Standardmäßig wird der Datenverkehr an die Anwendungsserver, die eine Authentifizierung voraussetzen, ebenfalls verschlüsselt; sie können jedoch auswählen, den Datenverkehr an Anwendungsserver nicht zu verschlüsseln und nur die Authentifizierung verwenden.

### NOTE

Die Authentifizierung ohne Verschlüsselung wird nur auf Anwendungsservern unterstützt, auf denen Windows Server 2012 R2, Windows Server 2012 oder Windows Server 2008 R2 ausgeführt wird.

### So konfigurieren Sie die Anwendungsserver

1. Klicken Sie im mittleren Bereich der Remotezugriffs-Verwaltungskonsole unter **Schritt 4 Anwendungsserver** auf **Konfigurieren**.

2. Klicken Sie im DirectAccess-Anwendungsserver-Setup-Assistent auf **Authentifizierung auf ausgewählte Anwendungsserver erweitern**, um die Authentifizierung von ausgewählten Anwendungsservern vorauszusetzen. Klicken Sie auf **Hinzufügen**, um die Sicherheitsgruppe des Anwendungsservers auszuwählen.
3. Um den Zugriff nur auf Server in der Sicherheitsgruppe des Anwendungsservers zu beschränken, müssen Sie das Kontrollkästchen **Zugriff nur für Server in den Sicherheitsgruppen zulassen** aktivieren.
4. Wenn Sie die Authentifizierung ohne Verschlüsselung verwenden möchten, wählen Sie den **Datenverkehr nicht verschlüsseln** aus. Kontrollkästchen **nur Authentifizierung verwenden**.
5. Klicken Sie auf **Fertig stellen**.

## 2,7. Zusammenfassung der Konfiguration und alternative Gruppenrichtlinienobjekte

Wenn die Konfiguration des Remotezugriffs abgeschlossen ist, wird das Dialogfeld **Überprüfung des Remotezugriffs** angezeigt. Sie können alle zuvor ausgewählten Einstellungen überprüfen, dazu gehören:

1. **GPO-Einstellungen:** Hier werden der Gruppenrichtliniename des DirectAccess-Servers und der Client-Gruppenrichtlinienobjektname aufgelistet. Außerdem können Sie auf die Verknüpfung **Ändern** neben der Überschrift **GPO-Einstellungen** klicken, um die GPO-Einstellungen zu ändern.
2. **Remoteclients:** Hier wird die DirectAccess-Clientkonfiguration angezeigt, einschließlich der Sicherheitsgruppe, des Status der Tunnelerzwingung, der Verbindungsprüfer und des DirectAccess-Verbindungsnamens.
3. **RAS-Server:** Hier wird die DirectAccess-Konfiguration angezeigt, einschließlich des öffentlichen Namens/Adresse, der Netzwerkadapterkonfiguration, der Zertifikatinformationen und der OTP-Informationen, falls konfiguriert.
4. **Infrastrukturserver:** Diese Liste enthält die Netzwerkadressenserver-URL, DNS-Suffixe, die von DirectAccess-Clients verwendet werden sowie Verwaltungsserverinformationen.
5. **Anwendungsserver:** Hier wird zusätzlich zum Status der End-to-End-Authentifizierung bestimmter Anwendungsserver der DirectAccess-Remoteverwaltungsstatus angezeigt.

## 2,8. Konfiguration des Remotezugriffsservers mithilfe von Windows PowerShell

### Befehle in Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

So führen Sie eine vollständige Installation in einer Edge-Topologie des Remote Zugriffs für DirectAccess nur in einer Domäne mit dem Stamm **Corp.contoso.com** und mithilfe der folgenden Parameter aus: Server-Gruppenrichtlinien Objekt: **DirectAccess-Servereinstellungen**, Client-GPO: DirectAccess-Client Einstellungen, interner Netzwerkadapter: **Corpnet**, externer Netzwerk Adapter: **Internet**, Verbindungs Adresse: **Edge1.contoso.com**

```
Install-RemoteAccess -Force -PassThru -ServerGpoName 'corp.contoso.com\DirectAccess Server Settings' -ClientGpoName 'corp.contoso.com\DirectAccess Client Settings' -DAInstallType 'FullInstall' -InternetInterface 'Internet' -InternalInterface 'Corpnet' -ConnectToAddress 'edge1.contoso.com' -NlsUrl 'https://nls.corp.contoso.com/'
```

So konfigurieren Sie den Remotezugriffsserver so, dass er die Computerzertifikatauthentifizierung verwendet, mit einem IPsec-Stammzertifikat, das von der Zertifizierungsstelle mit der Bezeichnung CORP-APP1-CA ausgestellt wird:

```
$certs = Get-ChildItem Cert:\LocalMachine\Root
$IPsecRootCert = $certs | Where-Object {$_['Subject -Match "corp-APP1-CA"]}
Set-DAServer -IPsecRootCertificate $IPsecRootCert
```

So fügen Sie die Sicherheitsgruppe hinzu, die die DirectAccess-Clients mit der Bezeichnung **DirectAccessClients** enthält, und entfernen die Standard-Domänencomputer-Sicherheitsgruppe:

```
Add-DAClient -SecurityGroupNameList @('corp.contoso.com\DirectAccessClients')
Remove-DAClient -SecurityGroupNameList @('corp.contoso.com\Domain Computers')
```

So aktivieren Sie den Remote Zugriff für alle Computer (nicht nur für Notebooks und Laptops) und zum Aktivieren des Remote Zugriffs für Windows 7-Clients:

```
Set-DAClient -OnlyRemoteComputers 'Disabled' -Downlevel 'Enabled'
```

So konfigurieren Sie die DirectAccess-Clienterfahrung, einschließlich des Anzeigenamens der Verbindung und der Webtest-URL:

```
Set-DAClientExperienceConfiguration -FriendlyName 'Contoso DirectAccess Connection' -PreferLocalNamesAllowed $False -PolicyStore 'corp.contoso.com\DirectAccess Client Settings' -CorporateResources @('HTTP:https://directaccess-WebProbeHost.corp.contoso.com')
```

## Vorheriger Schritt

- [Schritt 1: Konfigurieren der erweiterten DirectAccess-Infrastruktur](#)

## Nächster Schritt

- [Schritt 3: Überprüfen der Bereitstellung](#)

# Schritt 3 Überprüfen der erweiterten DirectAccess-Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie überprüfen, ob Sie die DirectAccess-Bereitstellung ordnungsgemäß konfiguriert haben.

## So überprüfen Sie den Zugriff auf interne Ressourcen über DirectAccess

1. Verbinden eines DirectAccess-Client Computers mit dem Unternehmensnetzwerk und Abrufen des Gruppenrichtlinie Objekts.
2. Klicken Sie im Benachrichtigungsbereich auf das Symbol **Netzwerkverbindungen**, um auf den DirectAccess-Medien-Manager zuzugreifen.
3. Klicken Sie auf **DirectAccess-Verbindung**, und Sie werden feststellen, dass der Status **Lokal verbunden** ist.
4. Verbinden Sie den Clientcomputer mit dem externen Netzwerk, und versuchen Sie, auf interne Ressourcen zuzugreifen.

Sie sollten auf alle Unternehmensressourcen zugreifen können.

## Vorheriger Schritt

- [Schritt 2: Konfigurieren von DirectAccess-Servern](#)

# Hinzufügen von DirectAccess zu einer vorhandenen Remotezugriffsbereitstellung (VPN)

09.04.2020 • 12 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

## Szenariobeschreibung

In diesem Szenario wird ein einzelner Computer mit Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 als DirectAccess-Server mit den empfohlenen Einstellungen konfiguriert, nachdem Sie das VPN bereits installiert und konfiguriert haben. Wenn Sie DirectAccess mit Unternehmens Features wie einem Cluster mit Lastenausgleich, der Bereitstellung für mehrere Standorte oder zweistufiger Client Authentifizierung konfigurieren möchten, schließen Sie das in diesem Thema beschriebene Szenario zum Einrichten eines einzelnen Servers ab, und richten Sie dann das Enterprise-Szenario ein, wie unter Bereitstellen des [Remote Zugriffs in einem Unternehmen](#)beschrieben.

## Inhalt dieses Szenarios

Zum Einrichten eines einzelnen Remotezugriffsservers sind mehrere Planungs- und Bereitstellungsschritte erforderlich.

### Planungsschritte

Die Planung besteht aus zwei Phasen:

#### 1. Planen der Infrastruktur für den Remote Zugriff

In dieser Phase beschreiben Sie die erforderliche Planung zum Einrichten der Netzwerkinfrastruktur, bevor Sie mit der Remotezugriffsbereitstellung beginnen. Sie umfasst das Planen der Netzwerk- und Servertopologie, Zertifikate, des Domain Name System (DNS), der Active Directory, die Konfiguration der Gruppenrichtlinienobjekte und des DirectAccess-Netzwerkadressenservers.

#### 2. Planen der Bereitstellung des Remote Zugriffs

In dieser Phase beschreiben Sie die erforderlichen Planungsschritte zur Vorbereitung der Remotezugriffsbereitstellung. Dazu gehört die Planung der Clientcomputer für den Remotezugriff, Server- und Clientauthentifizierungsanforderungen und Infrastrukturserver.

### Bereitstellungsschritte

Die Bereitstellung besteht aus drei Phasen:

#### 1. Konfigurieren der Remote Zugriffs Infrastruktur

In dieser Phase konfigurieren Sie das Netzwerk und Routing, die Firewalleinstellungen (falls erforderlich), die Zertifikate, DNS-Server, Active Directory- und Gruppenrichtlinienobjekt-Einstellungen und den DirectAccess-Netzwerkadressenserver.

#### 2. Konfigurieren der Einstellungen für den Remote Zugriffs Server

In dieser Phase konfigurieren Sie die Remotezugriffsclientcomputer, den Remotezugriffsserver und die Infrastrukturserver.

#### 3. Überprüfen der Bereitstellung

In dieser Phase überprüfen Sie die Bereitstellung auf die ordnungsgemäße Bereitstellung.

## Praktische Anwendungen

Die Bereitstellung eines einzelnen Remotezugriffsservers bietet Folgendes:

- **Einfache Zugriffsrechte**

Verwaltete Client Computer unter Windows 8 und Windows 7 können als DirectAccess-Client Computer konfiguriert werden. Diese Clients können, wenn sie sich im Internet befinden, über DirectAccess auf interne Netzwerkressourcen zugreifen, ohne sich über eine VPN-Verbindung anmelden zu müssen. Clientcomputer, die keines dieser Betriebssysteme verwenden, können per VPN eine Verbindung zum internen Netzwerk herstellen. Sowohl DirectAccess als auch VPN werden über dieselbe Konsole und mit denselben Assistenten verwaltet.

- **Einfache Verwaltung**

Die Remoteverwaltung von DirectAccess-Clientcomputern im Internet ist mithilfe von Remotezugriff-Administratoren über DirectAccess möglich, selbst wenn sich die Clientcomputer nicht im internen Unternehmensnetzwerk befinden. Clientcomputer, die nicht den Unternehmensanforderungen entsprechen, können automatisch über Verwaltungsserver gewartet werden.

## Für dieses Szenario erforderliche Rollen und Features

Die folgende Tabelle enthält die für dieses Szenario erforderlichen Rollen und Features:

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
Remotezugriffs-Rolle	<p>Die Rolle wird über die Server-Manager-Konsole oder Windows PowerShell installiert bzw. deinstalliert. Diese Rolle umfasst DirectAccess (zuvor ein Feature unter Windows Server 2008 R2) sowie die Routing- und RAS-Dienste (zuvor ein Rollendienst unter der Serverrolle für Netzwerkrichtlinien- und Zugriffsdiensste). Die Remotezugriffs-Rolle besteht aus zwei Komponenten:</p> <ol style="list-style-type: none"><li>1. DirectAccess-und RRAS-VPN (Routing and Remote Access Services): wird in der Remote Zugriffs-Verwaltungskonsole verwaltet.</li><li>2. RRAS-Routing: wird in der Routing-und RAS-Konsole verwaltet.</li></ol> <p>Die Remotezugriffs-Serverrolle ist von den folgenden Serverfeatures abhängig:</p> <ul style="list-style-type: none"><li>-Internetinformationsdienste (IIS)-Webserver: erforderlich, um den Netzwerkadressen Server auf dem Remote Zugriffs Server und den Standardweb Test zu konfigurieren.</li><li>-Interne Windows-Datenbank: wird für die lokale Kontoführung auf dem Remote Zugriffs Server verwendet.</li></ul>

ROLLE/FEATURE	AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD
<p>Feature "Tools für die Remotezugriffsverwaltung":</p>	<p>So installieren Sie dieses Feature:</p> <ul style="list-style-type: none"> <li>-Standardmäßig auf einem RAS-Server, wenn die Remote Zugriffs Rolle installiert ist. Unterstützt die Benutzeroberfläche der Remote-Verwaltungskonsole und die Windows PowerShell-Cmdlets.</li> <li>: Optional auf einem Server installiert, auf dem die Remote Zugriffs-Server Rolle nicht ausgeführt wird. In diesem Fall wird es für die Remoteverwaltung eines RAS-Computers verwendet, der DirectAccess und VPN ausführt.</li> </ul> <p>Das Feature "Tools für die Remotezugriffsverwaltung" besteht aus den folgenden Komponenten:</p> <ul style="list-style-type: none"> <li>-Remote Zugriffs-GUI</li> <li>-Remote Zugriffs Modul für Windows PowerShell</li> </ul> <p>Abhängigkeiten umfassen:</p> <ul style="list-style-type: none"> <li>-Gruppenrichtlinien-Verwaltungskonsole</li> <li>-RAS-Verbindungs-Manager-Verwaltungskit (CMAK)</li> <li>-Windows PowerShell 3,0</li> <li>-Tools und Infrastruktur für die grafische Verwaltung</li> </ul>

## Hardwareanforderungen

Für dieses Szenario müssen die folgenden Hardwareanforderungen erfüllt werden:

### Server Anforderungen

- Ein Computer, der die Hardwareanforderungen für Windows Server 2012 erfüllt.
- Auf dem Server muss mindestens ein Netzwerkadapter installiert, aktiviert und mit dem internen Netzwerk verbunden sein. Werden zwei Adapter verwendet, sollte ein Adapter mit dem internen Unternehmensnetzwerk und der andere mit dem externen Netzwerk (Internet) verbunden sein.
- Falls Teredo als IPv4- bis IPv6-Übergangsprotokoll benötigt wird, benötigt der externe Adapter des Servers zwei aufeinanderfolgenden öffentlichen IPv4-Adressen. Der Assistent zum Aktivieren von DirectAccess aktiviert nicht Teredo, selbst wenn zwei aufeinanderfolgende IP-Adressen vorhanden sind. Wenn nur eine IP-Adresse verfügbar ist, kann nur IP-HTTPS als Übergangsprotokoll verwendet werden.
- Mindestens ein Domänencontroller. RAS-Server und DirectAccess-Clients müssen Domänenmitglieder sein.
- Der Assistent zum Aktivieren von DirectAccess benötigt Zertifikate für IP-HTTPS und den Netzwerkadressenserver. Wenn das SSTP-VPN bereits ein Zertifikat verwendet, wird es für IP-HTTPS erneut verwendet. Wenn das SSTP-VPN nicht konfiguriert ist, können Sie ein Zertifikat für IP-HTTPS konfigurieren oder ein automatisch erstelltes selbstsigniertes Zertifikat verwenden. Für den Netzwerkadressenserver können Sie ein Zertifikat konfigurieren oder ein automatisch erstelltes selbstsigniertes Zertifikat verwenden.

### Client Anforderungen

- Auf einem Client Computer muss Windows 8 oder Windows 7 ausgeführt werden.

#### NOTE

Nur die folgenden Betriebssysteme können als DirectAccess-Clients verwendet werden: Windows Server 2012, Windows Server 2008 R2, Windows 8 Enterprise, Windows 7 Enterprise und Windows 7 Ultimate.

## Anforderungen an Infrastruktur und Management Server

- Während der Remoteverwaltung von DirectAccess-Clientcomputern initiieren die Clients die Kommunikation mit Verwaltungsservern, z. B. Domänencontrollern, System Center-Konfigurationsservern und Inhaltsregistrierungsstellen (HRA)-Servern, für Dienste, darunter Windows- und Antivirus-Updates sowie Network Access Protection (NAP)-Clientkompatibilität. Die erforderlichen Server sollten bereitgestellt werden, bevor mit der Bereitstellung des Remotezugriffs begonnen wird.
- Falls der Remotezugriff Client-NAP-Kompatibilität erfordert, sollten die NPS-Server und der HRA bereitgestellt werden, bevor mit der Bereitstellung des Remotezugriffs begonnen wird.
- Es ist ein DNS-Server erforderlich, auf dem Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008 mit SP2 ausgeführt wird.

## Software Anforderungen

Für dieses Szenario müssen die folgenden Softwareanforderungen erfüllt werden:

### Server Anforderungen

- Der Remotezugriffsserver muss Domänenmitglied sein. Der Server kann an der Schwelle zum internen Netzwerks oder geschützt durch eine Edgefirewall oder ein anderes Gerät bereitgestellt werden.
- Wird der RAS-Server durch eine Edgefirewall oder ein NAT-Gerät geschützt, muss das Gerät so konfiguriert sein, dass ein- und ausgehender Datenverkehr für den RAS-Server zugelassen wird.
- Die Person, die den Remotezugriff auf dem Server einrichtet, muss lokale Administratorberechtigungen für den Server und Benutzerberechtigungen für die Domäne besitzen. Zusätzlich benötigt der Administrator Berechtigungen für die Gruppenrichtlinien, die bei der DirectAccess-Bereitstellung verwendet werden. Um die Features nutzen zu können, die die DirectAccess-Bereitstellung auf mobile Computer beschränken, ist die Berechtigung zum Erstellen von WMI-Filtern für den Domänencontroller erforderlich.

### Remote Zugriffs-Client Anforderungen

- DirectAccess-Clients müssen Domänenmitglieder sein. Domänen, die Clients beinhalten, können zur selben Gesamtstruktur gehören wie der RAS-Server, oder sie können eine bidirektionale Vertrauensstellung mit dem RAS-Server und der Domäne innehaben.
- Eine Active Directory-Sicherheitsgruppe wird benötigt, um die Computer aufzunehmen, die als DirectAccess-Clients konfiguriert werden. Wird beim Konfigurieren der DirectAccess-Cienteinstellungen keine Sicherheitsgruppe angegeben, wird das Client-Gruppenrichtlinienobjekt standardmäßig auf alle Laptopcomputer (die DirectAccess-fähig sind) in der Sicherheitsgruppe "Domänencomputer" angewendet. Nur die folgenden Betriebssysteme können als DirectAccess-Clients verwendet werden: Windows Server 2012, Windows Server 2008 R2, Windows 8 Enterprise, Windows 7 Enterprise und Windows 7 Ultimate.

#### **NOTE**

Es wird empfohlen, für jede Domäne eine Sicherheitsgruppe zu erstellen, die Computer enthält, die als DirectAccess-Clients konfiguriert werden.

# Plan zum Aktivieren von DirectAccess

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

**Hinweis:** Windows Server 2012 kombiniert DirectAccess und RAS-Dienst (RAS) zu einer einzigen Remote Zugriffs Rolle. In diesem Abschnitt werden die Planungsschritte beschrieben, die zum Bereitstellen eines einzelnen RAS-Servers erforderlich sind, auf dem Windows Server 2016 mit grundlegenden Features ausgeführt wird.

Die Planungsphase umfasst die folgenden Schritte:

- [Schritt 1: Planen der DirectAccess-Infrastruktur](#)

In dieser Phase beschreiben Sie die erforderliche Planung zum Einrichten der Netzwerkinfrastruktur, bevor Sie mit der Remotezugriffbereitstellung beginnen. Sie umfasst das Planen der Netzwerk- und Servertopologie, Zertifikate, des Domain Name System (DNS), der Active Directory, die Konfiguration der Gruppenrichtlinienobjekte und des DirectAccess-Netzwerkadressenservers.

- [Schritt 2: Planen der DirectAccess-Bereitstellung](#)

In dieser Phase beschreiben Sie die erforderlichen Planungsschritte zur Vorbereitung der Remotezugriffbereitstellung. Dazu gehört die Planung der Clientcomputer für den Remotezugriff, Server- und Clientauthentifizierungsanforderungen und Infrastrukturserver.

# Schritt 1 Planen der DirectAccess-Infrastruktur

09.04.2020 • 34 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Der erste Schritt bei der Planung einer einfachen Remotezugriffsbereitstellung auf einem einzelnen Server ist die Planung der Infrastruktur, welche für die Bereitstellung erforderlich ist. In diesem Thema werden die Schritte zur Planung der Infrastruktur beschrieben:

AUFGABE	BESCHREIBUNG
Planen der Netzwerktopologie und -einstellungen	Entscheiden Sie über den Standort des Remotezugriffsservers (Edge oder hinter einem NAT-Gerät oder einer Firewall), und planen Sie die IP-Adressenvergabe und das Routing.
Planen der Firewallanforderungen	Planen Sie, den Remotezugriff über Edge-Firewalls zuzulassen.
Planen der Zertifikatanforderungen	Der Remotezugriff kann Kerberos oder Zertifikate zur Clientauthentifizierung verwenden. In dieser einfachen Remotezugriffsbereitstellung wird Kerberos automatisch konfiguriert und die Authentifizierung erfolgt mithilfe eines automatisch vom Remotezugriffsserver ausgestellten selbstsignierten Zertifikats.
Planen der DNS-Anforderungen	Planen der DNS-Einstellungen für den Remotezugriffsserver, die Infrastrukturserver, die Optionen für die lokale Namensauflösung und die Clientkonnektivität.
Planen von Active Directory	Planen Sie Ihre Domänencontroller und die Active Directory-Anforderungen.
Planen von Gruppenrichtlinienobjekten	Entscheiden Sie, welche Gruppenrichtlinienobjekte in Ihrer Organisation erforderlich sind und wie diese erstellt oder bearbeitet werden.

Diese Planungsaufgaben müssen nicht in einer bestimmten Reihenfolge durchgeführt werden.

## Planen der Netzwerktopologie und -einstellungen

### Planen von Netzwerkadapters und IP-Adressierung

1. Identifizieren Sie die Netzwerkadaptertopologie, die Sie verwenden möchten. der Remotezugriff kann mit folgenden Optionen eingerichtet werden:

- Mit zwei Netzwerkadapters: entweder am Edge mit einem Netzwerkadapter, der mit dem Internet verbunden ist, und der andere mit dem internen Netzwerk oder hinter einem NAT-, Firewall-oder Routergerät, wobei ein Netzwerkadapter mit einem Umkreis Netzwerk und der andere mit dem internen Netzwerk verbunden ist. Netzwerk.
- Hinter einem NAT-Gerät mit einem Netzwerkadapter: der Remote Zugriffs Server wird hinter einem NAT-Gerät installiert, und der einzige Netzwerkadapter wird mit dem internen Netzwerk verbunden.

2. Identifizieren Sie Ihre IP-Adressierungsanforderungen:

DirectAccess verwendet IPv6 mit IPsec, um eine sichere Verbindung zwischen DirectAccess-Clientcomputern und dem internen Unternehmensnetzwerk herzustellen. Jedoch erfordert DirectAccess nicht unbedingt Konnektivität mit dem IPv6-Internet oder nativen IPv6-Support auf internen Netzwerken. Stattdessen konfiguriert und verwendet es automatisch IPv6-Übergangstechnologien, um IPv6-Datenverkehr durch das IPv4-Internet (durch die Verwendung von 6to4, Teredo oder IP-HTTPS) und durch Ihr nur-IPv4-Intranet (durch die Verwendung von NAT64 oder ISATAP) zu tunnen. Eine Übersicht über diese Übergangstechnologien finden Sie in folgenden Ressourcen:

- [IPv6-Übergangs Technologien](#)
- [IP-HTTPS-tunnelingprotokollspezifikation](#)

3. Konfigurieren Sie erforderliche Adapter und Adressen entsprechend folgender Tabelle. Bei bereit Stellungen hinter einem NAT-Gerät mit einem einzelnen Netzwerkadapter sollten Sie Ihre IP-Adressen nur mit der Spalte "interner Netzwerkadapter" konfigurieren.

IP ADDRESS TYPE	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv4-Intranet und IPv4-Internet	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>-Eine statische öffentliche IPv4-Adresse mit den entsprechenden Subnetzmasken.</li> <li>-Eine Standard-Gateway-IPv4-Adresse Ihres Internet Firewall-oder lokalen Internetdienstanbieter-Routers (ISP).</li> </ul>	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>: Eine IPv4-Intranetadresse mit der entsprechenden Subnetzmaske.</li> <li>: Ein Verbindungs spezifisches DNS-Suffix des Intranetnamespaces. Zudem sollte der DNS-Server auf der internen Schnittstelle konfiguriert werden.</li> <li>-Konfigurieren Sie kein Standard Gateway auf Intranetschnittstellen.</li> </ul>	<p>Gehen Sie wie folgt vor, um den Remotezugriffsserver so zu konfigurieren, dass er alle Subnetze auf dem internen IPv4-Netzwerk erreicht:</p> <ol style="list-style-type: none"> <li>1. Listen Sie die IPv4-Adressbereiche für alle Speicherorte im Intranet auf.</li> <li>2. verwenden Sie die Befehle <b>Route Add-p</b> oder <b>Netsh Interface IPv4 Add Route</b>, um die IPv4-Adressbereiche als statische Routen in der IPv4-Routing Tabelle des Remote Zugriffs Servers hinzuzufügen.</li> </ol>

IP ADDRESS TYPE	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv6-Internet und IPv6-Intranet	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>-Verwenden Sie die automatisch konfigurierte Adress Konfiguration, die von Ihrem ISP bereitgestellt wird.</li> <li>Verwenden Sie den Befehl <b>Route Print</b>, um sicherzustellen, dass in der IPv6-Routing Tabelle eine IPv6-Standardroute vorhanden ist, die auf den ISP-Router zeigt.</li> <li>: Bestimmen Sie, ob der ISP-und der Intranetrouter in RFC 4191 beschriebene Standard Router-Einstellungen verwenden, und verwenden Sie eine höhere Standardeinstellung als ihre lokalen Intranetrouter. Wenn beide Fälle zutreffen, ist keine weitere Konfiguration für die Standardroute erforderlich.</li> <li>Die höhere Präferenz für den ISP-Router stellt sicher, dass die aktive IPv6-Standardroute des Remotezugriffsservers auf das IPv6-Internet zeigt.</li> </ul> <p>Wenn Sie über eine systemeigene IPv6-Infrastruktur verfügen, kann die Internetschnittstelle außerdem auch die Domänencontroller im Intranet erreichen, da der DirectAccess-Server ein IPv6-Router ist. Fügen Sie in diesem Fall Paketfilter zum Domänencontroller im Umkreisnetzwerk hinzu, die Konnektivität zur IPv6-Adresse der Internetschnittstelle des DirectAccess-Servers verhindern.</p>	<p>Konfigurieren Sie Folgendes:</p> <ul style="list-style-type: none"> <li>Wenn Sie keine Standard Einstellungsebenen verwenden, konfigurieren Sie Ihre Intranetschnittstellen mit dem Befehl <b>Netsh Interface IPv6 Set interfaceindex ignoredefaultroutes = aktiviert</b>. Dieser Befehl stellt sicher, dass der IPv6-Routingtabelle keine weiteren Standardrouten hinzugefügt werden, die auf Intranetrouter zeigen. Den SchnittstellenIndex Ihrer Intranetschnittstellen können Sie mit dem Befehl <b>netsh interface show interface</b> anzeigen.</li> </ul>	<p>Wenn Sie ein IPv6-Intranet haben, führen Sie folgende Schritte aus, um den Remotezugriffsserver so zu konfigurieren, dass er alle IPv6-Speicherorte erreicht:</p> <ol style="list-style-type: none"> <li>1. Listen Sie die IPv6-Adressräume für alle Speicherorte im Intranet auf.</li> <li>2. verwenden Sie den Befehl <b>Netsh Interface IPv6 Add Route</b>, um die IPv6-Adressbereiche als statische Routen in der IPv6-Routing Tabelle des Remote Zugriffs Servers hinzuzufügen.</li> </ol>

IP ADDRESS TYPE	EXTERNER NETZWERKADAPTER	INTERNER NETZWERKADAPTER	ROUTINGANFORDERUNGEN
IPv6-Internet und IPv4-Intranet	<p>Der Remotezugriffsserver leitet den Datenverkehr für die Standard-IPv6-Route mit dem Microsoft-IP6-zu-IP4-Adapter an ein IP6-zu-IP4-Relay im IPv4-Internet weiter. Sie können einen Remotezugriffsserver für die IPv4-Adresse des Microsoft-IP6-zu-IP4-Relays im IPv4-Internet (wird verwendet, wenn die systemeigene IPv6 nicht im Unternehmensnetzwerk bereitgestellt wird) mit dem Befehl "netsh interface ipv6 6to4 set relay name=192.88.99.1 state=enabled" konfigurieren.</p>		

#### NOTE

1. Wenn dem DirectAccess-Client eine öffentliche IPv4-Adresse zugewiesen wurde, verwendet diese die IP6-zu-IP4-Übergangstechnologie für die Verbindung mit dem Internet. Wenn der DirectAccess-Client mit IP6-zu-IP4 keine Verbindung mit dem DirectAccess-Server herstellen kann, wird IP-HTTPS verwendet.
2. Systemeigene IPv6-Clientcomputer können über eine systemeigene IPv6 eine Verbindung zum Remotezugriffsserver herstellen, und es ist keine Übergangstechnologie erforderlich.

#### Planen der Firewallanforderungen

Wenn sich der Remotezugriffsserver hinter einer Edge-Firewall befindet, sind folgende Ausnahmen für Remotezugriff-Datenverkehr erforderlich, wenn sich der Remotezugriffsserver auf dem IPv4-Internet befindet:

- IPv6-zu-IPv4-Datenverkehr-IP-Protokoll 41 eingehend und ausgehend.
- IP-HTTPS-TCP (Transmission Control Protocol)-Zielport 443 und TCP-Quellport 443 ausgehend.
- Wenn Sie den Remotezugriff mit einem einzigen Netzwerkadapter bereitstellen und den Netzwerkadressenserver auf dem Remotezugriffsserver installieren, sollte TCP-Port 62000 ebenfalls ausgenommen werden.

Die folgenden Ausnahmen sind für Remotezugriff-Datenverkehr erforderlich, wenn sich der Remotezugriffsserver auf dem IPv6-Internet befindet:

- IP-Protokoll 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend.

Wenden Sie bei zusätzlichen Firewalls die folgenden internen Netzwerkfirewallausnahmen für RAS-Datenverkehr an:

- ISATAP-Protokoll 41 eingehend und ausgehend
- TCP/UDP für den gesamten IPv4/IPv6-Datenverkehr

#### Planen der Zertifikatanforderungen

Zertifikatanforderungen für IPsec beinhalten ein Computerzertifikat, das von DirectAccess-Clientcomputern

verwendet wird, wenn diese die IPsec-Verbindung zwischen dem Client und dem Remotezugriffsserver herstellen, und einem Computerzertifikat, das von Remotezugriffsservern für das Herstellen von IPsec-Verbindungen mit DirectAccess-Clients verwendet wird. Für DirectAccess in Windows Server 2012 ist die Verwendung dieser IPsec-Zertifikate nicht obligatorisch. Der Assistent für erste Schritte konfiguriert den Remotezugriffsserver als Kerberos-Proxy, damit die IPsec-Authentifizierung ohne erforderliche Zertifikate durchgeführt werden kann.

1. **IP-HTTPS-Server:** Wenn Sie den Remote Zugriff konfigurieren, wird der Remote Zugriffs Server automatisch als IP-HTTPS-Weblistener konfiguriert. Die IP-HTTPS-Website erfordert ein Websitezertifikat, und Clientcomputer müssen in der Lage sein, die CRL-Website (Certificate Revocation List, Zertifikatsperrlisten) für das Zertifikat zu kontaktieren. Der Assistent zum Aktivieren von DirectAccess versucht, das SSTP VPN-Zertifikat zu verwenden. Wenn SSTP nicht konfiguriert ist, prüft er, ob im persönlichen Speicher des Computers ein Zertifikat für IP-HTTPS vorhanden ist. Wenn kein Zertifikat verfügbar ist, erstellt er automatisch ein selbstsigniertes Zertifikat.
2. **Netzwerkadressen Server:** der Netzwerkadressen Server ist eine Website, mit der erkannt wird, ob sich Client Computer im Unternehmensnetzwerk befinden. Der Netzwerkadressenserver erfordert ein Websitezertifikat. DirectAccess-Clients müssen die CRL-Website für das Zertifikat kontaktieren können. Der Assistent zum Aktivieren von DirectAccess prüft, ob im persönlichen Speicher des Computers ein Zertifikat für den Netzwerkadressenserver vorhanden ist. Wenn kein Zertifikat verfügbar ist, erstellt er automatisch ein selbstsigniertes Zertifikat.

Die einzelnen Zertifikatanforderungen werden in der folgenden Tabelle zusammengefasst:

IPSEC-AUTHENTIFIZIERUNG	IP-HTTPS-SERVER	NETZWERKADRESSEN SERVER
Eine interne Zertifizierungsstelle ist erforderlich, um Computer Zertifikate für den RAS-Server und Clients für die IPsec-Authentifizierung auszugeben, wenn Sie den Kerberos-Proxy nicht für die Authentifizierung verwenden.	Öffentliche Zertifizierungsstelle: Es wird empfohlen, eine öffentliche Zertifizierungsstelle zum Ausstellen des IP-HTTPS-Zertifikats zu verwenden. Dadurch wird sichergestellt, dass der CRL-Verteilungs Punkt extern verfügbar ist.	Interne Zertifizierungsstelle: Sie können eine interne Zertifizierungsstelle verwenden, um das Netzwerkadressen Server-Website Zertifikat auszustellen. Stellen Sie sicher, dass der Sperrlisten-Verteilungspunkt eine hohe Verfügbarkeit vom internen Netzwerk aus hat.
	Interne Zertifizierungsstelle: Sie können eine interne Zertifizierungsstelle zum Ausstellen des IP-HTTPS-Zertifikats verwenden. Sie müssen jedoch sicherstellen, dass der CRL-Verteilungs Punkt extern verfügbar ist.	Selbst signiertes Zertifikat: Sie können ein selbst signiertes Zertifikat für die Netzwerkadressen Server-Website verwenden. In bereit Stellungen mit mehreren Standorten können Sie jedoch kein selbst signiertes Zertifikat verwenden.
	Selbst signiertes Zertifikat: Sie können ein selbst signiertes Zertifikat für den IP-HTTPS-Server verwenden; Sie müssen jedoch sicherstellen, dass der CRL-Verteilungs Punkt extern verfügbar ist. Ein selbstsigniertes Zertifikat kann nicht in Bereitstellungen für mehrere Standorte verwendet werden.	

#### Planen von Zertifikaten für IP-HTTPS

Der Remotezugriffsserver fungiert als IP-HTTPS-Listener, und Sie müssen manuell ein HTTPS-Websitezertifikat auf dem Server installieren. Beachten Sie Folgendes bei der Planung:

- Die Verwendung einer öffentlichen Zertifizierungsstelle wird empfohlen, damit Zertifikatsperrlisten schneller verfügbar sind.
- Geben Sie im Feld Antragsteller die IPv4-Adresse des Internetadapters des Remotezugriffsservers oder die

FQDN der IP-HTTPS-URL an (die ConnectTo-Adresse). Falls sich der Remotezugriffsserver hinter einem NAT-Gerät befindet, sollte der öffentliche Name oder die Adresse des NAT-Geräts angegeben werden.

- Der allgemeine Name des Zertifikats sollte dem Namen der IP-HTTPS-Website entsprechen.
- Geben Sie im Feld "Erweiterte Schlüsselverwendung" die Serverauthentifizierungs-Objektkennung (OID) an.
- Geben Sie im Feld "Sperrlisten-Verteilungspunkte" einen Zertifikatsperrlisten-Verteilungspunkt an, auf den mit dem Internet verbundene DirectAccess-Clients zugreifen können.
- Das IP-HTTPS-Zertifikat muss einen privaten Schlüssel enthalten.
- Das IP-HTTPS-Zertifikat muss direkt in den persönlichen Speicher importiert werden.
- Die Namen von IP-HTTPS-Zertifikaten können Platzhalter enthalten.

#### Planen von Websitezertifikaten für den Netzwerkadressenserver

Beachten Sie bei der Planung der Netzwerkadressenserver-Website Folgendes:

- Im Feld Antragsteller muss eine IP-Adresse der Intranetschnittstelle des Netzwerkadressenservers oder der FQDN der Netzwerkadressen-URL angegeben sein.
- Im Feld Erweiterte Schlüsselverwendung muss die Serverauthentifizierungs-OID angegeben sein.
- Im Feld Sperrlisten-Verteilungspunkte muss ein Zertifikatsperrlisten-Verteilungspunkt angegeben sein, auf den mit dem Intranet verbundene DirectAccess-Clients zugreifen können. Der Zertifikatsperrlisten-Verteilungspunkt sollte nicht von außerhalb des internen Netzwerks zugänglich sein.
- Wenn Sie zu einem späteren Zeitpunkt eine Bereitstellung für mehrere Standorte oder im Cluster planen, sollte der Name des Zertifikats nicht dem internen Namen des Remotezugriffsservers entsprechen.

#### NOTE

Stellen Sie sicher, dass die Zertifikate für IP-HTTPS und den Netzwerkadressenserver einen **Antragstellernamen** haben. Wenn das Zertifikat keinen **Antragstellername**, aber einen **Alternativen Antragstellernamen** hat, wird es nicht vom RAS-Assistenten akzeptiert.

#### Planen der DNS-Anforderungen

In einer Remotezugriffbereitstellung ist DNS für Folgendes erforderlich:

- **DirectAccess-Client Anforderungen:** DNS wird verwendet, um Anforderungen von DirectAccess-Client Computern aufzulösen, die sich nicht im internen Netzwerk befinden. DirectAccess-Clients versuchen, eine Verbindung zum DirectAccess-Netzwerkadressenserver herzustellen, um zu bestimmen, ob sie sich im Internet oder auf dem internen Netzwerk befinden: Bei erfolgreicher Verbindung werden die Clients als im Intranet befindlich identifiziert, DirectAccess wird nicht verwendet, und Clientanforderungen werden mithilfe des DNS-Servers aufgelöst, welcher auf dem Netzwerkadapter des Clientcomputers konfiguriert ist. Wenn keine Verbindung hergestellt werden kann, wird davon ausgegangen, dass sich die Clients im Internet befinden. DirectAccess-Clients verwenden die Richtlinientabelle für die Namensauflösung, um zu ermitteln, welcher DNS-Server beim Auflösen von Namensanforderungen verwendet werden soll. Sie können angeben, dass Clients DirectAccess-DNS64 oder einen anderen internen DNS-Server für die Auflösung von Namen verwenden. Wenn Sie eine Namensauflösung durchführen, wird die NRPT von DirectAccess-Clients verwendet, um festzulegen, wie eine Anfrage behandelt werden soll. Clients fordern einen voll qualifizierten Namen oder einen Namen mit einer einzelnen Bezeichnung an, z. B. <https://internal>. Wenn ein Name mit einer einzelnen Bezeichnung angefordert wird, wird ein DNS-Suffix angehängt, um einen FQDN zu bilden. Wenn die DNS-Abfrage einem Eintrag in der NRPT entspricht, und DNS4 oder ein Intranet-DNS-Server für den Eintrag angegeben wurde, wird die Abfrage für die Namensauflösung mithilfe des angegebenen Servers

gesendet. Wenn eine Übereinstimmung vorhanden ist, aber kein DNS-Server angegeben wurde, weist dies auf eine Ausnahmeregel hin, und die normale Namensauflösung wird verwendet.

Wenn ein neues Suffix zur NRPT in der Remotezugriffs-Verwaltungskonsole hinzugefügt wird, können die Standard-DNS-Server für das Suffix automatisch erkannt werden, wenn Sie auf **Erkennen** klicken. Die automatische Erkennung funktioniert wie folgt:

1. Wenn das Unternehmensnetzwerk IPv4-basiert ist oder IPv4 und IPv6 verwendet, ist die Standardadresse die DNS64-Adresse des internen Adapters auf dem Remotezugriffsserver.
2. Wenn das Unternehmensnetzwerk IPv6-basiert ist, ist die Standardadresse die IPv6-Adresse der DNS-Server auf dem Unternehmensnetzwerk.

- **Infrastruktur Server**

1. **Netzwerkadressen Server:** DirectAccess-Clients versuchen, den Netzwerkadressen Server zu erreichen, um zu ermitteln, ob Sie sich im internen Netzwerk befinden. Clients im internen Netzwerk müssen in der Lage sein, den Namen des Netzwerkadressenservers aufzulösen, befinden sie sich jedoch im Internet, dürfen sie den Namen nicht auflösen. Um dies zu gewährleisten, wird der FQDN des Netzwerkadressenservers standardmäßig als Ausnahmeregel zum NRPT hinzugefügt. Außerdem werden bei der Konfiguration von RAS folgende Regeln automatisch erstellt:

- a. Eine DNS-Suffixregel für die Stammdomäne oder den Domänennamen des Remotezugriffsservers und die IPv6-Adressen, die den auf dem Remotezugriffsserver konfigurierten Intranet-DNS-Servern entsprechen. Wenn der Remotezugriffsserver z. B. Mitglied der Domäne corp.contoso.com ist, wird für das DNS-Suffix .corp.contoso.com eine Regel erstellt.
- b. Eine Ausnahmeregel für den FQDN des Netzwerkadressenservers. Wenn die Netzwerkadressen Server-URL z. b. <https://nls.corp.contoso.com> ist, wird eine Ausnahme Regel für den voll qualifizierten Namen (NLS.Corp.contoso.com) erstellt.

**IP-HTTPS-Server:** der RAS-Server fungiert als IP-HTTPS-Listener und verwendet das Serverzertifikat zur Authentifizierung bei IP-HTTPS-Clients. Der IP-HTTPS-Name muss von den DirectAccess-Clients mit den öffentlichen DNS-Servern aufgelöst werden können.

**Konnektivitätsverifizierer:** der Remote Zugriff erstellt einen Standard-Webtest, der von DirectAccess-Client Computern verwendet wird, um die Konnektivität zum internen Netzwerk zu überprüfen. Damit der Test wie erwartet funktioniert, müssen folgende Namen manuell in dem DNS registriert werden:

- a. DirectAccess-WebProbe Host sollte in die interne IPv4-Adresse des RAS-Servers oder die IPv6-Adresse in einer reinen IPv6-Umgebung aufgelöst werden.
- b. DirectAccess-corpconnectivityhost sollte in die localhost-Adresse (Loopback) aufgelöst werden. Ein A- und AAAA-Eintrag sollte erstellt werden, der A-Eintrag mit dem Wert 127.0.0.1 und der AAAA-Eintrag mit dem aus dem NAT64-Präfix und den letzten 32-Bit als 127.0.0.1 ermittelten Wert. Das NAT64-Präfix kann durch Ausführen des Cmdlets "get-netnattransitionconfiguration" abgerufen werden.

**NOTE**

Dies gilt nur in einer IPv4-Umgebung. In einer Umgebung mit IPv4 plus IPv6 oder in einer reinen IPv6-Umgebung sollte nur ein (AAAA)-Ressourceneintrag mit der Loopback-IP-Adresse ::1 erstellt werden.

Mithilfe anderer Webadressen über HTTP oder PING können Sie weitere Verbindungsprüfer erstellen.

Für jeden Verbindungsprüfer muss ein DNS-Eintrag vorhanden sein.

#### DNS-Serveranforderungen

- Für DirectAccess-Clients müssen Sie entweder einen DNS-Server mit Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 oder einen beliebigen DNS-Server verwenden, der IPv6 unterstützt.

#### Planen von Active Directory

Der Remote Zugriff verwendet Active Directory und Active Directory Gruppenrichtlinie Objekte wie folgt:

- **Authentifizierung:** Active Directory wird für die Authentifizierung verwendet. Der Intranettunnel verwendet für den Benutzer die Kerberos-Authentifizierung, um auf interne Ressourcen zuzugreifen.
- **Gruppenrichtlinien Objekte:** der Remote Zugriff sammelt Konfigurationseinstellungen in Gruppenrichtlinien Objekten, die auf RAS-Server, Clients und interne Anwendungsserver angewendet werden.
- **Sicherheitsgruppen:** der Remote Zugriff verwendet Sicherheitsgruppen, um DirectAccess-Client Computer und Remote Zugriffs Server zu erfassen und zu identifizieren. Die Gruppenrichtlinien werden auf die erforderlichen Sicherheitsgruppen angewendet.
- **Erweiterte IPSec-Richtlinien:** der Remote Zugriff kann die IPSec-Authentifizierung und-Verschlüsselung zwischen Clients und dem RAS-Server verwenden. Sie können die IPsec-Authentifizierung und - Verschlüsselung durch die angegebenen, internen Anwendungsserver erweitern.

#### Active Directory-Anforderungen

Bei der Planung von Active Directory für eine Remotezugriffbereitstellung ist Folgendes erforderlich:

- Mindestens ein Domänen Controller muss auf den Betriebssystemen Windows Server 2012, Windows Server 2008 R2 Windows Server 2008 oder Windows Server 2003 installiert sein.

Wenn sich der Domänencontroller in einem Umkreisnetzwerk befindet (und deshalb von einem Netzwerkadapter mit Internetzugriff des Remotezugriffsservers aus erreichbar ist), müssen Sie verhindern, dass der Remotezugriffsserver den Domänencontroller erreicht, indem Sie dem Domänencontroller Paketfilter hinzufügen, damit die Konnektivität zur IP-Adresse des Internetadapters unterbunden wird.
- Der Remotezugriffsserver muss Domänenmitglied sein.
- DirectAccess-Clients müssen Domänenmitglieder sein. Clients können folgenden Domänen angehören:
  - Domänen, die zur gleichen Gesamtstruktur wie der Remotezugriffsserver gehören.
  - Domänen mit bidirektonaler Vertrauensstellung zur Remotezugriffsserverdomäne.
  - Domänen in einer Gesamtstruktur mit bidirektonaler Vertrauensstellung zu der Gesamtstruktur, der die Remotezugriffdomäne angehört.

#### NOTE

- Der Remotezugriffsserver kann nicht als Domänencontroller verwendet werden.
- Der für den Remotezugriff verwendete Active Directory-Domänencontroller darf nicht von einem externen Internetadapter des Remotezugriffsservers aus erreichbar sein (der Adapter darf sich nicht im Domänenprofil der Windows-Firewall befinden).

#### Planen von Gruppenrichtlinienobjekten

Die bei der Konfiguration des Remotezugriffs konfigurierten DirectAccess-Einstellungen werden in gpos (GPO) erfasst. Die drei Gruppenrichtlinienobjekte werden mit DirectAccess-Einstellungen aufgefüllt und wie folgt verteilt:

- **DirectAccess-Client**-Gruppenrichtlinien Objekt: dieses Gruppenrichtlinien Objekt enthält Client Einstellungen, einschließlich der IPv6-Übergangstechnologie Einstellungen, NRPT-Einträge und der Verbindungs Sicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit. Das Gruppenrichtlinienobjekt wird auf die für die Clientcomputer angegebenen Sicherheitsgruppen angewendet.
- **DirectAccess-Server**-Gruppenrichtlinien Objekt: dieses Gruppenrichtlinien Objekt enthält die DirectAccess-Konfigurationseinstellungen, die auf jeden als RAS-Server konfigurierten Server in Ihrer Bereitstellung angewendet werden. Außerdem enthält es die Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit.
- **Anwendungsserver**-Gruppenrichtlinien Objekt: dieses Gruppenrichtlinien Objekt enthält Einstellungen für ausgewählte Anwendungsserver, auf die Sie optional die Authentifizierung und Verschlüsselung von DirectAccess-Clients erweitern können. Wenn die Authentifizierung und die Verschlüsselung nicht erweitert werden, wird dieses Gruppenrichtlinienobjekt nicht verwendet.

Gruppenrichtlinienobjekte werden automatisch vom Assistenten zum Aktivieren von DirectAccess erstellt und jedes Gruppenrichtlinienobjekt erhält einen Standardnamen.

**Caution**

Verwenden Sie folgendes Verfahren, um alle Remotezugriff-Gruppenrichtlinienobjekte zu sichern, bevor Sie die DirectAccess-Cmdlets ausführen: [Sichern und Wiederherstellen der Remotezugriffskonfiguration](#)

Es gibt zwei Möglichkeiten, Gruppenrichtlinienobjekte zu konfigurieren:

1. **Automatisch**: Sie können angeben, dass Sie automatisch erstellt werden. Für jedes Gruppenrichtlinienobjekt wird ein Standardname angegeben.
2. **Manuell**: Sie können GPOs verwenden, die vom Active Directory-Administrator vordefiniert wurden.

Beachten Sie, dass keine anderen Gruppenrichtlinienobjekte mehr konfiguriert werden können, nachdem DirectAccess auf die Verwendung bestimmter Gruppenrichtlinienobjekte konfiguriert wurde.

**Automatisch erstellte Gruppenrichtlinienobjekte**

Beachten Sie beim Verwenden automatisch erstellter Gruppenrichtlinienobjekte Folgendes:

Automatisch erstellte Gruppenrichtlinienobjekte werden entsprechend des Speicherorts und Verknüpfungszielparameters wie folgt angewendet:

- Bei Gruppenrichtlinienobjekten des DirectAccess-Servers zeigen der Speicherort und die Verknüpfungsparameter auf die Domäne, die den Remotezugriffsserver enthält.
- Beim Erstellen der Gruppenrichtlinienobjekte wird der Speicherort auf eine Domäne festgelegt, auf der das Gruppenrichtlinienobjekt erstellt wird. Der Gruppenrichtlinienobjektname wird in jeder Domäne nachgeschlagen und mit DirectAccess-Einstellungen aufgefüllt, falls vorhanden. Das Verknüpfungsziel wird auf den Stamm der Domäne festgelegt, in der das Gruppenrichtlinienobjekt erstellt wurde. Für jede Domäne, die Clientcomputer oder Anwendungsserver enthält, wird ein Gruppenrichtlinienobjekt erstellt, und das Gruppenrichtlinienobjekt wird mit dem Stamm der entsprechenden Domäne verknüpft.

Beim Verwenden automatisch erstellter Gruppenrichtlinienobjekte benötigt der DirectAccess-Serveradministrator zum Anwenden der DirectAccess-Einstellungen folgende Berechtigungen:

- Schreibberechtigungen für die Gruppenrichtlinienobjekte für jede Domäne.
- Verknüpfungsberechtigungen für alle ausgewählten Clientdomänenstämme.
- Verknüpfungsberechtigungen für die Server-Gruppenrichtlinien-Domänenstämme.
- Erstellen, Bearbeiten und Löschen von Sicherheitsberechtigungen, die für die Gruppenrichtlinienobjekte erforderlich sind.

- Es wird empfohlen, dass der Remotezugriffsadministrator über Leserechte für Gruppenrichtlinienobjekte für jede Domäne verfügt. So kann der Remotezugriff prüfen, dass beim Erstellen von Gruppenrichtlinienobjekten keine Gruppenrichtlinienobjekte mit doppelten Namen vorhanden sind.

Beachten Sie, dass eine Warnung ausgegeben wird, wenn die korrekten Berechtigungen zum Verknüpfen der Gruppenrichtlinienobjekte nicht vorhanden sind. Der Remotezugriffsvorgang wird fortgesetzt, Verknüpfungen werden jedoch nicht erstellt. Wenn diese Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, selbst wenn die Berechtigungen eingerichtet sind. Stattdessen muss der Administrator die Links manuell erstellen.

#### **Manuell erstellte Gruppenrichtlinienobjekte**

Beachten Sie beim Verwenden manuell erstellter Gruppenrichtlinienobjekte Folgendes:

- Die Gruppenrichtlinienobjekte sollten vorhanden sein, bevor Sie den Remotezugriffs-Setup-Assistenten ausführen.
- Beim Verwenden manuell erstellter Gruppenrichtlinienobjekte muss der Remotezugriffsadministrator in den manuell erstellten Gruppenrichtlinienobjekten über uneingeschränkte Berechtigungen für die Gruppenrichtlinienobjekte verfügen (Bearbeiten, Löschen, Ändern der Sicherheit).
- Beim Verwenden manuell erstellter Gruppenrichtlinienobjekte wird in der gesamten Domäne eine Suche nach einer Verknüpfung zum Gruppenrichtlinienobjekt durchgeführt. Wenn das Gruppenrichtlinienobjekt in der Domäne nicht verknüpft ist, wird im Domänenstamm automatisch eine Verknüpfung erstellt. Wenn die zum Erstellen der Verknüpfung erforderlichen Berechtigungen nicht verfügbar sind, wird eine Warnung ausgegeben.

Beachten Sie, dass eine Warnung ausgegeben wird, wenn die korrekten Berechtigungen zum Verknüpfen der Gruppenrichtlinienobjekte nicht vorhanden sind. Der Remotezugriffsvorgang wird fortgesetzt, Verknüpfungen werden jedoch nicht erstellt. Wenn diese Warnung ausgegeben wird, werden Verknüpfungen nicht automatisch erstellt, selbst wenn die Berechtigungen zu einem späteren Zeitpunkt hinzugefügt werden. Stattdessen muss der Administrator die Links manuell erstellen.

#### **Wiederherstellen eines gelöschten Gruppenrichtlinienobjekts**

Wenn ein Gruppenrichtlinienobjekt eines Remotezugriffsservers, -clients oder Anwendungsservers versehentlich gelöscht wurde und keine Sicherung verfügbar ist, müssen Sie die Konfigurationseinstellungen entfernen und sie neu konfigurieren. Wenn eine Sicherung verfügbar ist, können Sie das Gruppenrichtlinienobjekt aus der Sicherung wiederherstellen.

Die **Remote Zugriffs Verwaltung** zeigt die folgende Fehlermeldung an: das Gruppenrichtlinien Objekt (**GPO-Name**) wurde nicht gefunden. Führen Sie folgende Schritte aus, um die Konfigurationseinstellungen zu entfernen:

1. Führen Sie das PowerShell-Cmdlet **Uninstall-remoteaccess** aus.
2. Öffnen Sie die **Remote Zugriffs Verwaltung** erneut.
3. In der angezeigten Fehlermeldung werden Sie darauf hingewiesen, dass das Gruppenrichtlinienobjekt nicht gefunden werden konnte. Klicken Sie auf **Konfigurationseinstellungen entfernen**. Nach Abschluss des Vorgangs wird der Server in einem nicht konfigurierten Zustand wiederhergestellt.

# Schritt 2 Planen der DirectAccess-Bereitstellung

09.04.2020 • 8 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Nach der Planung der Remotezugriffinfrastruktur besteht der nächste Schritt zur Aktivierung von DirectAccess darin, die Einstellungen zum Aktivieren des DirectAccess-Assistenten zu planen.

AUFGABE	BESCHREIBUNG
Planen der Clientbereitstellung	Planen Sie die Methode zum Verbinden der Clientcomputer mithilfe von DirectAccess. Legen Sie fest, welche verwalteten Computer als DirectAccess-Clients konfiguriert werden sollen.
Planen der Remotezugriffsserverbereitstellung	Planen Sie die Bereitstellung des Remotezugriffsservers.

## Planen der Client Bereitstellung

Bei der Planung Ihrer Clientbereitstellung müssen zwei Entscheidungen getroffen werden:

- Soll DirectAccess für alle oder nur für mobile Computer verfügbar sein?

Bei der Konfiguration der DirectAccess-Clients im Assistenten zum Aktivieren von DirectAccess können Sie auswählen, dass nur mobile Computer in den angegebenen Sicherheitsgruppen eine Verbindung über DirectAccess aufbauen können. Wenn Sie nur den Zugriff für mobile Computer zulassen, konfiguriert der Remotezugriff automatisch einen WMI-Filter, um sicherzustellen, dass das Gruppenrichtlinienobjekt des DirectAccess-Clients nur auf mobile Computer in den angegebenen Sicherheitsgruppen angewendet wird. Der Remotezugriffsadministrator benötigt Berechtigungen zum Erstellen oder Bearbeiten der WMI-Filter für die Gruppenrichtlinie, um diese Einstellung zu aktivieren.

- In welchen Sicherheitsgruppen sollen die DirectAccess-Clientcomputer enthalten sein?

Die DirectAccess-Einstellungen befinden sich in dem Gruppenrichtlinienobjekt des DirectAccess-Clients. Das Gruppenrichtlinienobjekt wird auf Computer angewendet, die in den Sicherheitsgruppen enthalten sind, die Sie in dem Assistenten zum Aktivieren von DirectAccess angegeben haben. Sie können angeben, dass Sicherheitsgruppen in einer beliebigen unterstützten Domäne enthalten sein sollen. Bevor Sie den Remotezugriff konfigurieren, sollten die Sicherheitsgruppen erstellt werden. Nach Abschluss der Remotezugriffsbereitstellung können Sie Computer zur Sicherheitsgruppe hinzufügen, wenn Sie jedoch Clientcomputer hinzufügen, die sich in einer anderen Domäne befinden wie die Sicherheitsgruppe, dann wird das Client-Gruppenrichtlinienobjekt nicht auf diese Clients angewendet. Wenn Sie beispielsweise SG1 in Domäne A für DirectAccess-Clients erstellen und später Clients von Domäne B zu dieser Gruppe hinzufügen, wird das Client-Gruppenrichtlinienobjekt nicht auf Clients von Domäne B angewendet. Sie können dieses Problem vermeiden, indem Sie eine neue Client-Sicherheitsgruppe für jede Domäne erstellen, die die Clientcomputer enthält. Alternativ dazu können Sie auch das Add-DAClient-Cmdlet mit dem Namen des neuen Gruppenrichtlinienobjekts für die neue Domäne ausführen, wenn Sie keine neuen Sicherheitsgruppe erstellen möchten.

## Planen der Bereitstellung des Remote Zugriffs Servers

Beim Planen der Bereitstellung Ihres Remotezugriffsservers müssen Sie mehrere Entscheidungen treffen:

- **Netzwerktopologie:** bei der Bereitstellung eines Remote Zugriffs Servers sind zwei Topologien verfügbar:
  - **Zwei Adapter:** mit zwei Netzwerkadapters kann der Remote Zugriff mit einem direkt mit dem Internet verbundenen Netzwerkadapter konfiguriert werden, während der andere mit dem internen Netzwerk verbunden ist. Alternativ kann der Server hinter einem Edgegerät installiert werden, wie z. B. einer Firewall oder einem Router. In dieser Konfiguration ist ein Netzwerkadapter mit dem Umkreisnetzwerk und der andere mit dem internen Netzwerk verbunden.
  - **Einzelner Netzwerkadapter:** in dieser Konfiguration wird der RAS-Server hinter einem Edgegerät wie z. b. einer Firewall oder einem Router installiert. Der Netzwerkadapter ist mit dem internen Netzwerk verbunden.
- **Netzwerkadapter:** der Assistent zum Aktivieren von DirectAccess erkennt automatisch die Netzwerkadapter, die auf dem RAS-Server konfiguriert sind, basierend auf den Schnittstellen, die von VPN verwendet werden. Vergewissern Sie sich, dass die richtigen Adapter ausgewählt sind.
- **ConnectTo-Adresse:** Client Computer verwenden die ConnectTo-Adresse, um eine Verbindung mit dem Remote Zugriffs Server herzustellen. Die von Ihnen gewählte Adresse muss mit dem Antragstellernamen des IP-HTTPS-Zertifikats übereinstimmen, das Sie für die IP-HTTPS-Verbindung bereitstellen. Außerdem muss sie im öffentlichen DNS verfügbar sein. Weitere Informationen finden Sie unter dem Thema Planen von Websitezertifikaten für IP-HTTPS.
- **IP-HTTPS-Zertifikat:** Wenn das SSTP-VPN konfiguriert ist, übernimmt der Assistent zum Aktivieren von DirectAccess das Zertifikat, das von SSTP für IP-HTTPS verwendet wird. Wenn SSTP-VPN nicht konfiguriert ist, versucht der Assistent zu ermitteln, ob ein Zertifikat für IP-HTTPS konfiguriert wurde. Falls das nicht der Fall ist, stellt der Assistent automatisch selbstsignierte Zertifikate für IP-HTTPS bereit. Außerdem aktiviert er automatisch die Kerberos-Authentifizierung. Außerdem aktiviert der Assistent NAT64 und DNS64 für die Protokollübersetzung in der auf IPv4 beschränkten Umgebung.
- **IPv6-Präfixe:** Wenn der Assistent erkennt, dass IPv6 auf den Netzwerkadapters bereitgestellt wurde, erstellt er automatisch IPv6-Präfixe für das interne Netzwerk, ein IPv6-Präfix, das DirectAccess-Client Computern zugewiesen werden soll, und ein IPv6-Präfix, das VPN-Client Computern zugewiesen werden soll. Wenn die automatisch generierten Präfixe nicht mit Ihrer systemeigenen IPv6- oder ISATAP-Infrastruktur übereinstimmen, müssen Sie sie manuell ändern. Weitere Informationen finden Sie unter 1.1 Planen der Netzwerk- und Servertopologie und -einstellungen.
- **Windows 7-Clients:** Windows 7-Client Computer können standardmäßig keine Verbindung mit einer Windows Server 2012-Remote Zugriffs Bereitstellung herstellen. Wenn Sie in Ihrer Organisation über Windows 7-Client Computer verfügen, die Remote Zugriff auf interne Ressourcen benötigen, können Sie eine Verbindung herstellen. Clientcomputer, die auf interne Ressourcen zugreifen sollen, müssen Mitglied einer Sicherheitsgruppe sein, die Sie im Assistenten zum Aktivieren von DirectAccess angeben.

**NOTE**

Damit Windows 7-Client Computer mithilfe von DirectAccess eine Verbindung herstellen können, müssen Sie die Computer Zertifikat Authentifizierung verwenden.

- **Authentifizierung:** der Assistent zum Aktivieren von DirectAccess verwendet Active Directory, um die Anmelde Informationen des Benutzers zu authentifizieren. Weitere Informationen zum Bereitstellen einer zweistufigen Authentifizierung finden Sie unter [Bereitstellen des Remotezugriffs mit OTP-Authentifizierung](#).

# Aktivieren von DirectAccess

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

Windows Server 2016 und Windows Server 2012 kombinieren DirectAccess-und RAS-VPN (RAS-Dienst) zu einer einzigen Remote Zugriffs Rolle. Diese Übersicht bietet eine Einführung in die Konfigurationsschritte, die erforderlich sind, um einen einzelnen Remote Zugriffs Server mit Windows Server 2016 oder Windows Server 2012 mit grundlegenden Einstellungen bereitzustellen.

- [Schritt 1: Konfigurieren der DirectAccess-Infrastruktur](#). Dieser Schritt umfasst die Konfiguration der Netzwerk- und Servereinstellungen sowie der DNS- und Active Directory-Einstellungen.
- [Schritt 2: Konfigurieren Sie den DirectAccess-VPN-Server](#). Dieser Schritt umfasst das Konfigurieren von DirectAccess-Client Computern und Servereinstellungen.
- [Schritt 3: Überprüfen Sie die Bereitstellung](#). Dieser Schritt umfasst die Schritte zum Überprüfen der Bereitstellung.

Bevor Sie mit der Bereitstellung beginnen, überprüfen Sie die Planungsschritte unter [Planen der Aktivierung von DirectAccess](#).

# Schritt 1 Konfigurieren der DirectAccess-Infrastruktur

09.04.2020 • 27 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie die erforderliche Infrastruktur zur Aktivierung von DirectAccess für eine vorhandene VPN-Bereitstellung konfigurieren. Vergewissern Sie sich vor Beginn der Bereitstellungs Schritte, dass Sie die in [Schritt 1: Planen der DirectAccess-Infrastruktur](#) beschriebenen Planungsschritte abgeschlossen haben.

AUFGABE	BESCHREIBUNG
Konfigurieren von Servernetzwerkeinstellungen	Konfigurieren Sie die Servernetzwerkeinstellungen auf dem Remotezugriffsserver.
Konfigurieren des Routings im Unternehmensnetzwerk	Konfigurieren Sie das Routing im Unternehmensnetzwerk, damit der Datenverkehr ordnungsgemäß weitergeleitet wird.
Konfigurieren von Firewalls	Konfigurieren Sie bei Bedarf zusätzliche Firewalls.
Konfigurieren von Zertifizierungsstellen und Zertifikaten	Der Assistent zum Aktivieren von DirectAccess konfiguriert einen integrierten Kerberos-Proxy, der die Authentifizierung anhand der Benutzernamen und Kennwörter vornimmt. Außerdem konfiguriert er ein IP-HTTPS-Zertifikat auf dem Remotezugriffsserver.
Konfigurieren des DNS-Servers	Konfigurieren Sie DNS-Einstellungen für den Remotezugriffsserver.
Konfigurieren von Active Directory	Fügen Sie der Active Directory-Domäne Clientcomputer hinzu.
Konfigurieren der Gruppenrichtlinienobjekte	Konfigurieren Sie bei Bedarf Gruppenrichtlinienobjekte für die Bereitstellung.
Konfigurieren von Sicherheitsgruppen	Konfigurieren Sie Sicherheitsgruppen, die DirectAccess-Clientcomputer und weitere Sicherheitsgruppen enthalten, die für die Bereitstellung erforderlich sind.
Konfigurieren des Netzwerkadressenservers	Der Assistent zum Aktivieren von DirectAccess konfiguriert den Netzwerkadressenserver auf dem DirectAccess-Server.

## Konfigurieren von Servernetzwerk Einstellungen

Für eine einzelne Serverbereitstellung in einer Umgebung mit IPv4 und IPv6 sind folgende Netzwerkschnittstelleneinstellungen erforderlich. Sämtliche IP-Adressen können im **Netzwerk- und Freigabecenter** von Windows mit der Option **Adapttereinstellungen ändern** konfiguriert werden.

- Edgetopologie
  - Eine öffentliche, statische IPv4- oder IPv6-Adresse mit Internetzugriff.
  - Eine einzelne, interne, statische IPv4- oder IPv6-Adresse

- Hinter einem NAT-Gerät (mit zwei Netzwerkadapters)
  - Eine einzelne, interne, statische IPv4- oder IPv6-Adresse mit Netzwerkzugriff
- Hinter einem NAT-Gerät (mit einem Netzwerkadapter)
  - Eine einzelne, statische IPv4- oder IPv6-Adresse.

#### **NOTE**

Für den Fall, dass der Remotezugriffsserver zwei Netzwerkadapter besitzt (einer, der in dem Domänenprofil klassifiziert ist und der andere in einem öffentlichen/privaten Profil), jedoch nur eine einzelne NIC-Topologie verwendet wird, wird Folgendes empfohlen:

1. Vergewissern Sie sich, dass auch die zweite NIC in dem Domänenprofil klassifiziert ist.
2. Wenn die zweite NIC aus einem bestimmten Grund nicht für das Domänenprofil konfiguriert werden kann, muss der Bereich für die DirectAccess IPsec-Richtlinie manuell mithilfe der folgenden Windows PowerShell-Befehle festgelegt werden:

```
$gposession = Open-NetGPO -PolicyStore <Name of the server GPO>
Set-NetIPsecRule -DisplayName <Name of the IPsec policy> -GPOSession $gposession -Profile Any
Save-NetGPO -GPOSession $gposession
```

## Konfigurieren des Routings im Unternehmensnetzwerk

Konfigurieren Sie das Routing im Unternehmensnetzwerk wie folgt:

- Wenn in der Organisation eine systemeigene IPv6-Adresse bereitgestellt wird, fügen Sie ihr eine Route hinzu, damit die Router im internen Netzwerk den IPv6-Datenverkehr zurück über den Remotezugriffsserver leiten.
- Konfigurieren Sie die IPv4- und IPv6-Routen der Organisation manuell auf den Remotezugriffsservern. Fügen Sie eine öffentliche Route hinzu, sodass der gesamte Datenverkehr mit Organisations-IPv6-Präfix (/48) an das interne Netzwerk weitergeleitet wird. Fügen Sie außerdem für IPv4-Datenverkehr explizite Routen hinzu, damit IPv4-Datenverkehr an das interne Netzwerk weitergeleitet wird.

## Konfigurieren von Firewalls

Wenden Sie bei zusätzlichen Firewalls in der Bereitstellung die folgenden Firewallausnahmen mit Internetzugriff für RAS-Datenverkehr an, wenn der RAS-Server sich im IPv4-Internet befindet:

- IPv6-zu-IPv4-Datenverkehr-IP-Protokoll 41 eingehend und ausgehend.
- IP-HTTPS-TCP (Transmission Control Protocol)-Zielport 443 und TCP-Quellport 443 ausgehend. Hat der RAS-Server nur einen Netzwerkadapter und der Netzwerkadressenserver ist auf dem RAS-Server, wird auch TCP-Port 62000 benötigt.

Wenden Sie bei zusätzlichen Firewalls die folgenden Firewallausnahmen mit Internetzugriff für RAS-Datenverkehr an, wenn der RAS-Server sich im IPv6-Internet befindet:

- IP-Protokoll 50
- UDP-Zielport 500 eingehend und UDP-Quellport 500 ausgehend.

Wenden Sie bei zusätzlichen Firewalls die folgenden internen Netzwerkfirewallausnahmen für RAS-Datenverkehr an:

- ISATAP-Protokoll 41 eingehend und ausgehend

- TCP/UDP für den gesamten IPv4/IPv6-Datenverkehr

## Konfigurieren von Zertifizierungsstellen und Zertifikaten

Der Assistent zum Aktivieren von DirectAccess konfiguriert einen integrierten Kerberos-Proxy, der die Authentifizierung anhand der Benutzernamen und Kennwörter vornimmt. Außerdem konfiguriert er ein IP-HTTPS-Zertifikat auf dem Remotezugriffsserver.

### Konfigurieren von Zertifikat Vorlagen

Wenn Sie zur Ausstellung von Zertifikaten eine interne Zertifizierungsstelle verwenden, müssen Sie für das IP-HTTPS-Zertifikat und das Netzwerkadressenserver-Websitezertifikat eine Zertifikatvorlage konfigurieren.

**So konfigurieren Sie eine Zertifikatvorlage**

1. Erstellen Sie eine Zertifikatvorlage für die interne Zertifizierungsstelle, wie beschrieben in [Erstellen von Zertifikatvorlagen](#).
2. Stellen Sie die Zertifikatvorlage wie unter [Deploying Certificate Templates](#)beschrieben bereit.

### Konfigurieren des IP-HTTPS-Zertifikats

Für den Remotezugriff ist zum Authentifizieren von IP-HTTPS-Verbindungen mit dem Remotezugriffsserver ein IP-HTTPS-Zertifikat erforderlich. Für das IP-HTTPS-Zertifikat sind drei Zertifikatoptionen verfügbar:

- **Öffentlich:** wird von einem Drittanbieter bereitgestellt.

Dies ist ein Zertifikat, das für die IP-HTTPS-Authentifizierung verwendet wird. Wenn der Antragstellername des Zertifikats kein Platzhalter ist, muss er mit der extern auflösbar FQDN-URL übereinstimmen, die nur für Remotezugriffsserver-IP HTTPS-Verbindungen verwendet wird.

- **Privat:** die folgenden sind erforderlich, wenn Sie nicht bereits vorhanden sind:

- Ein Websitezertifikat, das für die IP-HTTPS-Authentifizierung verwendet wird. Beim Zertifikatantragsteller sollte es sich um einen extern auflösbar, vollqualifizierten Domänennamen (FQDN) handeln, der über das Internet erreichbar ist.
- Ein Zertifikatsperrlisten-Verteilungspunkt, der über einen öffentlich auflösbar FQDN erreichbar ist.

- **Selbst signiert:** Folgendes ist erforderlich, wenn Sie nicht bereits vorhanden sind:

#### NOTE

Selbstsignierte Zertifikate können nicht in Bereitstellungen für mehrere Standorte verwendet werden.

- Ein Websitezertifikat, das für die IP-HTTPS-Authentifizierung verwendet wird. Beim Zertifikatantragsteller sollte es sich um einen extern auflösbar FQDN handeln, der über das Internet erreichbar ist.
- Ein Zertifikatsperrlisten-Verteilungspunkt, der über einen öffentlich auflösbar vollqualifizierten Domänennamen (FQDN) erreichbar ist.

Stellen Sie sicher, dass das für die IP-HTTPS-Authentifizierung verwendete Websitezertifikat die folgenden Anforderungen erfüllt:

- Der allgemeine Name des Zertifikats sollte dem Namen der IP-HTTPS-Website entsprechen.
- Geben Sie im Feld Antragsteller die IPv4-Adresse des externen Adapters des Remotezugriffsservers oder die FQDN der IP-HTTPS-URL an.
- Geben Sie im Feld %amp;quot;Erweiterte Schlüsselverwendung%amp;quot; die

Serverauthentifizierungs-Objektkennung (OID) an.

- Geben Sie im Feld "Sperrlisten-Verteilungspunkte" einen Zertifikatsperrlisten-Verteilungspunkt an, auf den mit dem Internet verbundene DirectAccess-Clients zugreifen können.
- Das IP-HTTPS-Zertifikat muss einen privaten Schlüssel enthalten.
- Das IP-HTTPS-Zertifikat muss direkt in den persönlichen Speicher importiert werden.
- Die Namen von IP-HTTPS-Zertifikaten können Platzhalter enthalten.

**So installieren Sie das IP-HTTPS-Zertifikat von einer internen Zertifizierungsstelle**

1. Auf dem Remote Zugriffs Server: Geben Sie auf dem **Start** BildschirmMMC. exeein, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-ins hinzufügen oder entfernen** auf **Zertifikate, Hinzufügen, Computerkonto, Weiter, Lokaler Computer, Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
6. Klicken Sie zweimal auf **Weiter**.
7. Aktivieren Sie auf der Seite **Zertifikate anfordern** das Kontrollkästchen für die Zertifikat Vorlage, und klicken Sie bei Bedarf auf Weitere Informationen, die für die Registrierung dieses Zertifikats erforderlich sind.
8. Klicken Sie im Dialogfeld **Zertifikateigenschaften** auf der Registerkarte **Antragsteller** im Bereich **Antragstellename** unter **Typ** auf **Allgemeiner Name**.
9. Geben Sie im Feld **Wert** die IPv4-Adresse des externen Adapters des Remotezugriffsservers oder die FQDN der IP-HTTPS-URL an und klicken Sie anschließend auf **Hinzufügen**.
10. Wählen Sie unter **Alternativer Name** für **Typ** die Option **DNS** aus.
11. Geben Sie im Feld **Wert** die IPv4-Adresse des externen Adapters des Remotezugriffsservers oder die FQDN der IP-HTTPS-URL an und klicken Sie anschließend auf **Hinzufügen**.
12. Auf der Registerkarte **Allgemein** unter **Anzeigenname** können Sie einen Namen für das Zertifikat eingeben, sodass Sie es schneller identifizieren können.
13. Klicken Sie auf der Registerkarte **Erweiterungen** auf den Pfeil neben dem Feld **Erweiterte Schlüsselverwendung** und vergewissern Sie sich, dass in der Liste **Ausgewählte Optionen** Serverauthentifizierung angezeigt wird.
14. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
15. Überprüfen Sie im Detailbereich des Zertifikat-Snap-in, dass das neue Zertifikat unter Serverauthentifizierung mit der Option Beabsichtigte Zwecke registriert wurde.

## Konfigurieren des DNS-Servers

Sie müssen einen DNS-Eintrag für die Netzwerkadressenserver-Website für das interne Netzwerk in Ihrer Bereitstellung manuell konfigurieren.

### **So erstellen Sie die DNS-Einträge für den Netzwerkadressen Server und den Webtest**

1. Auf dem internen Netzwerk-DNS-Server: Geben Sie auf dem **Start** Bildschirm \* \* dnsmgmt.msc \* \* ein, und drücken Sie dann die EINGABETASTE.
2. Erweitern Sie im linken Bereich der **DNS-Manager**-Konsole die Forward-Lookupzone für Ihre Domäne. Klicken Sie mit der rechten Maustaste auf die Domäne, und anschließend auf **Neuer Host (A oder AAAA)**.
3. Geben Sie im Dialogfeld **Neuer Host** in das Feld **Name (bei Nichtangabe wird übergeordnete Domäne verwendet)** den DNS-Namen für die Netzwerkadressenserver-Website (mit diesem Namen verbinden sich die DirectAccess-Clients mit dem Netzwerkadressenserver) ein. Geben Sie in das Feld **IP-Adresse** die IPv4-Adresse des Netzwerkadressenservers ein und klicken Sie dann auf **Host hinzufügen**. Klicken Sie im Dialogfeld **DNS** auf **OK**.
4. Geben Sie im Dialogfeld **Neuer Host** in das Feld **Name (bei Nichtangabe wird übergeordnete Domäne verwendet)** den DNS-Namen des Webtests ein (der Name für Standard-Webtests lautet directaccess-webprobehost). Geben Sie in das Feld **IP-Adresse** die IPv4-Adresse des Webtests ein und klicken Sie dann auf **Host hinzufügen**. Wiederholen Sie diesen Vorgang für directaccess-corconnectivityhost und manuell erstellte Verbindungsprüfer. Klicken Sie im Dialogfeld **DNS** auf **OK**.
5. Klicken Sie auf **Fertig**.

#### *Befehle in Windows PowerShell*

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address
<network_location_server_IPv4_address>
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address
<network_location_server_IPv6_address>
```

Außerdem müssen Sie die DNS-Einträge für folgende Elemente konfigurieren:

- **Der IP-HTTPS-Server:** DirectAccess-Clients müssen in der Lage sein, den DNS-Namen des Remote Zugriffs Servers aus dem Internet aufzulösen.
- **CRL-Sperr Überprüfung:** DirectAccess verwendet Zertifikat Sperr Überprüfungen für die IP-HTTPS-Verbindung zwischen DirectAccess-Clients und dem RAS-Server sowie für die HTTPS-basierte Verbindung zwischen dem DirectAccess-Client und dem Netzwerkadressen Server. In beiden Fällen müssen DirectAccess-Clients in der Lage sein, auf den Zertifikatsperllisten-Verteilungspunkt zuzugreifen und ihn aufzulösen.

## Konfigurieren von Active Directory

Der Remotezugriffsserver und alle DirectAccess-Clientcomputer müssen zu einer Active Directory-Domäne zusammengeführt werden. DirectAccess-Clientcomputer müssen Mitglied folgender Domänenentypen sein:

- Domänen, die zur gleichen Gesamtstruktur wie der Remotezugriffsserver gehören.
- Domänen, die zu Gesamtstrukturen mit einer bidirektionalen Vertrauensstellung zur Remotezugriffsserver-Gesamtstruktur gehören.
- Domänen mit bidirektionaler Vertrauensstellung zur Remotezugriffsserverdomäne.

#### **So fügen Sie Clientcomputer zur Domäne hinzu**

1. Geben Sie auf dem **Start** Bildschirm **Explorer**, **exe** ein, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie mit der rechten Maustaste auf das Computersymbol und klicken Sie dann auf **Eigenschaften**.

3. Klicken Sie auf der Seite **System** auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf der Registerkarte **Computername** im Dialogfeld **Systemeigenschaften** auf **Ändern**.
5. Geben Sie unter **Computername** den Namen des Computers ein, falls Sie beim Beitritt des Servers zur Domäne auch den Computernamen ändern. Klicken Sie unter **Mitglied von** auf **Domäne**, und geben Sie dann den Namen der Domäne ein, für die der Beitritt des Servers durchgeführt werden soll, z. B. `%%amp;quot;corp.contoso.com%%amp;quot;`, und klicken Sie dann auf **OK**.
6. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, der über die Berechtigung zum Durchführen des Beitritts von Computern zur Domäne verfügt. Klicken Sie anschließend auf **OK**.
7. Klicken Sie auf **OK**, wenn das Begrüßungsdialogfeld für die Domäne angezeigt wird.
8. Klicken Sie auf **OK**, wenn Sie zum Neustarten des Computers aufgefordert werden.
9. Klicken Sie im Dialogfeld **Systemeigenschaften** auf „Schließen“. Klicken Sie bei Aufforderung auf **Jetzt neu starten**.

#### *Befehle in Windows PowerShell*

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

Beachten Sie, dass Sie nach der Eingabe des unten angegebenen Befehls `%%amp;quot;Add-Computer%%amp;quot;` die Domänenanmeldeinformationen bereitstellen müssen.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

## Konfigurieren von GPOs

Zum Bereitstellen des Remote Zugriffs benötigen Sie mindestens zwei Gruppenrichtlinie Objekte: ein Gruppenrichtlinie Objekt enthält Einstellungen für den RAS-Server und eine enthält Einstellungen für DirectAccess-Client Computer. Wenn Sie den Remote Zugriff konfigurieren, erstellt der Assistent automatisch die erforderlichen Gruppenrichtlinie Objekte. Wenn Ihre Organisation jedoch eine Benennungs Konvention erzwingt oder Sie nicht über die erforderlichen Berechtigungen zum Erstellen oder Bearbeiten von Gruppenrichtlinie Objekten verfügen, müssen Sie vor dem Konfigurieren des Remote Zugriffs erstellt werden.

Informationen zum Erstellen von Gruppenrichtlinie Objekten finden Sie unter [Erstellen und Bearbeiten eines Gruppenrichtlinie Objekts](#).

## IMPORTANT

Der Administrator kann die DirectAccess-Gruppenrichtlinie Objekte mithilfe der folgenden Schritte manuell mit einer Organisationseinheit verknüpfen:

1. Verknüpfen Sie die erstellten Gruppenrichtlinienobjekte mit den entsprechenden Organisationseinheiten, bevor Sie DirectAccess konfigurieren.
2. Wenn Sie DirectAccess konfigurieren, sollten Sie eine Sicherheitsgruppe für die Clientcomputer angeben.
3. Der Remote Zugriffs Administrator verfügt möglicherweise über Berechtigungen zum Verknüpfen der Gruppenrichtlinie Objekte mit der Domäne. In beiden Fällen werden die Gruppenrichtlinienobjekte automatisch konfiguriert. Wenn die Gruppenrichtlinienobjekte bereits mit einer Organisationseinheit verknüpft sind, werden die Verknüpfungen nicht entfernt und die die Gruppenrichtlinienobjekte werden nicht mit der Domäne verknüpft. Für ein Server-Gruppenrichtlinienobjekt muss die Organisationseinheit das Servercomputerobjekt enthalten, andernfalls wird das Gruppenrichtlinienobjekt mit dem Domänenstamm verknüpft.
4. Wenn die Verknüpfung mit der Organisationseinheit nicht vor dem Ausführen des DirectAccess-Assistenten erfolgt ist, kann der Domänen Administrator nach Abschluss der Konfiguration die DirectAccess-Gruppenrichtlinie Objekte mit den erforderlichen Organisationseinheiten verknüpfen. Die Verknüpfung zur Domäne kann entfernt werden. Die Schritte zum Verknüpfen eines Gruppenrichtlinie Objekts mit einer Organisationseinheit finden Sie [hier](#).

## NOTE

Wenn ein Gruppenrichtlinie Objekt manuell erstellt wurde, kann es während der DirectAccess-Konfiguration vorkommen, dass das Gruppenrichtlinie Objekt nicht verfügbar ist. Das Gruppenrichtlinie Objekt wurde möglicherweise nicht auf den nächstgelegenen Domänen Controller des Verwaltungs Computers repliziert. In diesem Fall kann der Administrator warten, bis die Replikation abgeschlossen ist oder er kann die Replikation erzwingen.

## Konfigurieren von Sicherheitsgruppen

Die DirectAccess-Einstellungen, die auf dem Client Computer Gruppenrichtlinie Objekt enthalten sind, werden nur auf Computer angewendet, die Mitglieder der Sicherheitsgruppe sind, die Sie beim Konfigurieren des Remote Zugriffs angeben. Außerdem müssen Sie eine Sicherheitsgruppe für diese Server erstellen, wenn Sie zum Verwalten Ihrer Anwendungsserver Sicherheitsgruppen verwenden.

### So erstellen Sie eine Sicherheitsgruppe für DirectAccess-Clients

1. Geben Sie auf dem **Start Bildschirm DSA**. mscein, und drücken Sie dann die EINGABETASTE. Erweitern Sie in der Konsole **Active Directory-Benutzer und -Computers** im linken Bereich die Domäne, die die Sicherheitsgruppe enthält, klicken Sie mit der rechten Maustaste auf **Benutzer**, zeigen Sie auf **Neu** und klicken Sie dann auf **Gruppe**.
2. Geben Sie im Dialogfeld **Neues Objekt - Gruppe** unter **Gruppenname** den Namen für die Sicherheitsgruppe ein.
3. Klicken Sie unter **Gruppenbereich** auf **Global**, unter **Gruppentyp** auf **Sicherheit** und anschließend auf **OK**.
4. Doppelklicken Sie auf die Sicherheitsgruppe der DirectAccess-Clientcomputer und dann im Dialogfeld **Eigenschaften** auf die Registerkarte **Mitglieder**.
5. Auf der Registerkarte **Mitglieder** klicken Sie auf **Hinzufügen**.
6. Wählen Sie im Dialogfeld zum **Auswählen von Benutzern, Kontakten Computern oder Dienstkonten** die Clientcomputer aus, für die DirectAccess aktiviert werden soll, und klicken Sie anschließend auf **OK**.



Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

## Konfigurieren des Netzwerkadressen Servers

Der Netzwerkadressenserver sollte sich auf einem Server mit hoher Verfügbarkeit befinden und über ein gültiges SSL-Zertifikat verfügen, dem die DirectAccess-Clients vertrauen. Für das Netzwerkadressenserver-Zertifikat sind zwei Zertifikatoptionen verfügbar:

- **Privat:** die folgenden sind erforderlich, wenn Sie nicht bereits vorhanden sind:
  - Ein Websitezertifikat, das für den Netzwerkadressenserver verwendet wird. Der Zertifikatantragsteller sollte die URL des Netzwerkadressenservers sein.
  - Ein Sperrlisten-Verteilungspunkt mit hoher Verfügbarkeit aus dem internen Netzwerk.
- **Selbst signiert:** Folgendes ist erforderlich, wenn Sie nicht bereits vorhanden sind:

### NOTE

Selbstsignierte Zertifikate können nicht in Bereitstellungen für mehrere Standorte verwendet werden.

- Ein Websitezertifikat, das für den Netzwerkadressenserver verwendet wird. Der Zertifikatantragsteller sollte die URL des Netzwerkadressenservers sein.

### NOTE

Wenn sich die Netzwerkadressenserver-Website auf einem Remotezugriffsserver befindet, wird bei der Konfiguration des Remotezugriffs automatisch eine Website erstellt, die an das von Ihnen angegebene Serverzertifikat gebunden ist.

### So installieren Sie das Netzwerkadressenserver-Zertifikat von einer internen Zertifizierungsstelle

1. Auf dem Server, auf dem die Netzwerkadressen Server-Website gehostet wird: Geben Sie auf dem **Start BildschirmMMC** ein, und drücken Sie dann die EINGABETASTE.
2. Klicken Sie in der MMC-Konsole im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie im Dialogfeld **Snap-ins hinzufügen oder entfernen** auf **Zertifikate, Hinzufügen, Computerkonto, Weiter, Lokaler Computer, Fertig stellen** und anschließend auf **OK**.
4. Öffnen Sie in der Konsolenstruktur des Zertifikat-Snap-Ins den Eintrag **Zertifikate (Lokaler Computer)\Persönlich\Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, zeigen Sie auf **Alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.
6. Klicken Sie zweimal auf **Weiter**.
7. Aktivieren Sie auf der Seite **Zertifikate anfordern** das Kontrollkästchen für die Zertifikat Vorlage, und klicken Sie bei Bedarf auf Weitere Informationen, die für die Registrierung dieses Zertifikats erforderlich sind.
8. Klicken Sie im Dialogfeld **Zertifikateigenschaften** auf der Registerkarte **Antragsteller** im Bereich

**Antragstellernname unter Typ auf Allgemeiner Name.**

9. Geben Sie in das Feld **Wert** den FQDN der Netzwerkadressenserver-Website ein und klicken Sie dann auf **Hinzufügen**.
10. Wählen Sie unter **Alternativer Name** für **Typ** die Option **DNS** aus.
11. Geben Sie in das Feld **Wert** den FQDN der Netzwerkadressenserver-Website ein und klicken Sie dann auf **Hinzufügen**.
12. Auf der Registerkarte **Allgemein** unter **Anzeigename** können Sie einen Namen für das Zertifikat eingeben, sodass Sie es schneller identifizieren können.
13. Klicken Sie auf **OK, Registrieren** und dann auf **Fertig stellen**.
14. Überprüfen Sie im Detailbereich des Zertifikat-Snap-in, dass das neue Zertifikat unter Serverauthentifizierung mit der Option Beabsichtigte Zwecke registriert wurde.

# Schritt 2: Konfigurieren des DirectAccess-VPN-Servers

09.04.2020 • 10 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird die Konfiguration der Client- und Servereinstellungen erläutert, die für eine einfache Remotezugriffsbereitstellung mit dem Assistenten zum Aktivieren von DirectAccess erforderlich sind.

In der folgenden Tabelle finden Sie eine Übersicht über die Schritte, die Sie in diesem Thema ausführen können.

AUFGABE	BESCHREIBUNG
Konfigurieren von DirectAccess-Clients	Konfigurieren Sie den Remotezugriffsserver mit den Sicherheitsgruppen, die die DirectAccess-Clients enthalten.
Konfigurieren der Netzwerktopologie	Konfigurieren Sie die Einstellungen des Remotezugriffsservers.
Konfigurieren der Suchliste für DNS-Suffixe	Ändern Sie die Suchliste für DNS-Suffixe bei Bedarf.
Konfiguration der Gruppenrichtlinienobjekte	Ändern Sie bei Bedarf die Gruppenrichtlinienobjekte.

## So starten Sie den Assistenten zum Aktivieren von DirectAccess

1. Klicken Sie in Server-Manager **auf Extras**, **und klicken Sie dann auf Remote Zugriff**. Der Assistent zum Aktivieren von DirectAccess wird automatisch gestartet, es sei denn, Sie haben den **Bildschirm nicht mehr anzeigen** ausgewählt.
2. Wenn der Assistent nicht automatisch gestartet wird, klicken Sie mit der rechten Maustaste auf den Server-Knoten in der Struktur Routing und RAS, und klicken Sie dann auf **DirectAccess aktivieren**.
3. Klicken Sie auf **Weiter**.

## Konfigurieren von DirectAccess-Clients

Damit ein Clientcomputer zur Verwendung von DirectAccess bereitgestellt werden kann, muss er zur ausgewählten Sicherheitsgruppe gehören. Nachdem DirectAccess konfiguriert wurde, werden Clientcomputer in der Sicherheitsgruppe bereitgestellt, damit sie das DirectAccess-Gruppenrichtlinienobjekt empfangen.

1. Klicken Sie auf der Seite **Gruppen auswählen** auf **Hinzufügen**.
2. Wählen Sie im Dialogfeld **Gruppen auswählen** die Sicherheitsgruppen aus, die DirectAccess-Clientcomputer enthalten.
3. Aktivieren Sie das Kontrollkästchen **DirectAccess ausschließlich für mobile Computer aktivieren**, damit nur mobile Computer auf das interne Netzwerk zugreifen können.
4. Aktivieren Sie das Kontrollkästchen **Tunnelerzwingung verwenden**, um den gesamten Client-Datenverkehr (an das interne Netzwerk und das Internet) bei Bedarf über den Remotezugriffsserver zu leiten.

5. Klicken Sie auf **Weiter**.

## Konfigurieren der Netzwerktopologie

Um den Remotezugriff bereitzustellen, müssen Sie den Remotezugriffsserver mit korrekten Netzwerkadaptersn, einer öffentlichen URL für den Remotezugriffsserver, zu dem Clientcomputer eine Verbindung aufbauen können (die ConnectTo-Adresse), einem IP-HTTPS-Zertifikat mit einem Antragsteller, der mit der ConnectTo-Adresse übereinstimmt, konfigurieren.

1. Klicken Sie auf der Seite **Netzwerktopologie** auf die Bereitstellungstopologie, die in Ihrer Organisation verwendet wird. Geben Sie unter **Geben Sie den öffentlichen Namen oder die öffentliche IPv4-Adresse an** den öffentlichen Namen für die Bereitstellung ein (dieser Name stimmt mit dem Antragstellernamen des IP-HTTPS-Zertifikats überein, z. B. edge1.contoso.com), und klicken Sie dann auf **Weiter**.

## Konfigurieren der Suchliste für DNS-Suffixe

Für DNS-Clients können Sie eine Suchliste für ein DNS-Domänensuffix konfigurieren, die die DNS-Suchfunktionen erweitert oder überprüft. Indem Sie zusätzliche Suffixe zu der Liste hinzufügen, können Sie in mehreren angegebenen DNS-Domänen nach kurzen, nicht qualifizierten Computernamen suchen. Wenn eine DNS-Abfrage fehlschlägt, kann der DNS-Client Dienst diese Liste verwenden, um andere Namen Suffix-Endungen an ihren ursprünglichen Namen anzufügen und DNS-Abfragen für diese alternativen FQDNs an den DNS-Server zu wiederholen.

1. Wählen Sie **DirectAccess-Clients mit der Suchliste für DNS-Clientsuffixe** konfigurieren, um zusätzliche Suffixe für Clientnamen-Suchvorgänge anzugeben.
2. Geben Sie in **Neues Suffix** einen neuen Suffix ein, und klicken Sie dann auf **Hinzufügen**. Außerdem können Sie die Such Reihenfolge ändern und Suffixe aus **Domänen Suffixen entfernen, um Sie zu verwenden**.

Nebenbei In einem Zusammenhang losen Namespace-Szenario (bei dem ein oder mehrere Domänen Computer ein DNS-Suffix aufweisen, das nicht mit der Active Directory Domäne identisch ist, zu der die Computer gehören), sollten Sie sicherstellen, dass die Suchliste so angepasst ist, dass Sie alle erforderlichen Suffixe enthält. Der RAS-Assistent konfiguriert den Active Directory-DNS-Namen standardmäßig als primäres DNS-Suffix auf dem Client. Der Administrator sollte sicherstellen, dass er das von den Clients zur Namensauflösung verwendete DNS-Suffix hinzufügt.

Für Computer und Server ist das folgende standardmäßige DNS-Suchverhalten vorgegeben und wird verwendet, wenn kurze, nicht qualifizierte Namen vervollständigt und aufgelöst werden. Wenn die Suffixsuchliste leer oder nicht angegeben ist, wird das primäre DNS-Suffix des Computers an kurze, nicht qualifizierte Namen angehängt, und eine DNS-Abfrage wird verwendet, um den resultierenden FQDN aufzulösen.

Wenn bei der Abfrage ein Fehler auftritt, kann der Computer zusätzliche Abfragen für alternative voll qualifizierte Namen durchführen, indem ein beliebiges Verbindungs spezifisches DNS-Suffix angehängt wird, das für Netzwerkverbindungen konfiguriert ist. Wenn keine Verbindungs spezifischen Suffixe konfiguriert sind oder Abfragen für diese resultierenden Verbindungs spezifischen FQDNs fehlschlagen, kann der Client dann mit dem Wiederholen von Abfragen auf der Grundlage der systematischen Reduzierung des primären Suffixe (auch als "Devolution" bezeichnet) beginnen.

Wenn das primäre Suffix z. B. "example.Microsoft.com" ist, kann der Prozess der Verkürzung Abfragen für den Kurznamen wiederholen, indem er in den Domänen "Microsoft.com" und "com" danach sucht.

Wenn die Suffixsuchliste nicht leer ist und mindestens ein DNS-Suffix angegeben wurde, ist der Versuch, kurze DNS-Namen zu qualifizieren und aufzulösen, nur auf die durch die angegebene Suffixliste möglichen FQDNs beschränkt.

Wenn die Abfragen für alle durch das Anfügen und Versuchen der Suffixe in der Liste gebildeten FQDNs nicht aufgelöst werden können, schlägt der Abfragevorgang fehl und als Ergebnis wird "Name nicht gefunden" ausgegeben.

#### **WARNING**

Wenn die Domänensuffixliste verwendet wird, senden die Clients weiterhin zusätzliche auf den verschiedenen DNS-Domänenamen basierende alternative Abfragen, wenn eine Abfrage nicht beantwortet oder aufgelöst wird. Nachdem ein Name mit einem Eintrag in der Suffixliste aufgelöst wurde, werden die nicht verwendeten Listeneinträge nicht versucht. Aus diesem Grund ist es am effizientesten, die Liste zunächst nach den am meisten verwendeten Domänensuffixen zu sortieren.

Suchen nach Domänennamensuffixen werden nur verwendet, wenn ein DNS-Name nicht vollqualifiziert ist. Um einen DNS-Namen voll zu qualifizieren, müssen Sie am Ende des Namens einen nachstehenden Punkt (.) eingeben.

## Konfiguration der Gruppenrichtlinienobjekte

Wenn Sie den Remote Zugriff konfigurieren, werden DirectAccess-Einstellungen in Gruppenrichtlinie Objekte (GPO) gesammelt.

Unter GPO-Einstellungen werden der Name des Gruppenrichtlinien Objekts für den DirectAccess-Server und der Name des Gruppenrichtlinien Objekts aufgeführt. Zusätzlich können Sie die GPO-Auswahleinstellungen ändern.

Zwei GPOs werden automatisch mit DirectAccess-Einstellungen aufgefüllt und auf diese Weise verteilt:

1. **DirectAccess-Client-Gruppenrichtlinienobjekt.** Dieses Gruppenrichtlinienobjekt enthält die Client-Einstellungen, einschließlich der Einstellungen für die IPv6-Übergangstechnologie, der Einträge in der Richtlinientabelle für die Namensauflösung und der Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit. Das Gruppenrichtlinienobjekt wird auf die für die Clientcomputer angegebenen Sicherheitsgruppen angewendet.
2. **DirectAccess-Server-Gruppenrichtlinienobjekt.** Dieses Gruppenrichtlinien Objekt enthält die DirectAccess-Konfigurationseinstellungen, die auf jeden als RAS-Server konfigurierten Server in Ihrer Bereitstellung angewendet werden. Außerdem enthält es die Verbindungssicherheitsregeln für die Windows-Firewall mit erweiterter Sicherheit.

## Zusammenfassung

Sobald die Konfiguration des Remote Zugriffs fertiggestellt ist, wird die **Zusammenfassung** angezeigt. Sie können die konfigurierten Einstellungen ändern oder auf **Fertig stellen** klicken, um die Konfiguration zu übernehmen.

# Schritt 3 Überprüfen der Bereitstellung

09.04.2020 • 2 minutes to read • [Edit Online](#)

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016

In diesem Thema wird beschrieben, wie Sie überprüfen, ob Sie die DirectAccess-Bereitstellung ordnungsgemäß konfiguriert haben.

## **So überprüfen Sie den Zugriff auf interne Ressourcen über DirectAccess**

1. Stellen Sie eine Verbindung von einem DirectAccess-Clientcomputer mit dem Unternehmensnetzwerk her, und rufen Sie die Gruppenrichtlinie ab.
2. Klicken Sie im Infobereich auf das Symbol **Netzwerkverbindungen**, um auf die DirectAccess-Medienverwaltung zuzugreifen.
3. Klicken Sie auf die **DirectAccess-Verbindung**. Als Status wird **Lokal verbunden** angezeigt.
4. Verbinden Sie den Clientcomputer mit dem externen Netzwerk, und versuchen Sie, auf interne Ressourcen zuzugreifen.

Sie sollten auf alle Unternehmensressourcen zugreifen können.

# Webanwendungsproxy in Windows Server 2016

09.04.2020 • 3 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Diese Inhalte sind für die lokale Version des webanwendungsproxys relevant. Informationen zum Aktivieren des sicheren Zugriffs auf lokale Anwendungen über die Cloud finden Sie in den [Azure AD Anwendungs Proxy-Inhalt](#).

In diesem Abschnitt werden die Neuerungen und Änderungen im webanwendungsproxy für Windows Server 2016 beschrieben. Die hier aufgeführten neuen Features und Änderungen haben bei der Arbeit mit der Vorschau wahrscheinlich die größten Auswirkungen.

## Neue Features des webanwendungsproxys in Windows Server 2016

- Vorauthentifizierung für http-Basis Anwendungs Veröffentlichung

HTTP Basic ist das Autorisierungs Protokoll, das von vielen Protokollen verwendet wird, einschließlich ActiveSync, um Rich-Clients, einschließlich Smartphones, mit Ihrem Exchange-Postfach zu verbinden. Der webanwendungsproxy interagiert traditionell mit AD FS mithilfe von Umleitungen, die auf ActiveSync-Clients nicht unterstützt werden. Diese neue Version des webanwendungsproxys unterstützt das Veröffentlichen einer App mithilfe von HTTP Basic, indem es der http-App ermöglicht, eine nicht anspruchsvolle Vertrauensstellung der vertrauenden Seite für die Anwendung für die Verbunddienst zu empfangen.

Weitere Informationen zur HTTP-Basis Veröffentlichung finden [Sie unter Veröffentlichen von Anwendungen mit AD FS Vorauthentifizierung](#).

- Platzhalter Domänen Veröffentlichung von Anwendungen

Zur Unterstützung von Szenarien wie SharePoint 2013 kann die externe URL für die Anwendung nun einen Platzhalter enthalten, mit dem Sie mehrere Anwendungen in einer bestimmten Domäne veröffentlichen können, z. b. `https://*. SP-apps. Configuration. com`. Dadurch wird die Veröffentlichung von SharePoint-apps vereinfacht.

- Umleitung von http zu https

Um sicherzustellen, dass Ihre Benutzer auf Ihre App zugreifen können, unterstützt der webanwendungsproxy nun die Umleitung von http zu HTTPS, auch wenn Sie den Typ "https" in der URL vernachlässigen.

- HTTP-Veröffentlichung

Es ist jetzt möglich, HTTP-Anwendungen mit Passthrough-Vorauthentifizierung zu veröffentlichen.

- Veröffentlichen von Remotedesktop Gateway-apps

Weitere Informationen zu RDG im webanwendungsproxy finden Sie unter [Veröffentlichen von Anwendungen mit SharePoint, Exchange und RDG](#).

- Neues Debugprotokoll zur besseren Problembehandlung und zum verbesserten Dienst Protokoll für einen kompletten Überwachungs Pfad und eine verbesserte Fehlerbehandlung

Weitere Informationen zur Problembehandlung finden Sie unter Problembehandlung für [Webanwendungs Proxy](#)

- Verbesserungen der Administratorkonsole
- Weitergabe von Client-IP-Adressen an Back-End

## Weitere Informationen

- [Neuerungen in Windows Server 2016](#)
- [Veröffentlichen von Anwendungen mit AD FS-Vorauthentifizierung](#)
- [Problembehandlung: Webanwendungsproxy](#)

# Veröffentlichen von Anwendungen mit ADFS-Vorauthentifizierung

14.04.2020 • 40 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Diese Inhalte sind für die lokale Version des webanwendungsproxys relevant. Informationen zum Aktivieren des sicheren Zugriffs auf lokale Anwendungen über die Cloud finden Sie in den [Azure AD Anwendungs Proxy-Inhalt](#).

In diesem Thema wird beschrieben, wie Sie Anwendungen über den webanwendungsproxy mithilfe der Vorauthentifizierung Active Directory-Verbunddienste (AD FS) (AD FS) veröffentlichen.

Für alle Anwendungs Typen, die Sie mit AD FS-Vorauthentifizierung veröffentlichen können, müssen Sie der Verbunddienst eine AD FS Vertrauensstellung der vertrauenden Seite hinzufügen.

Der allgemeine Ablauf der AD FS Vorauthentifizierung lautet wie folgt:

## NOTE

Dieser Authentifizierungs Ablauf gilt nicht für Clients, die Microsoft Store-Apps verwenden.

- Das Client Gerät versucht, auf eine veröffentlichte Webanwendung unter einer bestimmten Ressourcen-URL zuzugreifen. beispielsweise <https://app1.contoso.com/>.

Die Ressourcen-URL ist eine öffentliche Adresse, an der webanwendungsproxy eingehende HTTPS-Anforderungen überwacht.

Wenn die Umleitung von http zu HTTPS aktiviert ist, lauscht der webanwendungsproxy auch auf eingehende HTTP-Anforderungen.

- Der webanwendungsproxy leitet die HTTPS-Anforderung mit URL-codierten Parametern an den AD FS Server um, einschließlich der Ressourcen-URL und der apprealm (Bezeichner der vertrauenden Seite).

Der Benutzer authentifiziert sich mit der für den AD FS Server erforderlichen Authentifizierungsmethode. beispielsweise Benutzername und Kennwort, zweistufige Authentifizierung mit einem einmaligen Kennwort usw.

- Nachdem der Benutzer authentifiziert wurde, gibt der AD FS Server ein Sicherheits Token (das edgetoken) mit den folgenden Informationen aus und leitet die HTTPS-Anforderung zurück an den webanwendungsproxy-Server:

- Ressourcenbezeichner, auf den der Benutzer zuzugreifen versuchte
- Die Identität des Benutzers als Benutzer Prinzipal Name (User Principal Name, UPN).
- Ablaufdatum der Zugriffserteilungsgenehmigung (d. h. dem Benutzer wird für einen beschränkten Zeitraum, nach dem er sich erneut authentifizieren muss, Zugriff gewährt)
- Signatur der Informationen im Edgetoken

- Der webanwendungsproxy empfängt die umgeleitete HTTPS-Anforderung vom AD FS Server mit dem edgetoken und überprüft und verwendet das Token wie folgt:

- Überprüft, ob die edgetokensignatur aus dem Verbund Dienst stammt, der in der Konfiguration des webanwendungsproxys konfiguriert ist.
  - Er überprüft, ob das Token für die richtige Anwendung ausgestellt wurde.
  - Er überprüft, ob das Token noch gültig ist.
  - Er verwendet bei Bedarf die Benutzeridentität für die Überprüfungen, z. B. zum Abrufen eines Kerberos-Tickets, wenn der Back-End-Server zur Verwendung der integrierten Windows-Authentifizierung konfiguriert ist.
5. Wenn das edgetoken gültig ist, leitet der webanwendungsproxy die HTTPS-Anforderung über HTTP oder HTTPS an die veröffentlichte Webanwendung weiter.
  6. Der Client kann jetzt auf die veröffentlichte Webanwendung zugreifen, diese kann jedoch so konfiguriert sein, dass der Benutzer eine zusätzliche Authentifizierung durchführen muss. Wenn es sich bei der veröffentlichten Webanwendung z. B. um eine SharePoint-Website handelt und keine weitere Authentifizierung erforderlich ist, sieht der Benutzer die SharePoint-Website im Browser.
  7. Der webanwendungsproxy speichert ein Cookie auf dem Client Gerät. Das Cookie wird vom webanwendungsproxy verwendet, um zu ermitteln, dass diese Sitzung bereits vorauthentifiziert wurde und keine weitere Vorauthentifizierung erforderlich ist.

#### IMPORTANT

Achten Sie beim Konfigurieren der externen URL und der URL für den Back-End-Server darauf, dass Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) und keine IP-Adresse einfügen.

#### NOTE

Dieses Thema enthält Windows PowerShell-Beispiel-Cmdlets, mit deren Hilfe einige beschriebene Verfahren automatisiert werden können. Weitere Informationen finden Sie unter [Verwenden von Cmdlets](#).

## Veröffentlichen einer Anspruchs basierten Anwendung für Webbrowsers Clients

Um eine Anwendung zu veröffentlichen, die Ansprüche für die Authentifizierung verwendet, müssen Sie dem Verbunddienst eine Vertrauensstellung der vertrauenden Seite für die Anwendung hinzufügen.

Beim Veröffentlichen von anspruchsbasierter Anwendungen, auf die über einen Browser zugegriffen wird, ist der allgemeine Authentifizierungsablauf wie folgt:

1. Der Client versucht, mithilfe eines Webbrowsers auf eine Anspruchs basierte Anwendung zuzugreifen. beispielsweise <https://appserver.contoso.com/claimapp/>.
2. Der Webbrowsers sendet eine HTTPS-Anforderung an den webanwendungsproxy-Server, der die Anforderung an den AD FS-Server umleitet.
3. Der AD FS Server authentifiziert den Benutzer und das Gerät und leitet die Anforderung zurück an den webanwendungsproxy. Die Anforderung enthält jetzt das Edgetoken. Der AD FS Server fügt der Anforderung ein Single Sign-on-Cookie (SSO) hinzu, da der Benutzer bereits eine Authentifizierung für den AD FS Server durchgeführt hat.
4. Der webanwendungsproxy überprüft das Token, fügt ein eigenes Cookie hinzu und leitet die Anforderung an den Back-End-Server weiter.

5. Der Back-End-Server leitet die Anforderung an den AD FS-Server um, um das Anwendungs Sicherheits Token zu erhalten.
6. Die Anforderung wird vom AD FS Server an den Back-End-Server umgeleitet. Die Anforderung enthält jetzt das Anwendungstoken und das SSO-Cookie. Dem Benutzer wird Zugriff auf die Anwendung gewährt, ohne einen Benutzernamen oder ein Kennwort eingeben zu müssen.

In diesem Verfahren wird beschrieben, wie Sie eine anspruchsbaasierte Anwendung veröffentlichen, z. B. eine SharePoint-Website, auf die von Webbrowsersclients zugegriffen wird. Bevor Sie beginnen, sollten Sie sicherstellen, dass Sie Folgendes ausgeführt haben:

- Es wurde eine Vertrauensstellung der vertrauenden Seite für die Anwendung in der AD FS Management Console erstellt.
- Es wurde überprüft, ob ein Zertifikat auf dem webanwendungsproxy-Server für die zu veröffentlichte Anwendung geeignet ist.

#### **So veröffentlichen Sie eine anspruchsbaasierte Anwendung**

1. Klicken Sie auf dem webanwendungsproxy-Server in der Remote Zugriffs-Verwaltungskonsole im **Navigations** Bereich auf **webanwendungsproxy**, und klicken Sie dann im Bereich **Tasks** auf **veröffentlichen**.
2. Klicken Sie auf der Seite **Willkommen des Assistenten zum Veröffentlichen neuer Anwendungen** auf **Weiter**.
3. Klicken Sie auf der Seite **Vorauthentifizierung** auf **Active Directory-Verbunddienste (AD FS) (AD FS)**, und klicken Sie dann auf **weiter**.
4. Wählen Sie auf der Seite **Unterstützte Clients** die Option **Web und MSOFBA** aus, und klicken Sie dann auf **Weiter**.
5. Wählen Sie auf der Seite **Vertrauende Seite** in der Liste die vertrauende Seite für die zu veröffentlichte Anwendung aus, und klicken Sie dann auf **Weiter**.
6. Führen Sie auf der Seite **Veröffentlichungseinstellungen** die folgenden Schritte aus, und klicken Sie dann auf **Weiter**:
  - Geben Sie im Feld **Name** einen Anzeigenamen für die Anwendung ein.  
Dieser Name wird nur in der Remotezugriffs-Verwaltungskonsole in der Liste der veröffentlichten Anwendungen verwendet.
  - Geben Sie im Feld **Externe URL** die externe URL für diese Anwendung ein, z. B. <https://sp.contoso.com/app1/>.
  - Wählen Sie in der Liste **Externes Zertifikat** ein Zertifikat aus, dessen Antragsteller die externe URL enthält.
  - Geben Sie im Feld **URL des Back-End-Servers** die URL des Back-End-Servers ein. Beachten Sie, dass dieser Wert automatisch eingegeben wird, wenn Sie die externe URL eingeben. Sie sollten Sie nur ändern, wenn sich die URL des Back-End-Servers unterscheidet. beispielsweise <https://sp/app1/>.

#### NOTE

Der webanwendungsproxy kann Hostnamen in URLs übersetzen, aber keine Pfadnamen übersetzen. Daher können Sie unterschiedliche Hostnamen eingeben, während der Pfadname gleich sein muss. Beispielsweise können Sie eine externe URL <https://apps.contoso.com/app1/> und eine Back-End-Server-URL https://app-server/app1/eingeben. Es ist jedoch nicht möglich, eine externe URL <https://apps.contoso.com/app1/> und eine Back-End-Server-URL <https://apps.contoso.com/internal-app1/> einzugeben.

7. Überprüfen Sie auf der Seite **Bestätigung** die Einstellungen, und klicken Sie dann auf **Veröffentlichen**. Sie können den PowerShell-Befehl kopieren, um weitere veröffentlichte Anwendungen einzurichten.
8. Überprüfen Sie auf der Seite **Ergebnisse**, ob die Anwendung veröffentlicht wurde, und klicken Sie dann auf **Schließen**.

#### von *entsprechenden Windows PowerShell-Befehlen*

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Add-WebApplicationProxyApplication
    -BackendServerURL 'https://sp.contoso.com/app1/'
    -ExternalCertificateThumbprint '1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b'
    -ExternalURL 'https://sp.contoso.com/app1/'
    -Name 'SP'
    -ExternalPreAuthentication ADFS
    -ADFSRelyingPartyName 'SP_Relying_Party'
```

## Veröffentlichen einer integrierten Windows Authenticated-basierten Anwendung für Webbrower Clients

Webanwendungsproxy kann zum Veröffentlichen von Anwendungen verwendet werden, die die integrierte Windows-Authentifizierung verwenden. Das heißt, der webanwendungsproxy führt die Vorauthentifizierung nach Bedarf durch und kann dann SSO für die veröffentlichte Anwendung durchführen, die die integrierte Windows-Authentifizierung verwendet. Um eine Anwendung zu veröffentlichen, die die integrierte Windows-Authentifizierung verwendet, müssen Sie dem Verbunddienst eine Ansprüche nicht unterstützende Vertrauensstellung der vertrauenden Seite für die Anwendung hinzufügen.

Damit der webanwendungsproxy Single Sign-on (SSO) ausführen und die Delegierung von Anmeldeinformationen mithilfe der eingeschränkten Kerberos-Delegierung durchführen kann, muss der webanwendungsproxy-Server einer Domäne beitreten Siehe [Plan Active Directory](#).

Um Benutzern den Zugriff auf Anwendungen zu ermöglichen, die die integrierte Windows-Authentifizierung verwenden, muss der webanwendungsproxy-Server in der Lage sein, Benutzern die Delegierung für die veröffentlichte Anwendung Diese Konfiguration kann auf dem Domänencontroller für jede Anwendung vorgenommen werden. Dies können Sie auch auf dem Back-End-Server tun, wenn er unter Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird. Weitere Informationen finden Sie unter [What's New in Kerberos Authentication](#).

Eine exemplarische Vorgehensweise zum Konfigurieren des webanwendungsproxys zum Veröffentlichen einer Anwendung mithilfe der integrierten Windows-Authentifizierung finden Sie unter [Konfigurieren eines Standorts für die Verwendung der integrierten Windows-Authentifizierung](#).

Bei der Verwendung der integrierten Windows-Authentifizierung für Back-End-Server ist die Authentifizierung zwischen webanwendungsproxy und der veröffentlichten Anwendung nicht Anspruchs basiert, sondern verwendet

die eingeschränkte Kerberos-Delegierung, um Endbenutzer bei der Anwendung zu authentifizieren. Der allgemeine Ablauf wird im Folgenden beschrieben:

1. Der Client versucht, mithilfe eines Webbrowsers auf eine nicht Anspruchs basierte Anwendung zuzugreifen. beispielsweise <https://appserver.contoso.com/nonclaimapp/>.
2. Der Webbrowser sendet eine HTTPS-Anforderung an den webanwendungsproxy-Server, der die Anforderung an den AD FS-Server umleitet.
3. Der AD FS Server authentifiziert den Benutzer und leitet die Anforderung zurück an den webanwendungsproxy. Die Anforderung enthält jetzt das Edgetoken.
4. Der webanwendungsproxy überprüft das Token.
5. Wenn das Token gültig ist, ruft der webanwendungsproxy im Auftrag des Benutzers ein Kerberos-Ticket vom Domänen Controller ab.
6. Der webanwendungsproxy fügt das Kerberos-Ticket der Anforderung als Teil des Simple und Protected spschgo (GSS-API-Aushandlungs Mechanismus)-Tokens hinzu und leitet die Anforderung an den Back-End-Server weiter. Da die Anforderung das Kerberos-Ticket enthält, wird dem Benutzer der Zugriff auf die Anwendung gewährt, ohne sich zusätzlich authentifizieren zu müssen.

In diesem Verfahren wird beschrieben, wie Sie eine Anwendung mit integrierter Windows-Authentifizierung, z. B. eine Outlook Web App, veröffentlichen, auf die von Webbrowserclients zugegriffen wird. Bevor Sie beginnen, sollten Sie sicherstellen, dass Sie Folgendes ausgeführt haben:

- Es wurde eine nicht Ansprüche unterstützende Vertrauensstellung der vertrauenden Seite für die Anwendung in der AD FS Management Console erstellt.
- Konfigurieren des Back-End-Servers zum Unterstützen der eingeschränkten Kerberos-Delegierung auf dem Domänencontroller oder mithilfe des Set-ADUser-Cmdlets mit dem Parameter %&quot;-PrincipalsAllowedToDelegateToAccount%&quot;. Beachten Sie Folgendes: Wenn der Back-End-Server unter Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, können Sie diesen PowerShell-Befehl auch auf dem Back-End-Server ausführen.
- Stellen Sie sicher, dass die webanwendungsproxy-Server für die Delegierung an die Dienst Prinzipal Namen der Back-End-Server
- Es wurde überprüft, ob ein Zertifikat auf dem webanwendungsproxy-Server für die zu veröffentlichte Anwendung geeignet ist.

#### **So veröffentlichen Sie eine nicht anspruchsisierte Anwendung**

1. Klicken Sie auf dem webanwendungsproxy-Server in der Remote Zugriffs-Verwaltungskonsole im **Navigations** Bereich auf **webanwendungsproxy**, und klicken Sie dann im Bereich **Tasks** auf **veröffentlichen**.
2. Klicken Sie auf der Seite **Willkommen** des Assistenten zum **Veröffentlichen neuer Anwendungen** auf **Weiter**.
3. Klicken Sie auf der Seite **Vorauthentifizierung** auf **Active Directory-Verbunddienste (AD FS) (AD FS)**, und klicken Sie dann auf **weiter**.
4. Wählen Sie auf der Seite **Unterstützte Clients** die Option **Web und MSOFBA** aus, und klicken Sie dann auf **Weiter**.
5. Wählen Sie auf der Seite **Vertrauende Seite** in der Liste die vertrauende Seite für die zu veröffentlichte Anwendung aus, und klicken Sie dann auf **Weiter**.
6. Führen Sie auf der Seite **Veröffentlichungseinstellungen** die folgenden Schritte aus, und klicken Sie dann

auf Weiter:

- Geben Sie im Feld **Name** einen Anzeigenamen für die Anwendung ein.  
Dieser Name wird nur in der Remotezugriffs-Verwaltungskonsole in der Liste der veröffentlichten Anwendungen verwendet.
- Geben Sie im Feld **Externe URL** die externe URL für diese Anwendung ein, z. B. <https://owa.contoso.com/>.
- Wählen Sie in der Liste **Externes Zertifikat** ein Zertifikat aus, dessen Antragsteller die externe URL enthält.
- Geben Sie im Feld **URL des Back-End-Servers** die URL des Back-End-Servers ein. Beachten Sie, dass dieser Wert automatisch eingegeben wird, wenn Sie die externe URL eingeben. Sie sollten Sie nur ändern, wenn sich die URL des Back-End-Servers unterscheidet. beispielsweise <https://owa/>.

**NOTE**

Der webanwendungsproxy kann Hostnamen in URLs übersetzen, aber keine Pfadnamen übersetzen. Daher können Sie unterschiedliche Hostnamen eingeben, während der Pfadname gleich sein muss. Beispielsweise können Sie eine externe URL <https://apps.contoso.com/app1/> und eine Back-End-Server-URL <https://app-server/app1/> eingeben. Es ist jedoch nicht möglich, eine externe URL <https://apps.contoso.com/app1/> und eine Back-End-Server-URL <https://apps.contoso.com/internal-app1/> einzugeben.

- Geben Sie im Feld **Dienstprinzipalname des Back-End-Servers** den Dienstprinzipalnamen für den Back-End-Server ein, %quot;z. B. HTTP/owa.contoso.com%quot;
7. Überprüfen Sie auf der Seite **Bestätigung** die Einstellungen, und klicken Sie dann auf **Veröffentlichen**. Sie können den PowerShell-Befehl kopieren, um weitere veröffentlichte Anwendungen einzurichten.
8. Überprüfen Sie auf der Seite **Ergebnisse**, ob die Anwendung veröffentlicht wurde, und klicken Sie dann auf **Schließen**.

 von *entsprechenden Windows PowerShell-Befehlen*

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

```
Add-WebApplicationProxyApplication
    -BackendServerAuthenticationSpn 'HTTP/owa.contoso.com'
    -BackendServerURL 'https://owa.contoso.com/'
    -ExternalCertificateThumbprint '1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b'
    -ExternalURL 'https://owa.contoso.com/'
    -Name 'OWA'
    -ExternalPreAuthentication ADFS
    -ADFSRelyingPartyName 'Non-Claims_Relying_Party'
```

## Veröffentlichen einer Anwendung, die MS-ofba verwendet

Webanwendungsproxy unterstützt den Zugriff von Microsoft Office Clients wie Microsoft Word, die auf Dokumente und Daten auf Back-End-Servern zugreifen. Der einzige Unterschied zwischen diesen Anwendungen und einem Standardbrowser besteht darin, dass die Umleitung zum Sicherheitstokendienst nicht über eine reguläre HTTP-Umleitung erfolgt, sondern mit speziellen MS-ofba-Headern, wie in:

[https://msdn.microsoft.com/library/dd773463\(v=office.12\).aspx](https://msdn.microsoft.com/library/dd773463(v=office.12).aspx) angegeben. Die Back-End-Anwendung kann die anspruchsisierte Authentifizierung oder die integrierte Windows-Authentifizierung verwenden.

Zum Veröffentlichen einer Anwendung für Clients, die MS-ofba verwenden, müssen Sie der Verbunddienst eine Vertrauensstellung der vertrauenden Seite für die Anwendung hinzufügen. Je nach Anwendung können Sie die anspruchsisierte Authentifizierung oder die integrierte Windows-Authentifizierung verwenden. Daher muss die entsprechende Vertrauensstellung der vertrauenden Seite für die Anwendung hinzugefügt werden.

Damit der webanwendungsproxy Single Sign-on (SSO) ausführen und die Delegierung von Anmelde Informationen mithilfe der eingeschränkten Kerberos-Delegierung durchführen kann, muss der webanwendungsproxy-Server einer Domäne beitreten Siehe [Plan Active Directory](#).

Wenn die Anwendung die anspruchsisierte Authentifizierung verwendet, sind keine weiteren Planungsschritte erforderlich. Wenn die Anwendung die integrierte Windows-Authentifizierung verwendet hat, finden Sie weitere Informationen unter [Veröffentlichen einer integrierten Windows Authenticated-basierten Anwendung für Webbrowser Clients](#).

Der Authentifizierungs Ablauf für Clients, die das MS-ofba-Protokoll mithilfe der Anspruchs basierten Authentifizierung verwenden, wird im folgenden beschrieben. Bei der Authentifizierung für dieses Szenario kann das Anwendungstoken in der URL oder im Textkörper verwendet werden.

1. Der Benutzer arbeitet in einem Office-Programm und öffnet über die Liste **Zuletzt verwendete Dokumente** eine Datei auf einer SharePoint-Website.
2. Das Office-Programm zeigt ein Fenster mit einem Browsersteuerelement an, in dem der Benutzer Anmeldeinformationen eingeben muss.

**NOTE**

In manchen Fällen wird das Fenster möglicherweise nicht angezeigt, weil der Client bereits authentifiziert ist.

3. Der webanwendungsproxy leitet die Anforderung an den AD FS-Server um, der die Authentifizierung ausführt.
4. Der AD FS Server leitet die Anforderung zurück an den webanwendungsproxy. Die Anforderung enthält jetzt das Edgetoken.
5. Der AD FS Server fügt der Anforderung ein Single Sign-on-Cookie (SSO) hinzu, da der Benutzer bereits eine Authentifizierung für den AD FS Server durchgeführt hat.
6. Der webanwendungsproxy überprüft das Token und leitet die Anforderung an den Back-End-Server weiter.
7. Der Back-End-Server leitet die Anforderung an den AD FS-Server um, um das Anwendungs Sicherheits Token zu erhalten.
8. Die Anforderung wird an den Back-End-Server umgeleitet. Die Anforderung enthält jetzt das Anwendungstoken und das SSO-Cookie. Dem Benutzer wird Zugriff auf die SharePoint-Website gewährt, ohne zum Anzeigen der Datei einen Benutzernamen oder ein Kennwort eingeben zu müssen.

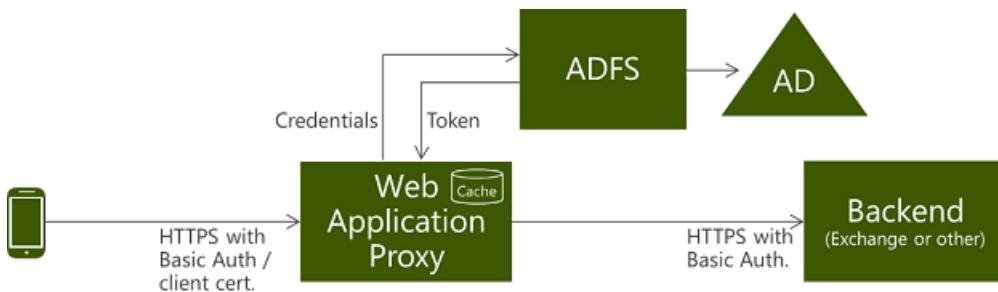
Die Schritte zum Veröffentlichen einer Anwendung, die MS-ofba verwendet, sind identisch mit den Schritten für eine Anspruchs basierte Anwendung oder eine nicht Anspruchs basierte Anwendung. Informationen zu Anspruchs basierten Anwendungen finden Sie unter Veröffentlichen einer Anspruchs basierten Anwendung für Webbrowser Clients für nicht Anspruchs basierte Anwendungen. Weitere Informationen finden Sie unter [Veröffentlichen einer integrierten Windows Authenticated-basierten Anwendung für Webbrowser Clients](#). Der webanwendungsproxy erkennt den Client automatisch und authentifiziert den Benutzer bei Bedarf.

## Veröffentlichen einer Anwendung, die HTTP Basic verwendet

HTTP Basic ist das Autorisierungs Protokoll, das von vielen Protokollen verwendet wird, um Rich-Clients, einschließlich Smartphones, mit Ihrem Exchange-Postfach zu verbinden. Weitere Informationen zu HTTP Basic

finden Sie unter [RFC 2617](#). Der webanwendungsproxy interagiert traditionell mit AD FS mithilfe von Umleitungen. die meisten Rich-Clients unterstützen keine Cookies oder Zustands Verwaltung. Auf diese Weise ermöglicht der webanwendungsproxy der http-APP, eine nicht anspruchsvolle Vertrauensstellung der vertrauenden Seite für die Anwendung für die Verbunddienst zu empfangen. Siehe [Plan Active Directory](#).

Der Authentifizierungs Ablauf für Clients, die HTTP Basic verwenden, wird im folgenden und in diesem Diagramm beschrieben:



1. Der Benutzer versucht, auf eine veröffentlichte Webanwendung einen Telefon Client zuzugreifen.
2. Die APP sendet eine HTTPS-Anforderung an die vom webanwendungsproxy veröffentlichte URL.
3. Wenn die Anforderung keine Anmelde Informationen enthält, gibt der webanwendungsproxy eine HTTP 401-Antwort an die APP zurück, die die URL des authentifizierenden AD FS Servers enthält.
4. Der Benutzer sendet die HTTPS-Anforderung erneut an die APP, wobei die Autorisierung im HTTPS-Authenticate-Anforderungs Header auf Basic und Benutzername und auf Basis 64 verschlüsseltes Kennwort des Benutzers festgelegt ist.
5. Da das Gerät nicht an AD FS umgeleitet werden kann, sendet der webanwendungsproxy eine Authentifizierungsanforderung an AD FS mit den Anmelde Informationen, einschließlich Benutzername und Kennwort. Das Token wird im Namen des Geräts abgerufen.
6. Um die Anzahl der an den AD FS gesendeten Anforderungen, den webanwendungsproxy, zu minimieren, überprüft nachfolgende Client Anforderungen mithilfe zwischen gespeicherter Token, solange das Token gültig ist. Der webanwendungsproxy bereinigt den Cache regelmäßig. Sie können die Größe des Caches mithilfe des Leistungs Zählers anzeigen.
7. Wenn das Token gültig ist, leitet der webanwendungsproxy die Anforderung an den Back-End-Server weiter, und dem Benutzer wird Zugriff auf die veröffentlichte Webanwendung gewährt.

Im folgenden Verfahren wird erläutert, wie http-Basisanwendungen veröffentlicht werden.

#### **So veröffentlichen Sie eine HTTP-Basisanwendung**

1. Klicken Sie auf dem webanwendungsproxy-Server in der Remote Zugriffs-Verwaltungskonsole im **Navigations** Bereich auf **webanwendungsproxy**, und klicken Sie dann im Bereich **Tasks** auf **veröffentlichen**.
2. Klicken Sie auf der Seite **Willkommen des Assistenten zum Veröffentlichen neuer Anwendungen** auf **Weiter**.
3. Klicken Sie auf der Seite **Vorauthentifizierung** auf **Active Directory-Verbunddienste (AD FS)** (AD FS), und klicken Sie dann auf **weiter**.
4. Wählen Sie auf der Seite **Unterstützte Clients** die Option **HTTP Basic** aus, und klicken Sie auf **weiter**.

Wenn Sie den Zugriff auf Exchange nur über mit dem Arbeitsplatz verbundene Geräte aktivieren möchten, aktivieren Sie das **Kontrollkästchen Zugriff nur für mit dem Arbeitsplatz verbundene Geräte aktivieren**. Weitere Informationen finden [Sie unter Verbinden mit einem Arbeitsplatz von einem beliebigen Gerät für SSO und nahtlose zweistufige Authentifizierung bei allen Unternehmensanwendungen](#).

5. Wählen Sie auf der Seite **Vertrauende Seite** in der Liste die vertrauende Seite für die zu veröffentlichte Anwendung aus, und klicken Sie dann auf **Weiter**. Beachten Sie, dass diese Liste nur auf Ansprüche abhängige Seiten enthält.
6. Führen Sie auf der Seite **Veröffentlichungseinstellungen** die folgenden Schritte aus, und klicken Sie dann auf **Weiter**:
  - Geben Sie im Feld **Name** einen Anzeigenamen für die Anwendung ein.  
Dieser Name wird nur in der Remotezugriffs-Verwaltungskonsole in der Liste der veröffentlichten Anwendungen verwendet.
  - Geben Sie im Feld **externe URL** die externe URL für diese Anwendung ein. Beispiel: Mail.contoso.com
  - Wählen Sie in der Liste **Externes Zertifikat** ein Zertifikat aus, dessen Antragsteller die externe URL enthält.
  - Geben Sie im Feld **URL des Back-End-Servers** die URL des Back-End-Servers ein. Beachten Sie, dass dieser Wert automatisch eingegeben wird, wenn Sie die externe URL eingeben. Sie sollten Sie nur ändern, wenn sich die URL des Back-End-Servers unterscheidet. beispielsweise Mail.contoso.com.
7. Überprüfen Sie auf der Seite **Bestätigung** die Einstellungen, und klicken Sie dann auf **Veröffentlichen**. Sie können den PowerShell-Befehl kopieren, um weitere veröffentlichte Anwendungen einzurichten.
8. Überprüfen Sie auf der Seite **Ergebnisse**, ob die Anwendung veröffentlicht wurde, und klicken Sie dann auf **Schließen**.

#### von *entsprechenden Windows PowerShell-Befehlen*

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

Dieses Windows PowerShell-Skript ermöglicht die Vorauthentifizierung für alle Geräte, nicht nur für Arbeitsplatz verbundene Geräte.

```
Add-WebApplicationProxyApplication
  -BackendServerUrl 'https://mail.contoso.com'
  -ExternalCertificateThumbprint '697F4FF0B9947BB8203A96ED05A3021830638E50'
  -ExternalUrl 'https://mail.contoso.com'
  -Name 'Exchange'
  -ExternalPreAuthentication ADFSforRichClients
  -ADFSRelyingPartyName 'EAS_Relying_Party'
```

Im folgenden werden nur mit dem Arbeitsplatz verbundene Geräte vorab authentifiziert:

```
Add-WebApplicationProxyApplication
  -BackendServerUrl 'https://mail.contoso.com'
  -ExternalCertificateThumbprint '697F4FF0B9947BB8203A96ED05A3021830638E50'
  -EnableHTTPRedirect:$true
  -ExternalUrl 'https://mail.contoso.com'
  -Name 'Exchange'
  -ExternalPreAuthentication ADFSforRichClients
  -ADFSRelyingPartyName 'EAS_Relying_Party'
```

**Veröffentlichen einer Anwendung, die OAuth2 verwendet, z. B. eine Microsoft Store-App**

Zum Veröffentlichen einer Anwendung für Microsoft Store-Apps müssen Sie der Verbunddienst eine Vertrauensstellung der vertrauenden Seite für die Anwendung hinzufügen.

Damit der webanwendungsproxy Single Sign-on (SSO) ausführen und die Delegierung von Anmelde Informationen mithilfe der eingeschränkten Kerberos-Delegierung durchführen kann, muss der webanwendungsproxy-Server einer Domäne beitreten Siehe [Plan Active Directory](#).

**NOTE**

Webanwendungsproxy unterstützt die Veröffentlichung nur für Microsoft Store-Apps, die das OAuth 2,0-Protokoll verwenden

In der AD FS-Verwaltungskonsole müssen Sie sicherstellen, dass der OAuth-Endpunkt Proxy aktiviert ist. Öffnen Sie dazu die AD FS-Verwaltungskonsole, erweitern Sie den Knoten **Dienst**, klicken Sie auf **Endpunkte**, suchen Sie in der Liste **Endpunkte** nach dem OAuth-Endpunkt, und vergewissern Sie sich, dass in der Spalte **Proxy aktiviert** der Wert **Ja** angezeigt wird.

Der Authentifizierungs Ablauf für Clients, die Microsoft Store-Apps verwenden, wird im folgenden beschrieben:

**NOTE**

Der webanwendungsproxy leitet zur Authentifizierung an den AD FS-Server weiter. Da Microsoft Store-Apps Umleitungen nicht unterstützen, ist es erforderlich, die URL des AD FS Servers mithilfe des Cmdlets Set-webapplicationproxyconfiguration und des oauthauthenticationurl-Parameters festzulegen, wenn Sie Microsoft Store-Apps verwenden.

Microsoft Store-Apps können nur mithilfe von Windows PowerShell veröffentlicht werden.

1. Der Client versucht, mithilfe einer Microsoft Store-App auf eine veröffentlichte Webanwendung zuzugreifen.
2. Die APP sendet eine HTTPS-Anforderung an die vom webanwendungsproxy veröffentlichte URL.
3. Der webanwendungsproxy gibt eine HTTP 401-Antwort an die APP zurück, die die URL des authentifizierenden AD FS Servers enthält. Dieser Prozess wird als "Ermittlung" bezeichnet.

**NOTE**

Wenn die APP die URL des authentifizierenden AD FS Servers kennt und bereits über ein Kombinations Token verfügt, das das OAuth-Token und das edgetoken enthält, werden die Schritte 2 und 3 in diesem Authentifizierungs Ablauf übersprungen.

4. Die APP sendet eine HTTPS-Anforderung an den AD FS-Server.
5. Die APP generiert mithilfe des Webauthentifizierungs Brokers ein Dialogfeld, in dem der Benutzer Anmelde Informationen für die Authentifizierung beim AD FS Server eingibt. Informationen zum Webauthentifizierungsbroker finden Sie unter [Webauthentifizierungsbroker](#).
6. Nach erfolgreicher Authentifizierung erstellt der AD FS-Server ein Kombinations Token, das das OAuth-Token und das edgetoken enthält, und sendet das Token an die app.
7. Die APP sendet eine HTTPS-Anforderung mit dem Kombinations Token an die vom webanwendungsproxy veröffentlichte URL.
8. Der webanwendungsproxy teilt das Kombinations Token in seine zwei Teile auf und überprüft das edgetoken.
9. Wenn das edgetoken gültig ist, leitet der webanwendungsproxy die Anforderung nur mit dem OAuth-Token an den Back-End-Server. Dem Benutzer wird der Zugriff auf die veröffentlichte Webanwendung gewährt.

Hier wird beschrieben, wie Sie eine Anwendung für OAuth2 veröffentlichen. Diese Art von Anwendung kann nur mithilfe von Windows PowerShell veröffentlicht werden. Bevor Sie beginnen, sollten Sie sicherstellen, dass Sie Folgendes ausgeführt haben:

- Es wurde eine Vertrauensstellung der vertrauenden Seite für die Anwendung in der AD FS Management Console erstellt.
- Stellen Sie sicher, dass der OAuth-Endpunkt in der AD FS-Verwaltungskonsole Proxy aktiviert ist, und notieren Sie sich den URL-Pfad.
- Es wurde überprüft, ob ein Zertifikat auf dem webanwendungsproxy-Server für die zu veröffentlichte Anwendung geeignet ist.

#### So veröffentlichen Sie eine OAuth2-App

1. Klicken Sie auf dem webanwendungsproxy-Server in der Remote Zugriffs-Verwaltungskonsole im **Navigations** Bereich auf **webanwendungsproxy**, und klicken Sie dann im Bereich **Tasks** auf **veröffentlichen**.
2. Klicken Sie auf der Seite **Willkommen des Assistenten zum Veröffentlichen neuer Anwendungen** auf **Weiter**.
3. Klicken Sie auf der Seite **Vorauthentifizierung** auf **Active Directory-Verbunddienste (AD FS) (AD FS)**, und klicken Sie dann auf **weiter**.
4. Wählen Sie auf der Seite **Unterstützte Clients OAuth2** aus, und klicken Sie dann auf **weiter**.
5. Wählen Sie auf der Seite **Vertrauende Seite** in der Liste die vertrauende Seite für die zu veröffentlichte Anwendung aus, und klicken Sie dann auf **Weiter**.
6. Führen Sie auf der Seite **Veröffentlichungseinstellungen** die folgenden Schritte aus, und klicken Sie dann auf **Weiter**:
  - Geben Sie im Feld **Name** einen Anzeigenamen für die Anwendung ein.  
Dieser Name wird nur in der Remotezugriffs-Verwaltungskonsole in der Liste der veröffentlichten Anwendungen verwendet.
  - Geben Sie im Feld **Externe URL** die externe URL für diese Anwendung ein, z. B. <https://server1.contoso.com/app1/>.
  - Wählen Sie in der Liste **Externes Zertifikat** ein Zertifikat aus, dessen Antragsteller die externe URL enthält.  
Um sicherzustellen, dass Ihre Benutzer auf Ihre App zugreifen können, aktivieren Sie das Kontrollkästchen **http-zu-HTTPS-Umleitung aktivieren**, auch wenn Sie in der URL nicht den Typ HTTPS eingeben.
  - Geben Sie im Feld **URL des Back-End-Servers** die URL des Back-End-Servers ein. Beachten Sie, dass dieser Wert automatisch eingegeben wird, wenn Sie die externe URL eingeben. Sie sollten Sie nur ändern, wenn sich die URL des Back-End-Servers unterscheidet. beispielsweise <https://sp/app1/>.

#### NOTE

Der webanwendungsproxy kann Hostnamen in URLs übersetzen, aber keine Pfadnamen übersetzen. Daher können Sie unterschiedliche Hostnamen eingeben, während der Pfadname gleich sein muss. Beispielsweise können Sie eine externe URL <https://apps.contoso.com/app1/> und eine Back-End-Server-URL <https://app-server/app1/> eingeben. Es ist jedoch nicht möglich, eine externe URL <https://apps.contoso.com/app1/> und eine Back-End-Server-URL <https://apps.contoso.com/internal-app1/> einzugeben.

7. Überprüfen Sie auf der Seite **Bestätigung** die Einstellungen, und klicken Sie dann auf **Veröffentlichen**. Sie können den PowerShell-Befehl kopieren, um weitere veröffentlichte Anwendungen einzurichten.
8. Überprüfen Sie auf der Seite **Ergebnisse**, ob die Anwendung veröffentlicht wurde, und klicken Sie dann auf **Schließen**.

Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen unterbrochen sein können.

So legen Sie die URL für die OAuth-Authentifizierung für eine Verbund Server Adresse von FS.contoso.com und den URL-Pfad/ADFS/oauth2/fest:

```
Set-WebApplicationProxyConfiguration -OAuthAuthenticationURL 'https://fs.contoso.com/adfs/oauth2/'
```

So veröffentlichen Sie die Anwendung

```
Add-WebApplicationProxyApplication  
-BackendServerURL 'https://storeapp.contoso.com/'  
-ExternalCertificateThumbprint '1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b'  
-ExternalURL 'https://storeapp.contoso.com/'  
-Name 'Microsoft Store app Server'  
-ExternalPreAuthentication ADFS  
-ADFSRelyingPartyName 'Store_app_Relying_Party'  
-UseOAuthAuthentication
```

## Siehe auch

- [Problembehandlung: Webanwendungsproxy](#)
- [Anwendungen über den webanwendungsproxy veröffentlichen](#)
- [Planen der Veröffentlichung von Anwendungen mit webanwendungsproxy](#)
- [Leitfaden für webanwendungsproxy](#)
- [Webanwendungsproxy-Cmdlets in Windows PowerShell](#)
- [Add-webapplicationproxyapplication](#)
- [Set-webapplicationproxyconfiguration](#)

# Veröffentlichen von Anwendungen mit SharePoint, Exchange und RDG

11.04.2020 • 17 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

Diese Inhalte sind für die lokale Version des webanwendungsproxys relevant. Informationen zum Aktivieren des sicheren Zugriffs auf lokale Anwendungen über die Cloud finden Sie in den [Azure AD Anwendungs Proxy-Inhalt](#).

In diesem Thema werden die erforderlichen Aufgaben zum Veröffentlichen von SharePoint Server, Exchange Server oder Remotedesktop Gateway (RDP) über den webanwendungsproxy beschrieben.

## NOTE

Diese Informationen werden unverändert bereitgestellt. Remotedesktopdienste unterstützt und empfiehlt [die Verwendung Azure-App Proxys, um sicheren Remote Zugriff auf lokale Anwendungen bereitzustellen](#).

## Veröffentlichen von SharePoint Server

Sie können eine SharePoint-Website mithilfe des webanwendungsproxys veröffentlichen, wenn die SharePoint-Website für die Anspruchs basierte Authentifizierung oder die integrierte Windows-Authentifizierung konfiguriert ist. Wenn Sie Active Directory-Verbunddienste (AD FS) (AD FS) für die Vorauthentifizierung verwenden möchten, müssen Sie eine vertrauende Seite mithilfe eines der Assistenten konfigurieren.

- Wenn die SharePoint-Website die anspruchsbasierte Authentifizierung verwendet, müssen Sie den Assistenten zum Hinzufügen der Vertrauensstellung der vertrauenden Seite für die Anwendung verwenden.
- Wenn die SharePoint-Website die integrierte Windows-Authentifizierung verwendet, müssen Sie den nicht anspruchsbasierten Assistenten zum Hinzufügen der Vertrauensstellung der vertrauenden Seite für die Anwendung verwenden. IWA kann mit einer anspruchsbasierten Webanwendung genutzt werden, sofern KDC entsprechend konfiguriert ist.

Um Benutzern die Authentifizierung mithilfe der integrierten Windows-Authentifizierung zu ermöglichen, muss der webanwendungsproxy-Server einer Domäne hinzugefügt werden.

Sie müssen die Anwendung zur Unterstützung der eingeschränkten Kerberos-Delegierung konfigurieren. Diese Konfiguration kann auf dem Domänencontroller für jede Anwendung vorgenommen werden. Sie können die Anwendung auch direkt auf dem Back-End-Server konfigurieren, wenn Sie unter Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird. Weitere Informationen finden Sie unter [What's New in Kerberos Authentication](#). Außerdem müssen Sie sicherstellen, dass die webanwendungsproxy-Server für die Delegierung der Dienst Prinzipal Namen der Back-End-Server konfiguriert sind. Eine exemplarische Vorgehensweise zum Konfigurieren des webanwendungsproxys zum Veröffentlichen einer Anwendung mithilfe der integrierten Windows-Authentifizierung finden Sie unter [Konfigurieren eines Standorts für die Verwendung der integrierten Windows-Authentifizierung](#).

Wenn die SharePoint-Website mithilfe alternativer Zugriffszuordnungen (AAM) oder hostbenannter Websitesammlungen konfiguriert ist, können Sie jeweils verschiedene URLs der externen und Back-End-Server zur Veröffentlichung Ihrer Anwendung verwenden. Wenn die SharePoint-Website jedoch nicht mithilfe von AAM oder hostbenannten Websitesammlungen konfiguriert ist, müssen Sie jeweils die gleichen externen und Back-End-

Server-URLs verwenden.

## Veröffentlichen von Exchange Server

In der folgenden Tabelle werden die Exchange-Dienste beschrieben, die Sie über den webanwendungsproxy veröffentlichen können, sowie die unterstützte Vorauthentifizierung für diese Dienste:

EXCHANGE-DIENST	VORAUTHENTIFIZIERUNG	HINWEISE
Outlook Web App	-AD FS mit nicht Anspruchs basierter Authentifizierung -Pass-Through -AD FS verwenden der Anspruchs basierten Authentifizierung für lokales Exchange 2013 Service Pak 1 (SP1)	Weitere Informationen finden Sie unter: <a href="#">Verwenden anspruchsbasierter Authentifizierung von AD FS mit Outlook Web App und EAC</a>
Exchange-Systemsteuerung	Pass-Through	
Outlook Anywhere	Pass-Through	Zur ordnungsgemäßen Funktion müssen drei URLs für Outlook Anywhere veröffentlicht werden: : Die automatische Erkennung-URL. -Der externe Hostname des Exchange-Servers. Das heißt, die URL, die für Clients zum Herstellen einer Verbindung konfiguriert ist. : Der interne voll qualifizierte Namen des Exchange-Servers.
Exchange ActiveSync	Pass-Through AD FS mithilfe des HTTP-Standard Autorisierungs Protokolls	

Um Outlook Web App mithilfe der integrierten Windows-Authentifizierung zu veröffentlichen, müssen Sie den nicht anspruchsbasierten Assistenten zum Hinzufügen der Vertrauensstellung der vertrauenden Seite für die Anwendung verwenden.

Um Benutzern die Authentifizierung mithilfe der eingeschränkten Kerberos-Delegierung zu ermöglichen, muss der webanwendungsproxy-Server einer Domäne hinzugefügt werden.

Sie müssen die Anwendung so konfigurieren, dass die Kerberos-Authentifizierung unterstützt wird. Außerdem müssen Sie einen Dienst Prinzipal Namen (Service Principal Name, SPN) für das Konto registrieren, unter dem der Webdienst ausgeführt wird. Dies ist auf dem Domänen Controller oder auf den Back-End-Servern möglich. In einer Exchange-Umgebung mit Lastenausgleich erfordert dies die Verwendung des alternativen Dienst Kontos. Weitere Informationen finden Sie unter [Konfigurieren der Kerberos-Authentifizierung für Client Zugriffs Server mit Lasten Ausgleich](#).

Sie können die Anwendung auch direkt auf dem Back-End-Server konfigurieren, wenn Sie unter Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird. Weitere Informationen finden Sie unter [What's New in Kerberos Authentication](#). Außerdem müssen Sie sicherstellen, dass die webanwendungsproxy-Server für die Delegierung der Dienst Prinzipal Namen der Back-End-Server konfiguriert sind.

## Veröffentlichen Remotedesktop Gateways über den webanwendungsproxy

Wenn Sie den Zugriff auf das Remote Zugriffs Gateway einschränken und die Vorauthentifizierung für den Remote

Zugriff hinzufügen möchten, können Sie es über den webanwendungsproxy ausführen. Dies ist eine sehr gute Möglichkeit, um sicherzustellen, dass Sie über eine umfassende Vorauthentifizierung für RDG einschließlich MFA verfügen. Die Veröffentlichung ohne Vorauthentifizierung ist ebenfalls eine Option und bietet einen einzigen Einstiegspunkt in Ihre Systeme.

#### **Veröffentlichen einer Anwendung in RDG mithilfe der Proxy-Passthrough-Authentifizierung für den webanwendungsproxy**

1. Die Installation unterscheidet sich abhängig davon, ob sich die Rollen für RD-Webzugriff (/RDWeb) und RD-Gateway (RPC) auf demselben Server oder auf unterschiedlichen Servern befinden.
  2. Wenn die RD-Webzugriff und RD-Gateway Rollen auf demselben RDG-Server gehostet werden, können Sie einfach den Stamm-FQDN im webanwendungsproxy wie <https://rdg.contoso.com/veröffentlichen>.
- Sie können die beiden virtuellen Verzeichnisse auch einzeln veröffentlichen, z.
- b.<https://rdg.contoso.com/rdweb/> und <https://rdg.contoso.com/rpc/>.
3. Wenn die RD-Webzugriff und die RD-Gateway auf separaten RDG-Servern gehostet werden, müssen Sie die beiden virtuellen Verzeichnisse einzeln veröffentlichen. Sie können dieselben oder andere externe voll qualifizierte Namen (z. B. <https://rdweb.contoso.com/rdweb/> und <https://gateway.contoso.com/rpc/>) verwenden.
  4. Wenn sich der externe und interne voll qualifizierte Dateityp unterscheiden, sollten Sie die Übersetzung der Anforderungs Kopfzeile für die RDWeb-Veröffentlichungs Regel nicht deaktivieren. Dies kann durch Ausführen des folgenden PowerShell-Skripts auf dem webanwendungsproxy-Server erreicht werden, sollte jedoch standardmäßig aktiviert werden.

```
Get-WebApplicationProxyApplication applicationname | Set-WebApplicationProxyApplication -  
DisableTranslateUrlInRequestHeaders:$false
```

#### **NOTE**

Wenn Sie umfangreiche Clients wie RemoteApp- und Desktop Verbindungen oder IOS-Remotedesktop Verbindungen unterstützen müssen, unterstützen diese keine Vorauthentifizierung, sodass Sie RDG mithilfe der Passthrough-Authentifizierung veröffentlichen müssen.

#### **Veröffentlichen einer Anwendung in RDG mithilfe des webanwendungsproxys mit Vorauthentifizierung**

1. Die Vorauthentifizierung des webanwendungsproxys bei RDG funktioniert, indem das von Internet Explorer erhaltene vorauthentifizierungs Cookie an den Remotedesktopverbindung-Client (mstsc. exe) übergeben wird. Diese wird dann vom Remotedesktopverbindung Client (mstsc. exe) verwendet. Diese wird dann von Remotedesktopverbindung Client als Authentifizierungs Nachweis verwendet.

Im folgenden Verfahren wird der Sammlungs Server aufgefordert, die erforderlichen benutzerdefinierten RDP-Eigenschaften in den RDP-Dateien der Remote-app einzuschließen, die an Clients gesendet werden. Diese weisen den Client an, dass eine Vorauthentifizierung erforderlich ist, und dass die Cookies für die Server Adresse für die Vorauthentifizierung an Remotedesktopverbindung Client (mstsc. exe) übergeben werden. In Verbindung mit der Deaktivierung der Funktion HttpOnly in der webanwendungsproxy-Anwendung ermöglicht der Remotedesktopverbindung Client (mstsc. exe) das Verwenden des webanwendungsproxy-Cookies, das über den Browser abgerufen wird.

Die Authentifizierung beim RD-Webzugriff Server verwendet weiterhin die RD-Webzugriff Formular Anmeldung. Dies bietet die geringste Anzahl von Eingabe Aufforderungen für die Benutzeroauthentifizierung, da das RD-Webzugriff Anmeldeformular einen Client seitigen Anmelde Informationsspeicher erstellt, der dann von Remotedesktopverbindung Client (mstsc. exe) für alle nachfolgenden Remote-App-Starts verwendet werden kann.

2. Erstellen Sie zunächst eine manuelle Vertrauensstellung der vertrauenden Seite in AD FS so, als ob Sie eine

Ansprüche unterstützende App veröffentlichen. Dies bedeutet, dass Sie eine Dummy-Vertrauensstellung der vertrauenden Seite erstellen müssen, um die Vorauthentifizierung zu erzwingen, damit Sie die Vorauthentifizierung ohne eingeschränkte Kerberos-Delegierung für den veröffentlichten Server erhalten. Nachdem sich ein Benutzer authentifiziert hat, wird alles andere weitergeleitet.

**WARNING**

Möglicherweise ist die Verwendung der Delegierung vorzuziehen, aber Sie löst die mstsc-SSO-Anforderungen nicht vollständig aus, und es gibt Probleme bei der Delegierung an das/RPC-Verzeichnis, da der Client erwartet, dass die RD-Gateway Authentifizierung selbst verarbeitet wird.

3. Führen Sie die Schritte in der AD FS Management Console aus, um eine manuelle Vertrauensstellung der vertrauenden Seite zu erstellen:

- a. Verwenden des Assistenten zur Vertrauensstellung der **vertrauenden Seite hinzufügen**
  - b. Wählen Sie die Option **Daten über die vertrauende Seite manuell eingeben**.
  - c. Akzeptieren Sie alle Standardeinstellungen.
- d. Geben Sie für den Bezeichner der vertrauenden Seite den externen voll qualifizierten Namen ein, den Sie für den RDG-Zugriff verwenden möchten, z. b. <https://rdg.contoso.com/>.

Dies ist die Vertrauensstellung der vertrauenden Seite, die Sie beim Veröffentlichen der APP im webanwendungsproxy verwenden.

4. Veröffentlichen Sie den Stamm der Site (z. b. <https://rdg.contoso.com/>) im webanwendungsproxy. Legen Sie die Vorauthentifizierung auf AD FS fest, und verwenden Sie die zuvor erstellte Vertrauensstellung der vertrauenden Seite. Dies ermöglicht RDWeb und/RPC, das gleiche webanwendungsproxy-Authentifizierungs Cookie zu verwenden.

Es ist möglich,/RDWeb und/RPC als separate Anwendungen zu veröffentlichen und sogar andere veröffentlichte Server zu verwenden. Sie müssen lediglich sicherstellen, dass Sie beide mit derselben Vertrauensstellung der vertrauenden Seite veröffentlichen, da das webanwendungsproxy-Token für die Vertrauensstellung der vertrauenden Seite ausgegeben wird

5. Wenn sich der externe und interne voll qualifizierte Dateityp unterscheiden, sollten Sie die Übersetzung der Anforderungs Kopfzeile für die RDWeb-Veröffentlichungs Regel nicht deaktivieren. Dies kann durch Ausführen des folgenden PowerShell-Skripts auf dem webanwendungsproxy-Server erreicht werden, sollte jedoch standardmäßig aktiviert sein:

```
Get-WebApplicationProxyApplication applicationname | Set-WebApplicationProxyApplication -  
DisableTranslateUrlInRequestHeaders:$true
```

6. Deaktivieren Sie die HttpOnly-Cookie-Eigenschaft im webanwendungsproxy für die veröffentlichte RDG-Anwendung. Um dem RDG-ActiveX-Steuerelement Zugriff auf das webanwendungsproxy-Authentifizierungs Cookie zu ermöglichen, müssen Sie die HttpOnly-Eigenschaft im webanwendungsproxy-Cookie deaktivieren.

Hierfür müssen Sie das Updaterollup vom [November 2014 für Windows RT 8.1, Windows 8.1 und Windows Server 2012 R2 \(KB3000850\)](#) installieren.

Führen Sie nach der Installation des Hotfixes das folgende PowerShell-Skript auf dem webanwendungsproxy-Server aus, und geben Sie den entsprechenden Anwendungsnamen

```
Get-WebApplicationProxyApplication applicationname | Set-WebApplicationProxyApplication -  
DisableHttpOnlyCookieProtection:$true
```

Das Deaktivieren von HttpOnly ermöglicht dem RDG-ActiveX-Steuerelement den Zugriff auf das webanwendungsproxy-Authentifizierungs Cookie

7. Konfigurieren Sie die relevante RDG-Sammlung auf dem Sammlungs Server so, dass der Remotedesktopverbindung Client (mstsc. exe) weiß, dass die Vorauthentifizierung in der RDP-Datei erforderlich ist.

- In Windows Server 2012 und Windows Server 2012 R2 kann dies erreicht werden, indem Sie auf dem RDG-Sammlungs Server das folgende PowerShell-Cmdlet ausführen:

```
Set-RDSessionCollectionConfiguration -CollectionName "<yourcollectionname>" -CustomRdpProperty  
"pre-authentication server address:s: <https://externalfqdn/rdweb/>`nrequire pre-  
authentication:i:1"
```

Stellen Sie sicher, dass Sie die < und > Klammern entfernen, wenn Sie durch ihre eigenen Werte ersetzen, z. b.:

```
Set-RDSessionCollectionConfiguration -CollectionName "MyAppCollection" -CustomRdpProperty "pre-  
authentication server address:s: https://rdg.contoso.com/rdweb/`nrequire pre-authentication:i:1"
```

- In Windows Server 2008 R2:
  - Melden Sie sich auf dem Terminal Server mit einem Konto an, das über Administrator Rechte verfügt.
  - Wechseln Sie zu **Start >Verwaltungs Tools > Terminal Dienste > TS RemoteApp-Manager**.
  - Klicken Sie im Bereich **Übersicht** von TS RemoteApp-Manager neben RDP-Einstellungen auf **ändern**.
  - Geben Sie auf der Registerkarte **Benutzerdefinierte RDP-Einstellungen** die folgenden RDP-Einstellungen in das Feld Benutzerdefinierte RDP-Einstellungen ein:

```
pre-authentication server address: s: https://externalfqdn/rdweb/
```

```
require pre-authentication:i:1
```

- e. Wenn Sie dies abgeschlossen haben, **Klicken Sie auf übernehmen**.

Dadurch wird der Sammlungs Server aufgefordert, die benutzerdefinierten RDP-Eigenschaften in die RDP-Dateien einzuschließen, die an Clients gesendet werden. Diese weisen den Client an, dass eine Vorauthentifizierung erforderlich ist, und dass die Cookies für die Server Adresse der Vorauthentifizierung an den Remotedesktopverbindung-Client (mstsc. exe) übergeben werden. In Verbindung mit der Deaktivierung von HttpOnly in der webanwendungsproxy-Anwendung ermöglicht es dem Remotedesktopverbindung Client (mstsc. exe), das über den Browser erhaltene webanwendungsproxy-Authentifizierungs Cookie zu verwenden.

Weitere Informationen zu RDP finden Sie unter [Konfigurieren des TS-Gateway-OTP-Szenarios](#).

## Siehe auch

- [Planen der Veröffentlichung von Anwendungen mit webanwendungsproxy](#)

- Problembehandlung: Webanwendungsproxy
- Leitfaden für webanwendungsproxy

# Problembehandlung: Webanwendungsproxy

09.04.2020 • 26 minutes to read • [Edit Online](#)

Gilt für: Windows Server 2016

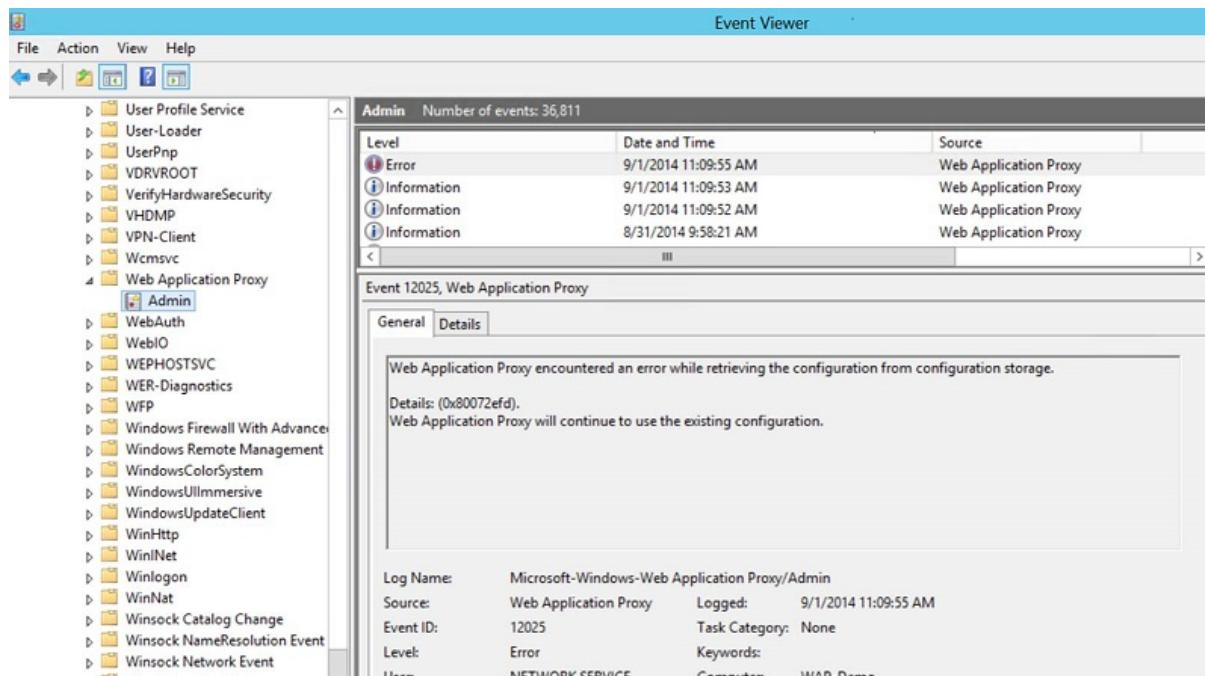
Diese Inhalte sind für die lokale Version des webanwendungsproxys relevant. Informationen zum Aktivieren des sicheren Zugriffs auf lokale Anwendungen über die Cloud finden Sie in den [Azure AD Anwendungs Proxy-Inhalt](#).

Dieser Abschnitt enthält Informationen zur Problembehandlung für den webanwendungsproxy, einschließlich Ereignis Erklärungen und-Lösungen Es gibt drei Stellen, an denen Fehler angezeigt werden:

- In der webanwendungsproxy-Administrator Konsole

Jede Ereignis-ID, die in der-Administrator Konsole aufgeführt ist, kann im Windows-Ereignisanzeige angezeigt werden. die entsprechenden Beschreibungen und Lösungen finden Sie unten.

Öffnen Sie Ereignisanzeige, und suchen Sie nach Ereignissen im Zusammenhang mit dem webanwendungsproxy unter **Anwendungs-und Dienst Protokolle > Microsoft > Windows > We > banwendungs Admin**



Bei Bedarf sind ausführliche Protokolle verfügbar, indem Sie die Analyse-und Debugprotokolle aktivieren und das Sitzungsprotokoll des webanwendungsproxys aktivieren, das Sie im Windows-Ereignisanzeige unter \ Microsoft \ Windows \ webanwendungsproxy \ Admin finden.

- In PowerShell-Fehlern

Ereignisse für Probleme, die während der Konfiguration aufgetreten sind, werden in PowerShell angezeigt.

Alle Fehler werden dem PowerShell-Benutzer mithilfe von standardmäßigen PowerShell-Fehler Aufforderungen angezeigt. Alle PowerShell-Befehle werden als Ereignisse protokolliert. Alle Ereignisse, die in PowerShell auftreten, werden im Windows-Ereignisanzeige mit der ID-Nummer 12016 aufgeführt und im PowerShell-Abschnitt unten definiert.

- Im Best Practices Analyzer

Diese Ereignisse werden im [Best Practices Analyzer für den webanwendungsproxy](#) beschrieben.

## PowerShell-Nachrichten

EREIGNIS ODER SYMPTOM	MÖGLICHE URSAUCE	AUFLÖSUNG
Das Vertrauensstellungs Zertifikat ("ADFS proxytrust-") ist ungültig.	Folgende Ursachen sind möglich: -Der Anwendungs Proxy Computer war zu lange nicht ausgelastet. : Trennen von Verbindungen zwischen dem webanwendungsproxy und AD FS -Probleme bei der Zertifikat Infrastruktur -Die Änderungen auf dem AD FS Computer oder der Erneuerungs Vorgang zwischen dem webanwendungsproxy und dem AD FS wurden alle 8 Stunden nicht wie geplant ausgeführt. Anschließend muss die Vertrauensstellung erneuert werden. -Die Uhr des webanwendungsproxy-Computers und der AD FS werden nicht synchronisiert.	Stellen Sie sicher, dass die Uhren synchronisiert sind. Führen Sie das install-webapplicationproxy-Cmdlet aus.
Die Konfigurationsdaten wurden in AD FS nicht gefunden.	Dies liegt möglicherweise daran, dass der webanwendungsproxy noch nicht vollständig installiert wurde oder aufgrund von Änderungen an der AD FS Datenbank oder der Beschädigung der Datenbank.	Ausführen des Cmdlets "Install-webapplicationproxy"
Fehler beim Versuch des webanwendungsproxys, die Konfiguration aus AD FS zu lesen.	Dies weist möglicherweise darauf hin, dass AD FS nicht erreichbar ist oder AD FS dass beim Versuch, die Konfiguration aus der AD FS Datenbank zu lesen, ein internes Problem aufgetreten ist.	Vergewissern Sie sich, dass AD FS erreichbar ist und ordnungsgemäß funktioniert.
Die in AD FS gespeicherten Konfigurationsdaten sind beschädigt, oder der webanwendungsproxy war nicht in der Lage, Sie zu analysieren.  OR  Webanwendungs Proxy konnte die Liste der vertrauenden Seiten nicht aus AD FS abrufen.	Dies kann vorkommen, wenn die Konfigurationsdaten in AD FS geändert wurden.	Starten Sie die Webanwendung proxyservice neu. Wenn das Problem weiterhin auftritt, führen Sie das install-webapplicationproxy-Cmdlet aus.

## Ereignisse Administratorkonsole

Die folgenden Administrator Konsolen Ereignisse sind im Allgemeinen ein Hinweis auf Authentifizierungsfehler, ungültige Tokens oder abgelaufene Cookies.

EREIGNIS ODER SYMPTOM	MÖGLICHE URSCHE	AUFLÖSUNG
11005 Der webanwendungsproxy konnte den Verschlüsselungsschlüssel für Cookies nicht mit dem geheimen Schlüssel aus der Konfiguration erstellen.	Der globale Konfigurationsparameter "accesscookiesverschlüsselungkey" wurde durch den PowerShell-Befehl geändert: Set-webapplicationproxyconfiguration-regenerateaccesscookiesverschlüsselungkey	Es sind keine Aktionen erforderlich. Das problematische Cookie wurde entfernt, und der Benutzer wurde zur Authentifizierung an STS umgeleitet.
12000 Der webanwendungsproxy konnte die Konfigurationsänderungen mindestens 60 Minuten nicht prüfen.	Der webanwendungsproxy kann nicht mithilfe des Befehls Get-webapplicationproxyconfiguration/Application auf die webanwendungsproxy-Konfiguration zugreifen. Dies wird in der Regel dadurch verursacht, dass keine Verbindung mit AD FS besteht oder dass die Vertrauensstellung mit AD FS erneuert werden muss.	Überprüfen Sie die Konnektivität mit AD FS. Hierzu können Sie den Link <a href="https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml">https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml</a> Make stellen Sie sicher, dass zwischen dem AD FS und dem webanwendungsproxy eine Vertrauensstellung hergestellt wird. Wenn diese Lösungen nicht funktionieren, führen Sie das install-webapplicationproxy-Cmdlet aus.
12003 Der webanwendungsproxy konnte das Zugriffs Cookie nicht analysieren.	Dies weist möglicherweise darauf hin, dass der webanwendungsproxy und der AD FS nicht verbunden sind oder dass Sie nicht die gleiche Konfiguration erhalten.	Überprüfen Sie die Konnektivität mit AD FS. Hierzu können Sie den Link <a href="https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml">https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml</a> Make stellen Sie sicher, dass zwischen dem AD FS und dem webanwendungsproxy eine Vertrauensstellung hergestellt wird. Wenn diese Lösungen nicht funktionieren, führen Sie das install-webapplicationproxy-Cmdlet aus.
12004 Der webanwendungsproxy hat eine Anforderung mit einem nicht gültigen Zugriffs Cookie empfangen.	Dieses Ereignis kann darauf hinweisen, dass der webanwendungsproxy und der AD FS nicht verbunden sind oder nicht die gleiche Konfiguration erhalten. Wenn Sie den Parameter "accesscookiesverschlüsselungkey" durch Set-webapplicationproxyconfiguration-regenerateaccesscookiesverschlüsselungkey PowerShell-Befehl ausgeführt haben, ist dieses Ereignis normal und erfordert keine Lösungsschritte.	Überprüfen Sie die Konnektivität mit AD FS. Hierzu können Sie den Link <a href="https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml">https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml</a> Make stellen Sie sicher, dass zwischen dem AD FS und dem webanwendungsproxy eine Vertrauensstellung hergestellt wird. Wenn diese Lösungen nicht funktionieren, führen Sie das install-webapplicationproxy-Cmdlet aus.
12008 Der webanwendungsproxy hat die maximal zulässige Anzahl zulässiger Kerberos-Authentifizierungs Versuche an den Back-End-Server	Dieses Ereignis kann auf eine falsche Konfiguration zwischen dem webanwendungsproxy und dem Back-End-Anwendungsserver oder einem Problem bei der Konfiguration von Datum und Uhrzeit auf beiden Computern hindeuten.	Der Back-End-Server hat das vom webanwendungsproxy erstellte Kerberos-Ticket abgelehnt. Vergewissern Sie sich, dass die Konfiguration des webanwendungsproxys und des Back-End-Anwendungsservers richtig konfiguriert Stellen Sie sicher, dass die Uhrzeit- und Datums Konfiguration auf dem webanwendungsproxy und dem Back-End-Anwendungsserver synchronisiert ist

EREIGNIS ODER SYMPTOM	MÖGLICHE URSCHE	AUFLÖSUNG
12011 Der webanwendungsproxy hat eine Anforderung mit einer nicht gültigen Zugriffs Cookie-Signatur erhalten.	Dieses Ereignis kann darauf hinweisen, dass der webanwendungsproxy und der AD FS nicht verbunden sind oder nicht die gleiche Konfiguration erhalten. Wenn Sie den Parameter "accesscookiesverschlüsselungkey" durch Set-webapplicationproxyconfiguration-regenerateaccesscookiesverschlüsselkey PowerShell-Befehl ausgeführt haben, ist dieses Ereignis normal und erfordert keine Lösungsschritte.	Überprüfen Sie die Konnektivität mit AD FS. Hierzu können Sie den Link <a href="https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml">https://&lt;FQDN_AD_FS_Proxy&gt;/verwenden/FederationMetadata/2007-06/FederationMetadata.xml</a> stellen. Stellen Sie sicher, dass zwischen dem AD FS und dem webanwendungsproxy eine Vertrauensstellung hergestellt wird. Wenn diese Lösungen nicht funktionieren, führen Sie das install-webapplicationproxy-Cmdlet aus.
12027 Unerwarteter Fehler beim Verarbeiten der Anforderung. Der angegebene Name ist kein ordnungsgemäß formatierter Kontoname.	Dieses Ereignis kann auf eine falsche Konfiguration zwischen dem webanwendungsproxy und dem Domänen Controller Server oder einem Problem bei der Konfiguration von Datum und Uhrzeit auf beiden Computern hindeuten.	Der Domänen Controller hat das vom webanwendungsproxy erstellte Kerberos-Ticket abgelehnt. Vergewissern Sie sich, dass die Konfiguration des webanwendungsproxys und des Back-End-Anwendungs Servers korrekt konfiguriert ist, insbesondere die SPN-Konfiguration. Stellen Sie sicher, dass der webanwendungsproxy in derselben Domäne wie der Domänen Controller angeschlossen ist, um sicherzustellen, dass der Domänen Controller eine Vertrauensstellung mit dem webanwendungsproxy herstellt. Stellen Sie sicher, dass die Uhrzeit- und Datums Konfiguration auf dem webanwendungsproxy
13012 Webanwendungsproxy hat eine nicht gültige edgetokensignatur		Stellen Sie sicher, dass Sie den webanwendungsproxy mit <a href="#">KB 2955164</a>
13013 Webanwendungsproxy hat eine Anforderung empfangen, die ein abgelaufenes Edge-Token enthielt	Webanwendungsproxy und AD FS verfügen nicht über synchronisierte Uhren.	Synchronisieren Sie die Uhren zwischen webanwendungsproxy und AD FS.
13014 Der webanwendungsproxy hat eine Anforderung mit einem ungültigen Edge-Token empfangen. Das Token ist ungültig, weil es nicht analysiert werden konnte.	Dies weist möglicherweise auf ein Problem mit der AD FS Konfiguration hin.	Überprüfen Sie die AD FS Konfiguration, und stellen Sie ggf. die Standardkonfiguration wieder her.
13015 Der webanwendungsproxy hat eine Anforderung mit einem abgelaufenen Zugriffs Cookie empfangen.	Dies kann auf Uhren hindeuten, die nicht synchronisiert sind.	Wenn Sie mit einem Cluster von webanwendungsproxy-Computern arbeiten, stellen Sie sicher, dass Uhrzeit und Datum der Computer synchronisiert sind.

EREIGNIS ODER SYMPTOM	MÖGLICHE URSCHE	AUFLÖSUNG
13016 Der webanwendungsproxy kann kein Kerberos-Ticket für den Benutzer abrufen, da kein UPN im edgetoken oder im Zugriffs Cookie vorhanden ist.	Es liegt ein Problem mit der STS-Konfiguration vor.	Korrigieren Sie die UPN-Anspruchs Konfiguration im STS.
13019 Der webanwendungsproxy kann aufgrund des folgenden allgemeinen API-Fehlers kein Kerberos-Ticket für den Benutzer abrufen.	Dieses Ereignis kann auf eine falsche Konfiguration zwischen dem webanwendungsproxy und dem Domänen Controller Server oder einem Problem bei der Konfiguration von Datum und Uhrzeit auf beiden Computern hindeuten.	Der Domänen Controller hat das vom webanwendungsproxy erstellte Kerberos-Ticket abgelehnt. Vergewissern Sie sich, dass die Konfiguration des webanwendungsproxys und des Back-End-Anwendungs Servers korrekt konfiguriert ist, insbesondere die SPN-Konfiguration Stellen Sie sicher, dass der webanwendungsproxy in derselben Domäne wie der Domänen Controller angeschlossen ist, um sicherzustellen, dass der Domänen Controller eine Vertrauensstellung mit dem webanwendungsproxy herstellt. Stellen Sie sicher, dass die Uhrzeit- und Datums Konfiguration auf dem webanwendungsproxy
13020 Der webanwendungsproxy kann kein Kerberos-Ticket für den Benutzer abrufen, da der Back-End-Server-SPN nicht definiert ist.	Dieses Ereignis kann auf eine falsche Konfiguration zwischen dem webanwendungsproxy und dem Domänen Controller Server oder einem Problem bei der Konfiguration von Datum und Uhrzeit auf beiden Computern hindeuten.	Der Domänen Controller hat das vom webanwendungsproxy erstellte Kerberos-Ticket abgelehnt. Vergewissern Sie sich, dass die Konfiguration des webanwendungsproxys und des Back-End-Anwendungs Servers korrekt konfiguriert ist, insbesondere die SPN-Konfiguration Stellen Sie sicher, dass der webanwendungsproxy in derselben Domäne wie der Domänen Controller angeschlossen ist, um sicherzustellen, dass der Domänen Controller eine Vertrauensstellung mit dem webanwendungsproxy herstellt. Stellen Sie sicher, dass die Uhrzeit- und Datums Konfiguration auf dem webanwendungsproxy
13022 Webanwendungsproxy kann den Benutzer nicht authentifizieren, da der Back-End-Server auf Kerberos-Authentifizierungs Versuche mit einem HTTP 401-Fehler reagiert	Dieses Ereignis kann auf eine falsche Konfiguration zwischen dem webanwendungsproxy und dem Back-End-Anwendungsserver oder einem Problem bei der Konfiguration von Datum und Uhrzeit auf beiden Computern hindeuten.	Der Back-End-Server hat das vom webanwendungsproxy erstellte Kerberos-Ticket abgelehnt. Vergewissern Sie sich, dass die Konfiguration des webanwendungsproxys und des Back-End-Anwendungs Servers richtig konfiguriert Stellen Sie sicher, dass die Uhrzeit- und Datums Konfiguration auf dem webanwendungsproxy und dem Back-End-Anwendungsserver synchronisiert ist

EREIGNIS ODER SYMPTOM	MÖGLICHE URSCHE	AUFLÖSUNG
13025 Vom Client wurde kein SSL-Zertifikat für den webanwendungsproxy vorhanden.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind. Stellen Sie sicher, dass der für den webanwendungsproxy konfigurierte Fingerabdruck korrekt ist.
13026 Der Client hat ein SSL-Zertifikat für den webanwendungsproxy vorgelegt, aber das Zertifikat ist ungültig: das Zertifikat stimmt nicht mit dem Fingerabdruck identisch.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind. Stellen Sie sicher, dass der für den webanwendungsproxy konfigurierte Fingerabdruck korrekt ist.
13028 Webanwendungsproxy hat eine Anforderung empfangen, die ein edgetoken enthielt, das noch nicht gültig ist.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind.
13030 Der Client hat ein SSL-Zertifikat für den webanwendungsproxy vorgelegt, aber der vertrauenswürdige Anbieter vertraut nicht der Zertifizierungsstelle, die das Client Zertifikat ausgestellt hat.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind. Stellen Sie sicher, dass der für den webanwendungsproxy konfigurierte Fingerabdruck korrekt ist.
13031 Der Client hat ein SSL-Zertifikat für den webanwendungsproxy vorgelegt, aber die Zertifikat Kette wurde in einem Stamm Zertifikat beendet, dem der Vertrauens Anbieter nicht vertraut.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind. Stellen Sie sicher, dass der für den webanwendungsproxy konfigurierte Fingerabdruck korrekt ist.
13032 Der Client hat ein SSL-Zertifikat für den webanwendungsproxy vorgelegt, aber das Zertifikat war für die angeforderte Verwendung ungültig.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind. Stellen Sie sicher, dass der für den webanwendungsproxy konfigurierte Fingerabdruck korrekt ist.
13033 Der Client hat ein SSL-Zertifikat für den webanwendungsproxy vorgelegt, aber das Zertifikat befand sich nicht innerhalb seines Gültigkeits Zeitraums, als die aktuelle Systemuhr oder der Zeitstempel in der signierten Datei überprüft wurde.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind. Stellen Sie sicher, dass der für den webanwendungsproxy konfigurierte Fingerabdruck korrekt ist.

EREIGNIS ODER SYMPTOM	MÖGLICHE URSCHE	AUFLÖSUNG
13034 Der Client hat ein SSL-Zertifikat für den webanwendungsproxy vorgelegt, das Zertifikat war jedoch ungültig.	Dieses Ereignis weist möglicherweise auf ein Problem bei der Konfiguration von Datum und Uhrzeit hin.	Stellen Sie sicher, dass die Zertifikat Infrastruktur gültig ist und die Uhrzeit und das Datum des webanwendungsproxys und der AD FS synchronisiert sind. Stellen Sie sicher, dass der für den webanwendungsproxy konfigurierte Fingerabdruck korrekt ist.

Die folgenden Administrator Konsolen Ereignisse weisen in der Regel darauf hin, dass Probleme mit der Konfiguration auftreten müssen, z. b. die Bereitstellung, nicht erfolgreiche Anforderungen, Back-End-Server, die nicht erreichbar sind, und Pufferüberläufe.

EREIGNIS ODER SYMPTOM	MÖGLICHE URSCHE	AUFLÖSUNG
12019 Der webanwendungsproxy konnte keinen Listener für die folgende URL erstellen.	Eine mögliche Ursache für das Ereignis ist, dass ein anderer Dienst dieselbe URL abhört.	Der Administrator muss sicherstellen, dass die gleichen URLs nicht von einem Administrator überwacht oder gebunden werden. Um dies zu überprüfen, führen Sie den folgenden Befehl aus: netsh http show urlacl. Wenn diese URL von einer anderen Komponente auf dem webanwendungsproxy-Computer verwendet wird, entfernen Sie Sie, oder verwenden Sie eine andere URL zum Veröffentlichen der Anwendungen über den webanwendungsproxy.
12020 Der webanwendungsproxy konnte keine Reservierung für die folgende URL erstellen.	Eine mögliche Ursache für das Ereignis besteht darin, dass ein anderer Dienst über eine Reservierung der gleichen URL verfügt.	Der Administrator muss sicherstellen, dass niemand an die gleichen URLs gebunden ist. Um dies zu überprüfen, führen Sie den folgenden Befehl aus: netsh http show urlacl. Wenn diese URL von einer anderen Komponente auf dem webanwendungsproxy-Computer verwendet wird, entfernen Sie Sie, oder verwenden Sie eine andere URL zum Veröffentlichen der Anwendungen über den webanwendungsproxy.
12021 Der webanwendungsproxy konnte das SSL-Serverzertifikat nicht binden. Alle anderen Konfigurationseinstellungen wurden angewendet.	Ein Konfigurationsdaten Satz mit SSL-Zertifikat Daten kann nicht erstellt und festgelegt werden.	Stellen Sie sicher, dass die für Webanwendungen proxyapplications konfigurierten Zertifikat Fingerabdrücke auf allen webanwendungsproxy-Computern mit einem privaten Schlüssel im lokalen Computerspeicher installiert sind.
13001 Das vom Back-End-Server an den webanwendungsproxy vorgelegte SSL-Serverzertifikat ist ungültig. das Zertifikat ist nicht vertrauenswürdig.	Es wurde mindestens ein Fehler im vom Server gesendeten Secure Sockets Layer (SSL)-Zertifikat gefunden. Dies könnte darauf hindeuten, dass der Back-End-Server ein ungültiges SSL bereitgestellt hat oder keine Vertrauensstellung zwischen dem webanwendungsproxy und dem Back-End-Server besteht.	Überprüfen eines Back-End-Server-SSL-Zertifikats Stellen Sie sicher, dass der webanwendungsproxy-Computer mit den richtigen Stamm Zertifizierungsstellen konfiguriert ist, um dem Back-End-Server

EREIGNIS ODER SYMPTOM	MÖGLICHE URSCHE	AUFLÖSUNG
13006	Wenn der Fehlercode 0x80072EE7 lautet, wird das failurrre-Problem dadurch verursacht, dass die URL des Back-End-Servers nicht aufgelöst werden kann. Andere Fehlercodes werden in <a href="https://msdn.microsoft.com/library/windows/desktop/aa384110(v=vs.85)">https://msdn.microsoft.com/library/windows/desktop/aa384110(v=vs.85)</a>	Überprüfen Sie, ob die URL des Back-End-Servers richtig ist und der Name des webanwendungsproxy-Computers ordnungsgemäß aufgelöst werden kann
13007 Die HTTP-Antwort vom Back-End-Server wurde nicht innerhalb des erwarteten Intervalls empfangen.	Timeout bei der Anforderung des Back-End-Servers, oder die Anforderung ist langsam oder reagiert nicht.	Prüfen Sie die Back-End-Serverkonfiguration. Wenn Sie sehr langsam ist, überprüfen Sie die Konnektivität mit dem Back-End-Server, und ändern Sie auch das Cmdlet "globale Konfigurationsparameter für den webanwendungsproxy" für inactivetransaktiontimeoutsec

## Weitere Informationen

[Neues im webanwendungsproxy unter Windows Server 2016](#)

[Arbeiten mit webanwendungsproxy](#)