Parallels Remote Application Server

Handbuch Verwaltungsportal

19.3

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
Schweiz
Tel.: + 41 52 672 20 30
www.parallels.com/de

Inhalt

Einführung 7
Parallels RAS 19-Versionsverlauf 7
Überblick 7
Neue Funktionen 8
Installation und Konfiguration 10
Voraussetzungen 10
Installation 10
Erste Schritte mit dem RAS-Verwaltungsportal 12
Anmelden beim RAS-Verwaltungsportal 12
RAS Web-Administrationsdienst konfigurieren 12
Benutzeroberfläche des RAS-Verwaltungsportals 14
Site-Kategorie 18
Farm-Einstellungen 19
Administratoren 19
Mailbox 20
Lizenzierung 20
Site-Einstellungen 23
Verbinden und Authentifizierung 23
Multifaktor-Authentifizierung 25
Verwenden von RADIUS 26
Verwenden von Google Authenticator 28
Konfiguration von MFA-Regeln 30
FSLogix-Profilcontainer 32
Verwaltung bestehender Profile durch Parallels RAS konfigurieren 34
Site-Standardeinstellungen und Hosts für FSLogix konfigurieren 36
Universelles Drucken 37
Universal Scanning 40
Infrastruktur 43
RD-Sitzungshosts 43
RD-Sitzungshost hinzufügen 43

Konfigurieren eines RD-Sitzungshosts....45
Verwalten eines RD-Sitzungshosts....53
RDSH-Gruppen....58
Virtual Desktop-Infrastruktur....59
Zertifikate....60
Erstellen eines selbstsignierten Zertifikats....61
Generieren einer Zertifikatsignaturanforderung (CSR)....62
Let's Encrypt-Zertifikate....63
Ein Zertifikat aus einer Datei importieren....65
Exportieren eines Zertifikats in eine Datei....65
Ein Zertifikat für Gateways und HALB zuweisen....66
Gateways....67
Gateway hinzufügen....68
Gateway konfigurieren....69
Gateways verwalten....84
Connection Brokers....85
Konfigurieren eines RAS Connection Brokers....85
Sekundären Connection Broker hinzufügen....87
RAS Connection Broker verwalten....90
Anbieter....91
Standardeinstellungen der Site....92
Sitzungen....93
Überblick....93
Sitzungsinformationen....93
Benutzersitzungen....98
Laufende Ressourcen....99
Veröffentlichung....101
Veröffentlichen einer Anwendung....102
Veröffentlichen eines Desktops....103
Veröffentlichen eines Dokuments....105
Veröffentlichen eines Ordners im Dateisystem....105
Verwalten veröffentlichter Ressourcen....106
Verwalten veröffentlichter Anwendungen....107
Verwalten veröffentlichter Desktops....109

Verwalten von Ordnern ... 110
Standardeinstellungen der Site (Publishing) ... 112
Verwenden von Filterregeln ... 114
Bevorzugtes Routing konfigurieren ... 115
Überwachung ... 118
Überblick ... 118
Installieren von RAS Performance Monitor ... 119
Überwachung im RAS-Verwaltungsportal aktivieren ... 120
Anzeigen von Leistungskennzahlen ... 121
Konfigurieren der Sicherheit für RAS Performance Monitor ... 123
RAS-Agents aktualisieren ... 125
Hilfe und Support ... 126
Anhang ... 127
Microsoft-Lizenzanforderungen in Parallels RAS ... 127
Port-Referenz ... 133
Parallels Client ... 133
Internetbrowser ... 134
HALB ... 135
RAS Secure Gateway ... 135
RAS Connection Broker ... 136
RAS-Konsole ... 138
SSRS ... 139
RAS-Berichterstellung ... 139
RAS Web-Administrationsdienst (REST/Verwaltungsportal) ... 139
RAS PowerShell ... 140
RAS Provider Agent ... 140
RAS-Registrierungsserver ... 142
RAS RD Session Host Agent ... 142
RAS Guest Agent ... 142
RAS Remote PC Agent ... 143
Mandantenmakler ... 143
Ports für Active Directory und Domain Services ... 144
Azure Virtual Desktop ... 144

RAS-Leistungsindikatoren 145
Index..... 148

KAPITEL 1

Einführung

In diesem Kapitel

Parallels RAS 19-Versionsverlauf 7
Überblick 7
Neue Funktionen 8

Parallels RAS 19-Versionsverlauf

In der folgenden Tabelle wird der Versionsverlauf von Parallels RAS 19 aufgeführt. Die Parallels RAS-Dokumentation wird bei jeder neuen Version aktualisiert. Dieser Leitfaden bezieht sich auf die neueste Version von Parallels RAS 19 aus der unten stehenden Tabelle. Wenn Sie eine neuere Version von Parallels RAS verwenden, laden Sie bitte die aktuelle Version des Leitfadens von https://www.parallels.com/de/products/ras/resources/ herunter.

Parallels RAS Version	Release	Datum
19.0	Erstveröffentlichung	27.07.2022
19.0	Update 1	31.08.2022
19.0	Hotfix 1	16.09.2022
19.0	Hotfix 2	30.09.2022
19.0	Hotfix 3	14.10.2022
19.1	Update 2	15.11.2022
19.2	Update 3	06.07.2023
19.3	Erstveröffentlichung	17.10.2023

Überblick

Das Parallels® RAS-Verwaltungsportal ist eine moderne, webbasierte Konfigurations- und Verwaltungskonsole, die für Parallels RAS-Administratoren entwickelt wurde, die einen Desktop-/Laptop-Computer oder ein mobiles Gerät zur Durchführung von Konfigurationen und täglichen Aktivitäten nutzen.

Das Parallels RAS-Verwaltungsportal bietet Administratoren folgende Möglichkeiten:

- Zentrale Bereitstellung, Verwaltung und Konfiguration der essentiellen Parallels RAS-Komponenten – wie RD-Sitzungshosts, Connection Broker und Secure Gateways.
- Veröffentlichung verschiedener Ressourcen von RD-Sitzungshosts.
- Konfigurieren der Einstellungen für FSLogix-Profilcontainer.
- Konfigurieren der Einstellungen für Drucken und Scannen.
- Verwalten von SSL-Zertifikaten.
- Konfigurieren der Verbindungseinstellungen und MFA (Google Authenticator oder anderer TOTP (Time-based One-time Passwords, TOTP) wie Microsoft Authenticator).
- Überwachen und Verwalten von Benutzersitzungen.
- Verwalten administrativer Konten und Sitzungen
- Konfigurieren des Postfachs.
- Verwalten Ihrer Lizenz.
- Kontaktaufnahme mit dem Support und Bereitstellen der notwendigen Systemberichte.

Hinweis: Weitere Funktionen und Fähigkeiten, die derzeit in der Desktop-basierten Parallels RAS-Konsole verfügbar sind, werden in zukünftigen Releases in das Parallels RAS-Verwaltungsportal aufgenommen, bis es letztendlich das Hauptverwaltungstool für Parallels RAS wird.

Die Verwaltung von Azure Virtual Desktop-Funktionen, die im Parallels RAS-Verwaltungsportal enthalten sind, sind experimentell und werden voraussichtlich in kommenden Versionen veröffentlicht.

Neue Funktionen

Parallels RAS 19.3

Parallels RAS 19.3 wartet mit folgenden neuen Funktionen auf:

- Support für FSLogix Office Containers support und erweiterte Verwaltung für FSLogix (S. 36).
- RADIUS wurde als MFA-Anbieter hinzugefügt (S. 26).
- Möglichkeit, das Benutzerpasswort über IdPs von Drittanbietern zu ändern (S. 23).

Parallels RAS 19.2

Parallels RAS 19.2 wartet mit folgenden neuen Funktionen auf:

- Die Möglichkeit, das Transportprotokoll für Verbindungen zwischen Parallels Client und einem Server auf RDSH auszuwählen (S. 46)
- Microsoft Authenticator wurde als TOTP-Provider hinzugefügt (S. 25).

KAPITEL 2

Installation und Konfiguration

In diesem Kapitel

Voraussetzungen 10
Installation 10

Voraussetzungen

Das RAS-Verwaltungsportal läuft auf jedem modernen Webbrowser, der HTML5 unterstützt, außer für Internet Explorer.

Stellen Sie sicher, dass Ihr Windows-Server die folgenden Updates installiert hat (RAS-Verwaltungsportal ist davon abhängig):

- Windows Server 2012 R2: KB2999226

Neuere Versionen von Windows Server erfordern keine spezifischen Updates.

Der Webdienst hört Webanfragen standardmäßig an den folgenden Ports ab.

- HTTPS: 20443
- HTTP: 20080

Installation

Um das RAS-Verwaltungsportal in einer RAS-Serverfarm zu aktivieren, müssen Sie die Komponente „RAS Web-Administrationsdienst“ installieren. Die Komponente wird automatisch installiert, wenn Sie eine reine Parallels RAS-Installation mit der Installationsoption „Typisch“ durchführen. Sie können die Komponente auch mit der Installationsoption „Benutzerdefiniert“ installieren und „RAS Web-Administrationsdienst“ als zu installierende Komponente auswählen. Wenn Sie z. B. das RAS-Verwaltungsportal auf einem dedizierten Rechner installieren möchten, sollten Sie die Installationsoption „Benutzerdefiniert“ verwenden und „RAS Web-Administrationsdienst“ als zu installierende Komponente auswählen.

Nachdem der RAS Web-Administrationsdienst installiert ist, müssen Sie ihn konfigurieren. Insbesondere müssen Sie eine RAS-Serverfarm angeben, die über das RAS-Verwaltungsportal

verwaltet werden soll, und eine Reihe weiterer Parameter konfigurieren. Eine vollständige Anleitung finden Sie unter RAS Web-Administrationsdienst konfigurieren (S. 12).

KAPITEL 3

Erste Schritte mit dem RAS-Verwaltungsportal

In diesem Kapitel

Anmelden beim RAS-Verwaltungsportal 12
RAS Web-Administrationsdienst konfigurieren 12
Benutzeroberfläche des RAS-Verwaltungsportals 14

Anmelden beim RAS-Verwaltungsportal

Um das RAS-Verwaltungsportal auf dem Rechner zu öffnen, auf dem Sie den RAS-Web-Verwaltungsdienst installiert haben, navigieren Sie zu Apps > Parallels und klicken auf Parallels RAS-Verwaltungsportal.

Um sich von einem entfernten Computer aus beim RAS-Verwaltungsportal anzumelden, geben Sie die folgende URL in einen Webbrowser ein:

```
https://<Server-Adresse>:20443
```

Die <Server-Adresse> ist der FQDN oder die IP-Adresse des Servers, auf dem der RAS-Web-Administrationsdienst installiert ist. Standardmäßig wird der Port 20443 für HTTPS-Verbindungen verwendet. Sie können die Portnummer bei Bedarf ändern, wie in RAS Web-Administrationsdienst konfigurieren (S. 12 beschrieben.

Geben Sie auf der Willkommensseite Ihren RAS-Administrator-Benutzernamen und Ihr Passwort ein und klicken Sie auf Anmelden.

RAS Web-Administrationsdienst konfigurieren

Bevor Sie beginnen, müssen Sie eventuell den RAS Web-Administrationsdienst wie unten beschrieben konfigurieren:

1. Klicken Sie im RAS-Verwaltungsportal auf das Symbol „Benutzer“ in der oberen rechten Ecke und wählen Sie Verwaltungsportal konfigurieren.

2 Sie werden aufgefordert, sich erneut anzumelden. Beachten Sie, dass der RAS Web-Administrationsdienst auf dem lokalen Server laufen muss, damit diese Anmeldung funktioniert. Dies ist notwendig, um zu verhindern, dass Benutzer von Remoteservern auf die Konfigurationsseiten des RAS Web-Administrationsdienstes zugreifen können.

3 Geben Sie den Benutzernamen und das Passwort eines Mitglieds der lokalen Administratoren oder der Domänenadministratoren ein und klicken Sie auf Anmelden.

4 Die Seite Konfiguration von RAS-Verwaltungsportal wird geöffnet.

5 Geben Sie im Feld RAS-Serverfarmadresse die Adresse der RAS-Serverfarm an, die von diesem RAS-Verwaltungsportal verwaltet werden soll. Dies ist die Adresse des in der Serverfarm installierten RAS Connection Brokers.

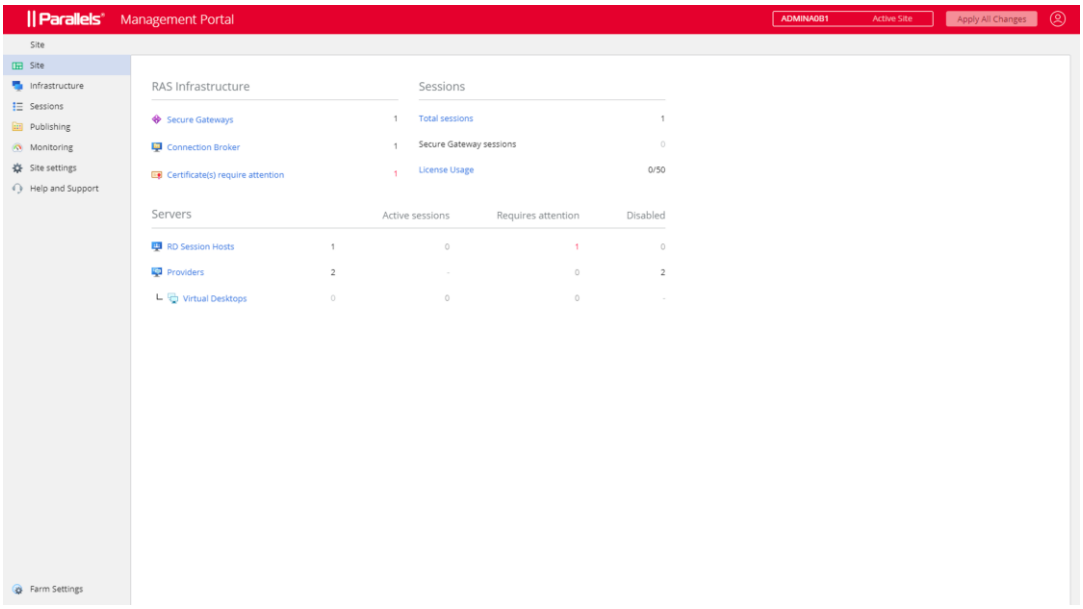
6 Im Abschnitt Erweiterte Einstellungen geben Sie Folgendes an:

- Zertifikat: Ein Zertifikat, das für diese Verbindung verwendet werden soll. Klicken Sie auf Hochladen, um ein Zertifikat auszuwählen.
- Passwort für das Zertifikat: Das Passwort für das Zertifikat.
- Port: Die Portnummer, auf der das RAS-Verwaltungsportal auf Verbindungen wartet. Der Standardport ist 20443. Diese Portnummer ist so gewählt, dass sie nicht mit den Ports des RAS Secure Gateway kollidiert. Sie können sie auf 443 ändern (falls möglich). In diesem Fall muss die Portnummer nicht in der Verbindungs-URL enthalten sein. Sie können sie auch in einen beliebigen benutzerdefinierten Anschluss ändern. Zum Beispiel die standardmäßige „URL“: „https://*:20443“ kann in „URL“ geändert werden: „http://*:20080“.
- Timeout der Administrator-Sitzung: Das Zeitlimit, nach der die Administrator-Sitzung getrennt wird.
- Abfrageintervall: Das Intervall, in dem das RAS-Verwaltungsportal die angezeigten Informationen aktualisiert. Sie können diese Zahl auf bis zu 30 Sekunden erhöhen, wenn viele Administratoren gleichzeitig arbeiten und/oder wenn Sie eine große Anzahl von Hosts, Sitzungen usw. haben.

7 Klicken Sie zum Abschluss auf Speichern.

Benutzeroberfläche des RAS-Verwaltungsportals

Alle Navigationen im RAS-Verwaltungsportal beginnen mit der Seitenleiste auf der linken Seite, in der die Managementkategorien aufgelistet sind. Die Kategorie Site ist standardmäßig ausgewählt.



Kategorien

Die folgende Tabelle zeigt alle verfügbaren Kategorien, die im RAS-Verwaltungsportal verwaltet werden können. Der Root-Administrator kann alle Kategorien sehen und verwalten. Administratoren anderer Typen (Power, Custom) benötigen möglicherweise Berechtigungen, um eine bestimmte Kategorie zu sehen.

Kategorie	Beschreibung
Site	Zeigt die aktuelle Site-Übersicht an.
Infrastruktur	Verwaltung der RAS-Infrastruktur, einschließlich RD-Sitzungen, Hosts, VDI, Gateways, Connection Broker usw.
Sitzungen	Sitzungsverwaltung.
Veröffentlichung	Veröffentlichung und Verwaltung der veröffentlichten Ressourcen.
Überwachung	RAS Performance Monitor.

Site-Einstellungen	Verbindung, Authentifizierung, FSLogix, Universelles Drucken und Scannen.
Hilfe und Support	Hilfe und Support.
Farm-Einstellungen	Diese Kategorie, die unten in der linken Seitenleiste angezeigt wird, verwaltet die globalen Einstellungen der Serverfarm, z. B. Administratoren, Mailbox, Lizenzierung.

Jede Kategorie wird später in diesem Leitfaden ausführlich beschrieben.

Admin-Berechtigungen

Einige Kategorien und Aktionen im RAS-Verwaltungsportal können je nach den in der RAS-Konsole konfigurierten Admin-Berechtigungen nicht angezeigt oder zugelassen werden. Informationen zur Konfiguration von Administratorrechten finden Sie im Parallels RAS-Administratorhandbuch. Suchen Sie im Leitfaden nach dem Thema Berechtigungen für Administratorkonten. Der Leitfaden ist auf der Parallels-Website unter https://www.parallels.com/de/products/ras/resources/ verfügbar.

Unterkategorien

Einige Kategorien haben Unterkategorien (nämlich Infrastruktur und Site-Einstellungen). Wenn Sie eine Kategorie ausgewählt haben, kann die rechte Seite des RAS-Verwaltungsportals einen oder mehrere zusätzliche Bereiche enthalten, in denen Sie eine Unterkategorie auswählen können.

Die Navigationsleiste

Bei einigen Komponenten sind die Einstellungen und Informationen nach Funktionen gruppiert (z. B. Allgemein, Eigenschaften, Sitzungen usw.). Wenn Sie die Komponenteneigenschaften anzeigen, wird in der Mitte eine Navigationsleiste angezeigt, mit der Sie diese Einstellungen durchsuchen können. Wenn Sie ein Element in der Navigationsleiste auswählen, werden die Einstellungen im rechten Fenster angezeigt.

Breadcrumbs

Wenn Sie Kategorien, Unterkategorien oder einzelne Artikel auswählen, wird oben auf der Seite ein Breadcrumb-Pfad angezeigt, die Ihnen zeigt, wo Sie sich befinden. Um einen oder mehrere Schritte zurückzugehen, klicken Sie auf einen Link im Pfad.

Elemente des Seitenkopfes

Der Seitenkopf enthält die folgenden Elemente:

- Die Serverfarm und die aktuellen Site-Namen. Wenn Sie mehr als eine Site haben, können Sie eine aus der Dropdownliste auswählen. Das RAS-Verwaltungsportal wechselt zu dieser Site und ermöglicht Ihnen die Verwaltung der Site-Komponenten.
- Das Symbol „Benutzer“ ist eine Dropdownliste mit den folgenden Elementen: Aktueller Benutzername (z. B. Administrator); Über (öffnet das Dialogfeld „Über“); Feedback geben (führt Sie zu einer Webseite, auf der Sie Parallels Feedback geben können); Verwaltungsportal konfigurieren (S. 12), Abmelden (meldet Sie ab).
- Alle Änderungen übernehmen: Diese Schaltfläche wendet Änderungen, die Sie im RAS-Verwaltungsportal vorgenommen haben, auf Serverfarmkomponenten an. Wenn Sie Komponenten und Objekte erstellen oder ändern, werden die Änderungen nicht automatisch auf die Komponenten der Serverfarm übertragen und haben keine Auswirkungen auf die Site oder die Serverfarm. Wenn Sie auf die Schaltfläche Alle Änderungen übernehmen klicken, werden die Änderungen für die gesamte Serverfarm oder Site übernommen. Beachten Sie, dass Sie nicht bei jeder Änderung auf diese Schaltfläche klicken sollten. Wenn Sie an einer Aufgabe arbeiten, die mehrere Änderungen in verschiedenen Bereichen erfordert, schließen Sie alle Änderungen ab und klicken Sie dann auf die Schaltfläche Alle Änderungen übernehmen, damit alle Änderungen gemeinsam übernommen werden.

Bearbeiten

Wenn Sie eine Ansicht öffnen, in der Sie einige Einstellungen ändern können, ist die Ansicht normalerweise schreibgeschützt. Um die Bearbeitung zu aktivieren, klicken Sie auf die Schaltfläche Bearbeiten in der oberen rechten Ecke. Der Name der Schaltfläche ändert sich in Speichern. Wenn Sie mit der Bearbeitung fertig sind, klicken Sie auf Speichern. Um die Änderungen zu verwerfen, klicken Sie auf Abbrechen.

Bitte beachten Sie, dass ein Objekt, das von einem Administrator zur Bearbeitung geöffnet wurde, nicht gleichzeitig von einem anderen Administrator bearbeitet werden kann. Wenn Sie versuchen, die Bearbeitung für ein solches Objekt zu aktivieren, erhalten Sie eine Fehlermeldung mit dem Namen des Administrators, der das Objekt gesperrt hat.

Symbolleiste zum Bearbeiten

Einige Ansichten (insbesondere Listen) verfügen über eine Symbolleiste in der oberen rechten Ecke, über die Sie Aktionen ausführen können. Um den Namen eines Symbolleistenelements zu sehen, führen Sie den Mauszeiger über das Element. Die Symbolleiste enthält die folgenden Standardfunktionen (Symbole):

- Filter anzeigen: Einen Filter angeben, um nur die Einträge anzuzeigen, die diesem Filter entsprechen.
- Spalten auswählen: Die Tabellenspalten auswählen, die angezeigt oder ausgeblendet werden sollen.

- Hinzufügen: Einen neuen Eintrag hinzufügen. Zum Beispiel ein neues Gateway oder einen neuen RD-Sitzungshost usw. hinzufügen.
- Aktualisieren: Ansicht aktualisieren.
- Ellipsis: Das Ellipsenmenü kann in verschiedenen Ansichten unterschiedliche Einträge haben. Einige Elemente haben entsprechende Symbolleistenelemente (z. B. Hinzufügen, Aktualisieren).

Je nachdem, in welcher Ansicht Sie sich befinden, können weitere Elemente vorhanden sein. Zum Beispiel: Laufende Prozesse anzeigen und Sitzungen anzeigen.

Wizards

Wenn Sie einer Serverfarm eine Komponente hinzufügen, öffnet sich in der Regel ein Assistent, der Sie durch eine Reihe von Seiten führt, auf denen Sie Komponenteneinstellungen und -optionen festlegen. Ein Assistent verfügt über die üblichen Navigationsschaltflächen Weiter und Zurück sowie über die Schaltfläche Abbrechen, mit der der Assistent geschlossen und der Vorgang abgebrochen wird.

Modale Dialogfelder

Wenn Sie auf einige Menü- und Navigationsleistenelemente klicken, wird ein modales Dialogfeld angezeigt. Dabei handelt es sich in der Regel um Elemente, bei denen Sie eine Aktion bestätigen oder zusätzliche Informationen eingeben müssen.

Ansichten der Objekteigenschaften

Alle Objekte (Komponenten) im RAS-Verwaltungsportal haben Eigenschaften. Um diese Eigenschaften anzuzeigen, wählen Sie eine Kategorie und eine Unterkategorie aus und klicken auf den Objektnamen in der Liste. Dadurch wird eine Ansicht geöffnet, in der die Objekteigenschaften mit einer eigenen Navigationsleiste angezeigt werden, über die Sie das Objekt konfigurieren, Aktionen durchführen und zusätzliche Informationen anzeigen können.

KAPITEL 4

Site-Kategorie

Die Kategorie Site bietet Ihnen einen Überblick über die aktuelle Site und zeigt Benachrichtigungen über wichtige Ereignisse, wie z. B. Probleme bei der Lizenzierung, RAS-Agenten, die einer Aktualisierung bedürfen usw., an.

In der Hauptansicht der Site-Kategorie finden Sie die unten beschriebenen Abschnitte.

RAS-Infrastruktur

Zeigt RAS-Komponenten, wie den RAS Connection Broker und RAS Secure Gateway, an. Wenn Sie mehr als eine Kategorie eines bestimmten Typen haben, wird auf der rechten Seite die Anzahl der installierten Komponenten angezeigt.

Klicken Sie auf eine Komponente, um die Verwaltungsansicht aufzurufen. Sie können die Verwaltungsansicht auch über die Kategorie Infrastruktur (etwas weiter hinten finden Sie weitere Informationen darüber) aufrufen.

Sitzungen

Dieser Abschnitt zeigt Informationen zur Sitzung und Lizenznutzung an. Um zu den Ansichten „Sitzung“ oder „Lizenzverwaltung“ zu springen, klicken Sie einfach auf den entsprechenden Link.

Hosts

Im Abschnitt Hosts werden Informationen über verfügbare Sitzungshosts, darunter auch RD-Sitzungshosts und VDI (falls verfügbar) angezeigt. Klicken Sie auf die verfügbaren Links, um die Verwaltungsansicht für einen bestimmten Host-Typ oder Provider aufzurufen. Die Host-Informationen umfassen die Anzahl aktiver Sitzungen auf einem Host, ob es ein Problem mit dem Host gibt, das Ihre Aufmerksamkeit erfordert und ob der Host aktuell deaktiviert ist.

KAPITEL 5

Farm-Einstellungen

Um globale Farm-Einstellungen zu verwalten, klicken Sie unten auf der Seitenleiste auf Farm-Einstellungen.

In diesem Kapitel

Administratoren 19
Mailbox 20
Lizenzierung 20

Administratoren

Konten

So fügen Sie einer Parallels RAS-Farm ein Administratorkonto hinzu:

1. Navigieren Sie in der RAS-Konsole zu Farm-Einstellungen > Administratoren > Konten.
2. Klicken Sie mit der rechten Maustaste auf einen beliebigen Punkt in der Liste und wählen Sie dann Hinzufügen aus.
3. Geben Sie die neuen Kontoeigenschaften an.

   Beachten Sie, dass zum Zeitpunkt der Erstellung dieses Handbuchs nur ein Root-Administrator im Management-Portal hinzugefügt werden kann.
4. Wählen Sie in der Dropdownliste Systembenachrichtigungen die Option E-Mail aus, um alle Systembenachrichtigungen an die angegebene E-Mail-Adresse zu senden, oder wählen Sie Keine, um die Benachrichtigungen über das E-Mail-System für dieses Konto zu deaktivieren.
5. Klicken Sie auf Erstellen, um das Konto zu erstellen.

Klicken Sie auf den Kontonamen und dann auf Bearbeiten, um ein Konto zu bearbeiten.

Klicken Sie mit der rechten Maustaste auf ein Konto und wählen Sie dann die Option Löschen aus, um ein Konto zu löschen.

Sitzungen

Navigieren Sie zu Farm-Einstellungen > Administratoren > Sitzungen, um aktuelle RAS-Verwaltungssitzungen anzuzeigen.

Um sich von einer Sitzung abzumelden, klicken Sie mit der rechten Maustaste darauf und wählen dann die Option Sitzung beenden aus.

Mailbox

Eine Mailbox-Konfiguration in einer RAS-Farm wird verwendet, um E-Mail-Einladungen an Benutzer zu senden, die einer Parallels RAS-Farm beitreten möchten, und um Ereignisbenachrichtigungen an andere E-Mail-Adressen zu senden. Für eine Serverfarm kann nur eine Mailbox konfiguriert werden.

So konfigurieren Sie eine Mailbox:

1. Navigieren Sie in der RAS-Konsole zu Farm-Einstellungen > Mailbox.
2. Klicken Sie auf Bearbeiten und geben Sie Folgendes an:
   - Mailserver: Geben Sie den Servernamen des Postfachs ein. Beispielsweise mail.company.com:500
   - TLS/SSL: Wählen Sie aus, ob Sie TLS- oder SSL-Protokollierung verwenden möchten.
   - Der Proxy-Server erfordert Authentifizierung: Wählen Sie diese Option, wenn Ihr Proxy-Server Authentifizierung erfordert. Wenn das der Fall ist, geben Sie außerdem den Benutzernamen und das Passwort in die dafür vorgesehenen Felder ein.
   - Absender-Informationen: Geben Sie die E-Mail-Adresse ein.
3. Klicken Sie auf Speichern.

Lizenzierung

Navigieren Sie zu Farm-Einstellungen > Lizenzierung, um die Parallels RAS-Lizenzierungsinformationen anzuzeigen. Folgende Informationen werden angezeigt:

- Lizenztyp: Der Typ der aktuell verwendeten Parallels RAS-Lizenz (z. B. Abonnement, Testversion usw.).
- Ablaufdatum: Das Ablaufdatum der Lizenz (oder die Anzahl der verbleibenden Tage, je nach Lizenztyp).

- Maximal zulässige gleichzeitige Benutzer: Die maximale Anzahl gleichzeitiger Benutzer, die die aktuelle Lizenz erlaubt.
- Benutzerspitze: Die Anzahl der bisherigen Höchstzahl der gleichzeitigen Benutzer im Falle eines Abonnements bzw. die monatlichen Höchstzahl der gleichzeitigen Benutzer und die tägliche Nutzung im Falle einer SPLA-Lizenz.
- Aktuelle Benutzer: Die Anzahl der Benutzer, die derzeit mit der Farm verbunden sind.

Bitte beachten Sie, dass Sie diese Informationen (und mehr) auch in Ihrem Parallels-Account einsehen können. Weitere Informationen finden Sie im Parallels RAS-Lizenzierungshandbuch, das auf der Parallels-Website verfügbar ist.

Lizenz-Verwaltung

Klicken Sie auf den Link Lizenz-Verwaltung oben auf der Seite Lizenzierung, um die Seite Lizenz-Verwaltung aufzurufen.

Wenn Sie ein Parallels Business-Konto haben, melden Sie sich bitte mit den Zugangsdaten für dieses Konto an. Wenn Sie kein Konto besitzen, klicken Sie auf Registrieren, geben Sie die entsprechenden Informationen ein und klicken Sie auf Registrieren. Ein Business-Konto für Ihre Organisation wird erstellt. Weitere Informationen zu Parallels-Konten und das Parallels My Account-Portal finden Sie im Parallels RAS-Lizenzierungshandbuch auf der Parallels-Website unter folgender URL: https://www.parallels.com/de/products/ras/resources/.

Sobald Sie dort angemeldet sind, können Sie auf der Seite „Lizenz-Verwaltung“ Folgendes tun:

- Aktivieren Sie die Farm mit dem in Ihrem Abonnement inbegriffenen Lizenzschlüssel. Wenn Sie sich mit Ihrem Parallels Business-Konto anmelden, werden die Lizenzinformationen abgerufen und auf dem Bildschirm angezeigt. Um die Farm zu aktivieren, wählen Sie in der Liste einen Lizenzschlüssel aus und klicken auf Weiter.
- Testversion aktivieren – Wählen Sie die Option Testversionslizenz aktivieren aus und klicken Sie auf Weiter.
- Deaktivieren der aktuell verwendeten Lizenz – Wählen Sie die Option Lizenz deaktivieren aus und klicken Sie auf Weiter. Dier Lizenzschlüssel wurde erfolgreich deaktiviert und kann verwendet werden, um eine andere Farm zu aktivieren. Sie können die Farm jederzeit reaktivieren, indem Sie diesen oder einen anderen Lizenzschlüssel verwenden.

Wenn Sie in einem der oben beschriebenen Szenarien auf Weiter klicken, werden die Seite Fortschritt und der entsprechende Fortschritt des Vorgangs angezeigt. Sobald dieser Vorgang abgeschlossen ist, wird die Seite mit dem entsprechenden Ergebnis aktualisiert.

Sobald Sie die Farm aktiviert haben, können Sie mit der Verwaltung derselben beginnen. Wenn Sie die Farm deaktiviert haben, werden im Verwaltungsportal alle Einstellungen außer Lizenzierung deaktiviert.

KAPITEL 6

Site-Einstellungen

Die Gruppierung auf der nächsten Ebene in der Serverfarm-Hierarchie ist die Site, die Kernkomponenten, Sitzungshosts und andere Objekte enthält, die Verbindungen und Remote-Anwendungsdienste bereitstellen.

Um die globalen Site-Einstellungen zu verwalten, klicken Sie in der Seitenleiste auf die Kategorie Seiten-Einstellungen.

In diesem Kapitel

Verbinden und Authentifizierung 23
Multifaktor-Authentifizierung 25
FSLogix-Profilcontainer 32
Universelles Drucken 37
Universal Scanning 40

Verbinden und Authentifizierung

Die Verbindungs- und Authentifizierungseinstellungen verwalten Sie über Site-Einstellungen > Verbindung.

Wahl des Authentifizierungstyps

Wenn sich die Benutzer mit einer Site verbinden wollen, müssen sie sich vor der Anmeldung authentifizieren. Um den Authentifizierungstyp im Fenster Verbinden zu konfigurieren, wählen Sie Authentifizierung und dann eine der folgenden Optionen aus:

- Anmeldeinformationen. Die Benutzer-Anmeldeinformationen werden durch das Windows-System validiert, auf dem RAS läuft. Die für die Windows-Authentifizierung benutzten Anmeldedaten werden auch verwendet, um sich bei einer RDP-Sitzung anzumelden.
- Smartcard. Smartcard-Authentifizierung. Ähnlich wie bei der Windows-Authentifizierung können Smartcard-Anmeldedaten sowohl von RAS als auch von RDP verwendet werden. Daher müssen Smartcard-Anmeldedaten nur einmal eingegeben werden. Anders als bei der Windows-Authentifizierung muss der Benutzer nur die PIN der Smartcard kennen. Der

Benutzername wird automatisch aus der Smartcard bezogen, daher muss der Benutzer ihn nicht eingeben.

- Web (SAML). SAML SSO-Authentifizierung.

Beachten Sie: Wenn die Smartcard-Authentifizierung deaktiviert ist, verknüpft RAS Connection Broker den Local Security Authority Subsystem Service (LSASS) nicht. Die Smartcard-Authentifizierung kann in Parallels Client für Windows, Mac und Linux verwendet werden. Beachten Sie auch, dass Smartcards nicht zur Authentifizierung verwendet werden können, wenn der Parallels Client innerhalb einer RDP-Sitzung ausgeführt wird.

Für die Verwendung von Smartcards muss ein gültiges Zertifikat auf einem Endgerät installiert sein. Dazu müssen Sie das Stammzertifikat der Zertifizierungsstelle in den Schlüsselspeicher des Geräts importieren.

Ein Zertifikat muss die folgenden Kriterien erfüllen:

- Das Feld „Key Usage“ muss eine digitale Signatur enthalten.
- Das Feld „Alternative Antragstellernamen“ (Subject Alternative Name – SAN) muss einen Benutzerhauptnamen („User Principal Name“, UPN) enthalten.
- Das Feld „Enhanced Key Usage“ muss die Anmeldung an der Smartcard und die Client-Authentifizierung enthalten.

Authentifizierungsdomänen

Um eine Domain (oder mehrere Domains) anzugeben, für die diese Authentifizierung ausgeführt werden soll, wählen Sie eine der folgenden Optionen aus:

- Spezifisch: Wählen Sie diese Option aus und geben Sie einen spezifischen Domänennamen ein.
- Alle vertrauenswürdigen Domänen. Wenn die Informationen über Benutzer, die sich mit Parallels RAS verbinden, in verschiedenen Domänen innerhalb eines Server-Forests gespeichert sind, wählen Sie die Option Alle vertrauenswürdigen Domänen, um eine Authentifizierung bei mehreren Domänen vorzunehmen.
- Client-Domäne verwenden, falls angegeben. Wählen Sie diese Option, um die Domäne zu verwenden, die in den Eigenschaften der Parallels Clientverbindung festgelegt ist. Wenn auf Seiten des Clients kein Domänenname angegeben ist, wird die Authentifizierung entsprechend den oben angeführten Einstellungen durchgeführt.
- Verwendung von NetBIOS-Anmeldeinformationen für Clients vorgeben. Wenn diese Option ausgewählt ist, ersetzt der Parallels Client den Benutzernamen durch den NetBIOS-Benutzernamen.

Hinweis: Wenn ein Zertifikat auf Ihrer Smartcard den Hauptnamen eines Benutzers (UPN) im Feld „Alternativer Antragstellername“ (Subject Alternative Name – SAN) nicht enthält (oder wenn das Feld „Alternativer Antragstellername“ überhaupt nicht vorhanden ist) müssen Sie die Option Verwendung von NetBIOS-Anmeldeinformationen für Clients vorgeben.

Empfehlung: Nachdem Sie die Domänennamen geändert oder andere Änderungen in Verbindung mit der Authentifizierung durchgeführt haben, sollten Sie zwischengespeicherte Session-IDs löschen. Zu diesem Zeitpunkt kann das nur von der RAS-Konsole aus gemacht werden. Dort klicken Sie auf die Schaltfläche Zwischengespeicherte Session-IDs löschen (auf der Registerkarte Einstellungen).

Um die Authentifizierung von Benutzersitzungen für Benutzer auf einer eigenständigen Maschine durchzuführen, müssen Sie anstelle des Domänennamens das Format [Arbeitsgruppenname] / [Computername] verwenden. Wenn Sie beispielsweise Benutzer anhand einer Liste lokaler Benutzer auf einem Computer namens SERVER1 authentifizieren möchten, der Mitglied der Arbeitsgruppe WORKGROUP ist, lautet der Eintrag im Feld „Domäne“ wie folgt: WORKGROUP/SERVER1.

Domainpasswort ändern

Sie können Parallels Client so konfigurieren, dass er eine benutzerdefinierte URL zum Ändern von Domain-Passwörtern verwendet.

Damit Parallels Client eine benutzerdefinierte URL zum Ändern von Domain-Passwörtern verwendet:

1. Wählen Sie die Option Benutzerdefinierten Link für das Feld „Domain-Passwort ändern“.
2. Den Link in das untenstehende Textfeld eingeben.

Erlaubte Geräte

Im Fenster Erlaubte Geräte geben Sie an, ob Clients die neuesten Sicherheitspatches installiert haben müssen, um sich mit der Farm verbinden zu dürfen. Diese Option muss normalerweise ausgewählt werden, um Ihre Umgebung vor Sicherheitsrisiken zu schützen. Sie sollten sie nur deaktivieren, wenn Sie eine ältere Version von Parallels Client verwenden müssen, auf der keine Sicherheitspatches installiert sind. Weitere Informationen finden Sie im folgenden Artikel der Wissensdatenbank: https://kb.parallels.com/de/125112.

Multifaktor-Authentifizierung

Um die Multi-Faktor-Authentifizierung (MFA) zu konfigurieren, navigieren Sie zu Site-Einstellungen > Verbindung > Multi-Faktor-Authentifizierung.

Wenn die Multifaktor-Authentifizierung verwendet wird, müssen die Benutzer in zwei aufeinanderfolgenden Phasen authentifiziert werden, um Zugriff auf die Liste der Anwendungen zu erhalten: Native Authentifizierung (Active Directory / LDAP) und eine der folgenden MFA:

- RADIUS (S. 26)
  - Azure MFA (RADIUS)
  - Duo (RADIUS)
  - FortiAuthenticator (RADIUS)
  - TekRADIUS
  - RADIUS
- TOTP
  - Google Authenticator (S. 28)
  - Microsoft Authenticator
  - TOTP (Einmalpasswort)
- Deepnet
- SafeNet

Bitte beachten Sie, dass das RAS-Verwaltungsportal zum Zeitpunkt der Erstellung dieses Dokuments nur verwendet werden kann, um RADIUS oder TOTP MFA-Anbieter hinzuzufügen und zu konfigurieren. Um andere Anbieter zu konfigurieren, müssen Sie die Desktop-basierte Parallels RAS-Konsole verwenden.

Verwenden von RADIUS

RADIUS MFA-Anbieter hinzufügen

RADIUS MFA-Anbieter hinzufügen:

1. Navigieren Sie zu Site-Einstellungen > Verbindung > Multi-Faktor-Authentifizierung.
2. Klicken Sie auf das Plus-Symbol und wählen Sie dann den Anbieter aus, den Sie hinzufügen möchten.
3. Geben Sie Folgendes an:
   - Name: Name des Anbieters.
   - Beschreibung: Beschreibung des Anbieters.
   - Wählen Sie in der Tabelle Design die Designs aus, die diesen MFA-Anbieter verwenden sollen.

4 Klicken Sie auf Weiter.

5 Geben Sie Folgendes an:

- Anzeigename: Geben Sie den Namen des Verbindungstyps ein, der auf dem Anmeldebildschirm auf dem Client angezeigt wird. Dies sollte der Name sein, den Ihre Benutzer eindeutig verstehen.
- Primärer Server und Sekundärer Server: Mit diesem beiden Feldern können Sie angeben, ob in der Konfiguration ein oder zwei RADIUS-Server enthalten sein sollen. Wenn Sie zwei Server angeben, können Sie Hochverfügbarkeit für RADIUS-Hosts konfigurieren (siehe unten). Geben Sie einen Server ein, indem Sie seinen Hostnamen oder die IP-Adresse eingeben oder klicken Sie auf die Schaltfläche [...], um einen Server über Active Directory auszuwählen.

  Wenn zwei RADIUS-Server angegeben sind, wählen Sie aus der Dropdownliste HA-Modus einen der folgenden Hochverfügbarkeitsmodi aus. Aktiv-aktiv (parallel) bedeutet, dass der Befehl an beide Server zugleich geschickt wird. Es wird der verwendet, der zuerst antwortet. Aktiv-passiv (Failover) bedeutet, dass Failover und Zeitlimit verdoppelt werden und Parallels RAS auf Antwort beider Hosts wartet.
- HA-Modus: Siehe Primärer Server und Sekundärer Server oben: Wenn nur der Primäre Server angegeben ist, ist dieses Feld deaktiviert.
- Port: Geben Sie die Portnummer für den RADIUS-Server ein. Klicken Sie auf die Schaltfläche Standard, um den Standardwert zu verwenden.
- Zeitlimit: Geben Sie das Zeitlimit für das Paket in Sekunden an.
- Erneute Versuche: Geben Sie die Anzahl der erneuten Versuche für die Herstellung einer Verbindung an.
- Geheimer Schlüssel: Geben Sie den geheimen Schlüssel ein.
- Passwortverschlüsselung: Wählen Sie PAP (Password Authentication Protocol) oder CHAP (Challenge Handshake Authentication Protocol), je nach den Einstellungen auf Ihrem RADIUS-Server.

6 Klicken Sie zum Abschluss auf Erstellen.

RADIUS MFA-Anbieter konfigurieren

Einen RADIUS MFA-Anbieter konfigurieren:

1 Navigieren Sie zu Site-Einstellungen > Verbindung > Multi-Faktor-Authentifizierung.

2 Doppelklicken Sie auf den Anbieter, den Sie konfigurieren möchten.

3 Klicken Sie auf die Schaltfläche Bearbeiten.

4 Folgende Kategorien können konfiguriert werden:

- Kategorien Algemein und Verbindung: Siehe oben.
- Attribute: Siehe https://download.parallels.com/ras/v19/docs/de_DE/Parallels-RAS-19-Administrators-Guide/46769.htm.

  Hinweis: Einmal erstellte Attribute können im RAS-Verwaltungsportal nicht mehr bearbeitet werden. Um Attribute zu bearbeiten, verwenden Sie die desktopbasierte Parallels RAS-Konsole.

- Automatisierung: Siehe https://download.parallels.com/ras/v19/docs/de_DE/Parallels-RAS-19-Administrators-Guide/46770.htm.
- Beschränkungen: Siehe MFA-Regeln konfigurieren (S. 30).

5 Klicken Sie zum Abschluss auf Speichern.

Verwenden von Google Authenticator

In diesem Abschnitt erklären wir, wie Sie den Google Authenticator konfigurieren.

So konfigurieren Sie Google Authenticator:

1 Navigieren Sie zu Site-Einstellungen > Verbindung > Multi-Faktor-Authentifizierung.

2 Doppelklicken Sie auf den Google Authenticator, den Sie konfigurieren möchten.

3 Klicken Sie auf die Schaltfläche Bearbeiten.

4 Geben Sie Folgendes an:

- Name: Name des Anbieters.
- Beschreibung: Beschreibung des Anbieters.
- Wählen Sie in der Tabelle Design die Designs aus, die diesen MFA-Anbieter verwenden sollen.
- Anzeigename: Der Standardname ist hier „Google Authenticator“. Der Name wird im Registrierungsdialog im Parallels Client im folgenden Satz angezeigt: „Installieren Sie die Google Authenticator-App auf Ihrem iOS- oder Android-Gerät“. Wenn Sie den Namen ändern, enthält der Satz den von Ihnen angegebenen Namen, wie z. B. „Installieren Sie <neuer Name> auf Ihrem iOS- oder Android-Gerät“. Technisch gesehen können Sie jede beliebige Authentifizierer-Anwendung verwenden (daher die Möglichkeit, den Namen zu ändern), aber zum Zeitpunkt dieses Artikels wird ausschließlich die Google Authenticator-Anwendung offiziell unterstützt.
- Ändern Sie, falls erforderlich, die standardmäßig vorgegebene TOTP-Toleranz.

- Im Abschnitt Registrierung können Sie die Benutzerregistrierung über Google Authenticator bei Bedarf einschränken. Sie können allen Benutzern die Registrierung ohne Einschränkungen erlauben (Option Zulassen), die Registrierung bis zum angegebenen Datum und zur angegebenen Zeit erlauben (Option Zulassen bis) oder die Registrierung vollständig deaktivieren (Option Nicht zulassen). Wenn die Registrierung aufgrund eines abgelaufenen Zeitraums oder der aktivierten Option Nicht zulassen deaktiviert wurde, wird einem Benutzer, der versucht, sich anzumelden, eine Fehlermeldung angezeigt, die besagt, dass die Registrierung deaktiviert ist, und dem Benutzer rät, sich an den Systemadministrator zu wenden. Wenn Sie die Registrierung einschränken oder deaktivieren, kann Google Authenticator oder ein anderer TOTP-Anbieter weiterhin verwendet werden, jedoch mit zusätzlicher Sicherheit, durch die keine weitere Benutzerregistrierung zugelassen wird. Hierbei handelt es sich um eine Sicherheitsmaßnahme, um Benutzer mit kompromittierten Anmeldeinformationen davon abzuhalten, sich bei MFA zu registrieren.
- Das Feld Benutzer zurücksetzen im Abschnitt Benutzerverwaltung wird verwendet, um den Token zurückzusetzen, den ein Benutzer erhalten hat, als er versucht hat, sich zum ersten Mal mit Google Authenticator bei Parallels RAS anzumelden. Wenn Sie einen Benutzer zurücksetzen, muss er das Registrierungsverfahren erneut durchlaufen (siehe Verwendung von Google Authenticator im Parallels Client unten). Sie können nach bestimmten Benutzern suchen, alle Benutzer zurücksetzen oder die Liste der Benutzer aus einer CSV-Datei importieren.
- Beschränkungen: Siehe MFA-Regeln konfigurieren (S. 30).

5 Klicken Sie zum Abschluss auf Speichern.

Verwendung von Google Authenticator im Parallels Client

Wichtig: Um Google Authenticator oder andere TOTP-Anbieter verwenden zu können, muss die Zeit auf einem Benutzergerät mit der Zeit auf dem RAS Connection Broker-Server synchronisiert sein. Andernfalls schlägt die Google-Authentifizierung fehl.

Google Authenticator wird im Parallels Client unterstützt und läuft auf allen unterstützten Plattformen (mobil, Desktop und Web Client).

Um Google Authenticator zu verwenden, muss ein Nutzer die Authenticator-App auf seinem iOS- oder Android-Gerät installieren. Besuchen Sie einfach Google Play oder den App Store und installieren Sie die App. Sobald die Authenticator-App installiert ist, kann der Benutzer eine Verbindung zu Parallels RAS mit Zwei-Faktor-Authentifizierung herstellen.

So wird die Verbindung mit Parallels RAS hergestellt:

1 Der Benutzer öffnet den Parallels Client oder das Nutzerportal und meldet sich mit seinen Zugangsdaten an.

2 Das Multi-Faktor-Authentifizierungsdialogfeld wird geöffnet und zeigt einen Barcode (auch bekannt als QR-Code) und einen geheimen Schlüssel an.

3 Der Nutzer öffnet die Google Authenticator-App auf seinem mobilen Gerät:

- Wenn er es zum ersten Mal benutzt, tippt er auf Beginnen und dann auf Barcode scannen.
- Wenn ein Nutzer bereits ein anderes Konto in Google Authenticator hat, tippt er auf das Plus-Zeichen-Symbol und wählt Barcode scannen.

4 Der Benutzer scannt dann den Barcode, der im Anmeldedialog des Parallels Clients angezeigt wird.

Wenn das Scannen aus irgendeinem Grund nicht funktioniert, wechselt der Benutzer zurück zur App, wählt Enter a provided key (Bereitgestellten Schlüssel eingeben) und gibt dann den Kontonamen und den Schlüssel ein, der im Anmeldedialogfeld des Parallels Clients angezeigt wird.

5 Der Benutzer tippt dann auf Add account (Konto hinzufügen) in der App, dadurch wird ein Konto erstellt und ein Einmal-Passwort angezeigt.

6 Der Benutzer geht zurück zum Parallels Client, klickt auf Weiter und gibt das Einmal-Passwort in das Feld OTP ein.

Bei jeder weiteren Anmeldung muss der Nutzer nur seine Zugangsdaten (oder gar nichts, wenn die Option Passwort speichern ausgewählt wurde) und ein einmaliges Passwort eingeben, das er von der Google Authenticator-App erhält (die Anwendung generiert ständig ein neues Passwort). Wenn ein RAS-Administrator einen Benutzer zurücksetzt (siehe Feldbeschreibung Benutzer zurücksetzen am Anfang dieses Abschnitts), muss der Benutzer den oben beschriebenen Registrierungsvorgang wiederholen.

Konfiguration von MFA-Regeln

Die Multifaktor-Authentifizierung (MFA) kann für alle Benutzerverbindungen aktiviert oder deaktiviert werden, aber Sie können für bestimmte Verbindungen auch komplexe Regeln konfigurieren. Mit dieser Funktion können Sie verschiedene MFA für denselben Benutzer oder Computer erstellen, aktivieren oder deaktivieren, die je nachdem gelten, von wo und über welches Gerät sich der Benutzer angemeldet hat. Jeder MFA-Anbieter hat eine Regel, die aus einem oder mehreren Kriterien für den Abgleich mit Benutzer-Verbindungen besteht. Jedes Kriterium besteht wiederum aus einem oder mehreren spezifischen Objekten, die abgeglichen werden können.

Sie können die folgenden Objekte abgleichen:

- Benutzer, eine Gruppe, zu der der Benutzer gehört, oder der Computer, von dem aus der Benutzer eine Verbindung herstellt.

- Das Secure Gateway, mit dem sich der Benutzer verbindet.
- Name des Client-Geräts.
- Betriebssystem des Client-Geräts.
- IP-Adresse.
- Hardware-ID. Das Format einer Hardware-ID hängt vom Betriebssystem des Clients ab.

Beachten Sie bitte folgende Hinweise zu den Regeln:

- Die Kriterien werden mit dem AND-Operator verknüpft. Wenn eine Regel beispielsweise ein Kriterium enthält, das auf bestimmte IP-Adressen zutrifft, und ein Kriterium, das auf die Betriebssysteme der Client-Geräte zutrifft, wird die Regel angewendet, wenn eine Benutzer-Verbindung mit einer der IP-Adressen UND einem der Client-Betriebssysteme übereinstimmt.
- Die Kriterien werden mit dem OR-Operator verknüpft. Wenn Sie z. B. nur ein Kriterium für passende Client-Geräte-Betriebssysteme erstellen, wird die Regel angewendet, wenn eines der Betriebssysteme mit der Clientverbindung übereinstimmt.

So konfigurieren Sie eine Regel:

1 Navigieren Sie zu Site-Einstellungen > Verbindung > Multi-Faktor-Authentifizierung.

2 Doppelklicken Sie auf den Google Authenticator, den Sie konfigurieren möchten.

3 Klicken Sie auf den Link Beschränkungen.

4 Klicken Sie auf die Schaltfläche Bearbeiten.

5 Deaktivieren Sie die Option Standardeinstellungen erben.

6 Geben Sie die Kriterien für die Regel an. Folgende Steuerelemente sind verfügbar:

- Erlauben: gibt an, dass der MFA-Anbieter aktiviert werden muss, wenn eine Benutzer-Verbindung den Kriterien entspricht. Klicken Sie auf Erlauben, um die Option auf Ablehnen zu ändern.
- Ablehnen: legt fest, dass die Richtlinie des MFA-Anbieters nicht aktiviert werden darf, wenn eine Benutzer-Verbindung den Kriterien entspricht. Klicken Sie auf Ablehnen, um die Option auf Erlauben zu ändern.
- (+): fügt ein neues Kriterium hinzu. Wenn Sie ein Secure Gateway, einen Client-Gerätenamen, ein Client-Gerätebetriebssystem, eine IP-Adresse oder eine Hardware-ID abgleichen möchten, klicken Sie auf (+).
- Ist: gibt an, dass der MFA-Anbieter aktiviert sein muss (oder deaktiviert, durch Erlauben und Ablehnen) wenn eine Benutzer-Verbindung den Kriterien entspricht. Klicken Sie auf „Ist“, um dieses Steuerungselement auf Ist nicht zu ändern. Dieses Steuerungselement wird angezeigt, wenn mindestens ein Objekt hinzugefügt wurde.

- Ist nicht: gibt an, dass der MFA-Anbieter aktiviert sein muss (oder deaktiviert, durch Erlauben und Ablehnen) wenn eine Benutzer-Verbindung den Kriterien nicht entspricht. Klicken Sie auf „Ist nicht“, um dieses Steuerungselement auf Ist zu ändern. Dieses Steuerungselement wird angezeigt, wenn mindestens ein Objekt hinzugefügt wurde.

Sie können die Kriterien auch aktivieren/deaktivieren, indem Sie links daneben auf den Schalter klicken.

7 Klicken Sie zum Abschluss auf Speichern.

FSLogix-Profilcontainer

Hinweis: Wenn Sie eine bestehende FSLogix-Profilcontainer-Konfiguration haben, die von Parallels RAS verwaltet werden soll, lesen Sie bitte zusätzliche Anweisungen in Verwaltung bestehender Profile durch Parallels RAS konfigurieren (S. 34).

Microsoft FSLogix Profile Container ist die bevorzugte Benutzerprofil-Verwaltungslösung als Nachfolger von Roaming Profiles und Benutzerprofil-Disks (UPDs). Es soll den Benutzerkontext in nicht persistenten Umgebungen aufrechterhalten, die Anmeldezeiten minimieren, eine native Profilerfahrung bieten und damit Kompatibilitätsprobleme beseitigen.

Ab Version 18 bietet Ihnen Parallels die Möglichkeit, FSLogix-Profilcontainer zu integrieren, zu konfigurieren, zu warten und zu unterstützen. Dabei werden Storage Spaces Direct, Azure Files und Azure NetApp Files unterstützt, basierend auf den unterstützten Protokollen wie SMB und Cloud Cache für Ausfallsicherheit und Verfügbarkeit.

Folgende FSLogix-Profilcontainer werden unterstützt

Parallels RAS wurde mit FSLogix-Profilcontainer-Releases bis einschließlich Release 2105 getestet.

Voraussetzungen

FSLogix-Profilcontainer-Lizenzberechtigung, die in den folgenden Lizenzen enthalten ist:

- Microsoft 365 E3, E5
- Microsoft 365 A3, A5, Student Use Benefits
- Microsoft 365 F1, F3
- Microsoft 365 Business
- Windows 10 Enterprise E3, E5
- Windows 10 Education A3, A5

- Windows 10 VDA pro Benutzer
- Client-Zugriffslizenz (CAL) für Remotedesktopdienste (RDS)
- Abonnenten-Zugangslizenz (SAL) für Remotedesktopdienste (RDS)

Weitere Voraussetzungen sind:

- Profilcontainer-Speicherung gemäß den Empfehlungen von FSLogix konfiguriert.
- Richtlinien für Gruppenrichtlinienobjekte (Group Policy Object, GPO), die sich auf FSLogix beziehen, müssen auf Hosts deaktiviert werden, auf denen Parallels RAS FSLogix-Einstellungen verwaltet.

Installieren Sie die FSLogix-Profilcontainer-Anwendung in Parallels RAS

So installieren Sie die FSLogix-Profilcontainer-Anwendung im Parallels RAS-Verwaltungsportal:

1. Navigieren Sie zu Site-Einstellungen > FSLogix.
2. Klicken Sie im rechten Fensterbereich auf Bearbeiten und wählen Sie eine der folgenden Installationsmethoden aus:
   - Manuell installieren: Nutzen Sie die FSLogix-Profilcontainer-Anwendung, die manuell auf einem Host installiert wird (Parallels RAS installiert den FSLogix-Agent nicht).
   - Online installieren: Installieren Sie FSLogix-Profilcontainer von der Microsoft-Website. Wählen Sie in der Dropdownliste eine der folgenden unterstützten Versionen aus: Wählen Sie Benutzerdefinierte URL aus und geben Sie eine URL in das Feld ein, um eine benutzerdefinierte URL anzugeben. Klicken Sie auf Aktuellste erkennen, um die aktuellste unterstützte Version anzuzeigen. Die aktuellste Version wird identifiziert und dann der Dropdownliste Online installieren hinzugefügt.
   - Von einer Netzwerkfreigabe aus installieren: Installieren Sie den FSLogix-Agent, den Sie lokal zur Verfügung haben (Parallels RAS benötigt ein offizielles ZIP-Archiv, wie es von Microsoft bereitgestellt wird).
   - Von RAS Connection Broker pushen: Die aktuellste Version des FSLogix-Agent wird heruntergeladen und im RAS Connection Broker gespeichert, um sie dann auf die Ziel-Sitzungshosts zu übertragen.

Konfigurieren eines Sitzungshosts zur Verwendung mit FSLogix-Profilcontainer

Bitte beachten Sie, dass zum Zeitpunkt der Erstellung dieses Dokuments das RAS-Verwaltungsportal nur verwendet werden kann, um RD-Sitzungshosts für die Verwendung von FSLogix-Profilcontainern zu konfigurieren. Für andere Hosttypen verwenden Sie bitte die desktopbasierte RAS-Konsole.

So konfigurieren Sie einen Sitzungshost:

1. Navigieren Sie zu Infrastruktur > RD-Sitzungshosts.
2. Klicken Sie auf einen Host in der Liste und dann auf Eigenschaften.
3. Klicken Sie im mittleren Bereich auf Benutzerprofil.
4. Klicken Sie auf Bearbeiten, um die Bearbeitung zu ermöglichen. Um die Standardwerte des Hostpools oder der Site zu überschreiben, deaktivieren Sie Standardwerte übernehmen und geben Ihre eigenen Einstellungen ein. Um die Standardwerte des Hostpools oder der Site zu ändern, klicken Sie auf den entsprechenden Link und führen Sie dann die Bearbeitung in der jeweiligen Ansicht durch.
5. Legen Sie die Einstellungen nach Ihren Bedürfnissen fest.

Verwaltung bestehender Profile durch Parallels RAS konfigurieren

In diesem Thema wird beschrieben, wie Sie vorhandene FSLogix-Profilcontainer so konfigurieren, dass sie von Parallels RAS verwaltet werden. Die Konfiguration des FSLogix-Profilcontainers definiert, wie und wohin das Profil umgeleitet wird. Normalerweise konfigurieren Sie Profile über Registry-Einstellungen und GPO. Parallels RAS bietet Ihnen die Möglichkeit, Profile von der Parallels RAS-Konsole oder dem RAS-Verwaltungsportal aus zu konfigurieren, ohne externe Tools zu verwenden.

Vor dem Start

Bevor Sie FSLogix Profile Containers in Parallels RAS konfigurieren, sollten Sie Folgendes beachten:

- Die Profile selbst müssen Sie nicht ändern; bestehende Profile bleiben erhalten.
- Sie können Ihre vorhandenen Speicherorte für FSLogix-Profilcontainer wie etwa SMB-Netzwerkfreigaben oder Cloud Cache weiterhin verwenden.

Vorbereitende Schritte

Bitte führen Sie die folgenden vorbereitenden Schritte aus:

1. Sichern Sie Ihre vorhandenen Profile. Es ist höchst unwahrscheinlich, dass Profildaten verloren gehen oder beschädigt werden, aber es ist das beste Verfahren, vor jeder Änderung der Profilkonfiguration einen gültigen Backup zu erstellen.
2. Schalten Sie die GPO-Konfiguration von FSLogix-Profilcontainern aus. Dieser Schritt ist wichtig, weil Sie nicht gleichzeitig die GPO- und die Parallels RAS-Verwaltung von FSLogix-Profilen aktiviert haben können.
3. Bevor Sie FSLogix-Profile für einen Server in einer RAS-Serverfarm konfigurieren, stellen Sie sicher, dass auf dem Server keine Benutzersitzungen ausgeführt werden. Als Vorschlag

können Sie den Übergang in einem Wartungsfenster außerhalb der Arbeitszeiten vornehmen.

GPO und FSLogix-Konfiguration replizieren

Um bestehende FSLogix-Profilcontainer in Parallels RAS zu konfigurieren, müssen Sie Ihr bestehendes GPO auf die FSLogix-Konfiguration in Parallels RAS replizieren. Dies kann in der Parallels RAS-Konsole oder im Parallels-Verwaltungsportal erfolgen.

So konfigurieren Sie Profile im RAS-Verwaltungsportal:

1. Navigieren Sie zu Infrastruktur > RD-Sitzungshosts.
2. Klicken Sie auf einen Host in der Liste und dann auf Eigenschaften.
3. Klicken Sie im mittleren Bereich auf Benutzerprofil.
4. Geben Sie im Listenfeld Speicherort von Profil-Datenträgern die vorhandenen SMB- oder Cloud-Cache-Speicherorte an, an denen Sie Ihre FSLogix-Profile aufbewahren. Geben Sie außerdem das Format des Profil-Datenträgers, den Zuordnungstyp und die Standardgröße an.
5. Im mittleren Fenster klicken Sie auf die Objekte Benutzer und Gruppen, Ordner und Erweitert, um den Rest der FSLogix-Einstellungen, die Sie möglicherweise auf Ihren Servern haben, wie z. B. Benutzerausschlüsse, Ordnerausschlüsse und andere, zu konfigurieren.

Bitte beachten Sie, dass zum Zeitpunkt der Erstellung dieses Dokuments das RAS-Verwaltungsportal nur verwendet werden kann, um RD-Sitzungshosts für die Verwendung von FSLogix-Profilcontainern zu konfigurieren. Für andere Hosttypen verwenden Sie bitte die desktopbasierte RAS-Konsole (wie unten beschrieben).

So konfigurieren Sie Profile in der RAS-Konsole:

1. Öffnen Sie die Registerkarte Benutzerprofile auf einem Host, Site-Standardeinstellungen oder dem Dialogfeld Vorlagen-Eigenschaften.
2. Geben Sie im Listenfeld Speicherort von Profil-Datenträgern die vorhandenen SMB- oder Cloud-Cache-Speicherorte an, an denen Sie Ihre FSLogix-Profile aufbewahren. Geben Sie außerdem das Format des Profil-Datenträgers, den Zuordnungstyp und die Standardgröße an.
3. Klicken Sie auf die Schaltfläche Zusätzliche Einstellungen und konfigurieren Sie den Rest der FSLogix-Einstellungen, die Sie möglicherweise auf Ihren Servern haben, wie z. B. Benutzerausschlüsse, Ordnerausschlüsse und andere.

Empfehlungen und Tests

Wenn Sie die Schritte im vorherigen Abschnitt ausführen, konfigurieren Sie nicht gleich mehrere (oder alle) Server in einer RAS-Serverfarm. Beginnen Sie mit einem einzelnen Server (z. B. einem RD-Sitzungshost) und testen Sie ihn dann mit einer einzelnen Benutzerverbindung. Konfigurieren Sie danach einige andere Server und testen Sie, indem sich derselbe Benutzer nacheinander bei mehreren Servern anmeldet, um zu bestätigen, dass das Profil geladen und die Personalisierung unabhängig von einem Sitzungshost beibehalten wird. Wenn alles in Ordnung ist, konfigurieren Sie andere Host-, Hostpool- oder Site-Standardwerte.

Ihre RAS-Benutzer können sich jetzt mit Parallels RAS verbinden, indem sie bereits vorhandene FSLogix-Profilcontainer verwenden, die jetzt zentral über Parallels RAS verwaltet werden.

Site-Standardeinstellungen und Hosts für FSLogix konfigurieren

FSLogix konfigurieren:

1 Führen Sie einen der folgenden Schritte aus:

- Um die Standardeinstellungen des Standorts zu konfigurieren, gehen Sie zu Infrastruktur > Hostpools > RD-Sitzungshosts > Eigenschaften > Standardeinstellungen des Standorts > Benutzerprofil.
- Um Hostpools zu konfigurieren, gehen Sie zu Infrastruktur > Hostpools > <Hostpoolname> > Eigenschaften > Benutzerprofil.
- Um einzelne Hosts zu konfigurieren, gehen Sie zu Infrastruktur > RD-Sitzungshosts > <Hostname> > Eigenschaften > Benutzerprofil.

2 Wenn Sie die Profilcontainer verwenden möchten, gehen Sie zu Benutzerprofil > FSLogix – Profilcontainer:

- Benutzer und Gruppen: Legen Sie ein- und ausschließende Benutzer- und Gruppenlisten fest. Standardmäßig wird "Jeder" zur Einschlussliste des FSLogix-Profils hinzugefügt. Wenn einige Benutzerprofile lokal bleiben sollen, können Sie diese Benutzer zur Ausschlussliste hinzufügen. Benutzer und Gruppen können in beiden Listen vorhanden sein, aber das Ausschließen hat Vorrang.
- Ordner: Legen Sie ein- und ausschließende Listen für Ordner fest. Sie können aus vorhandenen Ordnern auswählen oder einen Ordner eingeben. Bitte beachten Sie, dass sich die Ordner im Pfad des Benutzerprofils befinden müssen.
- Disks: Geben Sie die Einstellungen des Profildatenträgers an. Standorttyp: Wählen Sie einen Speicherorttyp für Profildatenträger (SMB-Speicherort oder Cloud Cache) und geben Sie dann einen oder mehrere Speicherorte an. Speicherort von Profil-Datenträgern: Speicherort(e) von Profil-Datenträgern. Dies sind die Speicherorte

der VHD(X)-Dateien (die Einstellung VHDLocations in der Registry, wie in der FSLogix-Dokumentation angegeben). Benutzerprofil-Datenträgerformat: Wählen Sie entsprechend Ihren Anforderungen zwischen VHD und VHDX. VHDX ist ein neueres Format und hat mehr Funktionen. Zuweisungstyp: Wählen Sie Dynamisch oder Voll. Diese Einstellung wird in Verbindung mit der Einstellung Standardgröße (siehe unten) verwendet, um die Größe eines Profils zu verwalten. Dynamisch bewirkt, dass der Profilcontainer nur den minimalen Speicherplatz auf der Festplatte verwendet, unabhängig von der zugewiesenen Standardgröße. Wenn ein Benutzerprofil mit mehr Daten gefüllt wird, wächst die Datenmenge auf der Festplatte bis zu der angegebenen Standardgröße, überschreitet diese aber nie. Standardgröße: Gibt die Größe der neu erstellten VHD(X) in Megabyte an.

- Erweitert: Auf dieser Registerkarte können Sie erweiterte Registrierungseinstellungen für FSLogix vornehmen. Die Einstellungen sind standardmäßig deaktiviert. Um eine Einstellung zu aktivieren, aktivieren Sie das Kontrollkästchen vor ihrem Namen. In der RAS-Konsole finden Sie eine Beschreibung der Einstellungen. Weitere Informationen zur Konfiguration der FSLogix-Profilcontainer finden Sie unter https://docs.microsoft.com/de-de/fslogix/profile-container-configuration-reference.

3 Wenn Sie die Office-Container verwenden möchten, gehen Sie zu Benutzerprofil > FSLogix – Office-Container.:

- Benutzer und Gruppen: Wie oben.
- Disks: Wie oben.
- Erweitert: Wie oben.

4 Wenn Sie Cloud-Cache konfigurieren möchten, gehen Sie zu Benutzerprofil > FSLogix – Cloud-Cache.Weitere Informationen zur diesen Einstellungen finden Sie unter https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=ccd#fslogix-settings-profile-odfc-cloud-cache-logging.

5 Wenn Sie die Protokollierung konfigurieren möchten, gehen Sie zu Benutzerprofil > FSLogix – Protokollierung.Weitere Informationen zur diesen Einstellungen finden Sie unter https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=ccd#fslogix-settings-profile-odfc-cloud-cache-logging.

Universelles Drucken

Mithilfe der Druckerumleitung können die Benutzer einen Druckauftrag von einer Remote-Anwendung oder Desktop an ihren lokalen Drucker umleiten, wobei es sich um den mit dem Computer des Benutzers verbundenen Drucker oder einen Netzwerkdrucker handeln kann, der über eine IP-Adresse angesteuert wird. Universal Printing vereinfacht das Druckverfahren

und löst die meisten Druckerprobleme, da ein Remoteserver für einen spezifischen lokalen Drucker auf der Clientseite keinen Druckertreiber benötigt. Ein Benutzer kann daher unabhängig davon drucken, welcher Drucker lokal installiert ist, und der RAS-Administrator braucht nicht für jeden Drucker, der mit dem lokalen Netzwerk verbunden ist, einen Druckertreiber zu installieren.

Navigieren Sie zu Site-Einstellungen > Universelles Drucken, um das universelle Drucken zu konfigurieren.

Druckereinstellungen: Umbenennungsmuster

Standardmäßig benennt Parallels Remote Application Server die Drucker nach folgendem Muster um: `%PRINTERNAME% for %USERNAME% by Parallels`. Nehmen wir beispielsweise an, ein Benutzer mit dem Namen Alice hat einen lokalen Drucker mit dem Namen Printer1. Wenn Alice eine Remote-Anwendung oder einen Desktop startet, bekommt ihr Drucker den Namen `Printer1 für Alice über Parallels`.

Sie können das Muster für das Umbenennen von Druckern ändern, indem Sie ein neues Muster in das Eingabefeld Druckerumbenennung / Muster eingeben. Um die vordefinierten Variablen anzuzeigen, die Sie verwenden können, klicken Sie auf die Schaltfläche Variable hinzufügen. Die Variablen sind:

- `%CLIENTNAME%` – der Name des Client-Computers.
- `%PRINTERNAME%` – der Name des Druckers auf der Clientseite.
- `%SESSIONID%` – RAS-Sitzungs-ID.
- `%USERNAME%` – der Name des Benutzers, der mit RAS verbunden ist.
- `<2X Universal Printer>` – Dies ist ein veralteter Modus, der bedeutet, dass nur ein Druckerobjekt in der RDP-Sitzung erstellt wird.

Sie können im Muster für die Druckerumbenennung auch andere Zeichen verwenden. So können Sie beispielsweise das folgende häufig verwendete Muster definieren:

```
Client/%CLIENTNAME%#/%PRINTERNAME%.
```

Mit dem oben aufgezeigten Muster (und der Benutzerin Alice aus dem vorab genannten Beispiel) wird der lokale Drucker `Client/Alice's Computer#/Printer1` benannt.

Sie können auch ein anderes Muster für die Druckerumbenennung für jeden Server in der Liste Server der Site festlegen.

Hinweis: Umgeleitete Drucker sind nur für den Administrator und den Benutzer zugänglich, der den Drucker umgeleitet hat.

Druckereinstellungen: Druckerbindung

Wenn mandantendefinierte Drucker an eine Remotesitzung weitergeleitet werden, dauert es länger und wirkt sich auf die gesamte Sitzungsaufbauzeit aus. Um die Benutzerfreundlichkeit zu verbessern, können Sie die zuvor erstellten Drucker der Benutzer wiederverwenden. Stellen Sie dazu die Option Druckerbindung auf Druckerbindungsoptimierung aktivieren ein.

Treiber

Ein Systemadministrator kann die Liste von Druckertreibern auf der Clientseite steuern, denen erlaubt oder verwehrt wird, die Umleitungsberechtigungen für Universal Printing zu verwenden.

Diese Funktion ermöglicht Folgendes:

- Vermeidung der Überlastung von Server Ressourcen durch unnütze Druckerumleitungen. Da die meisten Benutzer alle lokalen Drucker umleiten (Standardeinstellung) wird eine große Anzahl von umgeleiteten Geräten auf dem Server erstellt, die nicht wirklich benutzt werden. Das gilt hauptsächlich für verschiedene papierlose Druckertreiber wie PDFCreator, Microsoft XPS Writer oder diverse Faxgeräte.
- Vermeidung der Instabilität von Servern bei bestimmten Druckern. Es gibt Drucker, die Instabilität auf dem Server bewirken können (Spoolerdienste) und in weiterer Folge die Druckdienste für alle verbundenen Benutzer unmöglich machen. Es ist sehr wichtig, dass der Administrator die Möglichkeit hat, diese Treiber in die Ablehnungsliste einzufügen, um die Druckdienste funktionsfähig zu halten.

So geben Sie die Druckertreiber im Abschnitt Treiber ein:

1 Wählen Sie in der Dropdownliste Modus aus folgenden Optionen aus, welchen Druckern eine Umleitung gestattet wird:

- Druckerumleitung für jeden Treiber zulassen|: (Standardeinstellung). Bei dieser Option gibt es keine Begrenzung der Arten von Druckertreibern, die ein Drucker verwenden kann, um Umleitungsberechtigungen zu nutzen.
- Druckerumleitung für einen der folgenden Treiber zulassen: Wählen Sie diese Option aus und fügen Sie die „zugelassenen“ Treiber der Liste hinzu. Um einen Treiber hinzuzufügen, klicken Sie auf das Pluszeichen-Symbol und tippen Sie den Treibernamen ein.
- Druckerumleitung für einen der folgenden Treiber nicht zulassen: Dies ist wahrscheinlich die sinnvollste Option im Kontext dieser Funktion. Die Drucker, die die in der Liste festgelegten Druckertreiber verwenden, erhalten keine Umleitungsberechtigungen. Alle anderen Drucker können die Umleitung nutzen.

2 Um einen Druckertreiber aus der Liste zu entfernen, klicken Sie auf das Minussymbol.

Beachten Sie bitte Folgendes:

- Wenn Sie einen Druckertreiber der Liste hinzufügen, geben Sie den *Treibernamen* ein, nicht den Druckernamen.
- Für den Vergleich der Treibernamen wird die Groß- und Kleinschreibung nicht berücksichtigt und es muss eine genaue Übereinstimmung gegeben sein (keine Teile von Namen, keine Platzhalter).
- Die Einstellungen, die Sie auf dieser Registerkarte vornehmen, betreffen die gesamte Site (nicht einen einzelnen Server).

Schriftarten

Schriftarten müssen eingebettet werden, damit ein Dokument bei seiner Ausgabe per Universellem Drucken in den lokalen Spooler des Clients übertragen und anschließend gedruckt werden kann. Stehen dem Client die Schriftarten nicht zur Verfügung, wird das Dokument nicht ordnungsgemäß dargestellt.

Festlegen von nicht einzubettenden Schriftarten: Um eine bestimmte Schriftart von der Einbettung auszuschließen, wählen Sie diese in der Liste aus. Um eine oder mehrere Schriftart(en) hinzuzufügen, klicken Sie auf das Pluszeichen-Symbol.

Schriftarten automatisch installieren: Um einen bestimmten Schriftarttyp auf Servern oder Clients automatisch zu installieren, klicken Sie auf das Pluszeichen-Symbol im Abschnitt Schriftarten automatisch installieren.

Hinweis: Schriftarten auf der Liste für die automatische Installation sind standardmäßig von der Einbettung ausgenommen, weil sie auf den Windows-Clients installiert werden würden und daher nicht eingebettet werden müssen.

Universal Scanning

Durch die Scannerumleitung werden Benutzer, die mit einem Remotedesktop verbunden sind oder auf eine veröffentlichte Anwendung zugreifen, in die Lage versetzt, mit einem Scanner, der an den Clientcomputer angeschlossen ist, einen Scan durchzuführen. Dieses Kapitel beschreibt, wie Sie RAS Universal Scanning-Services konfigurieren und verwenden.

Navigieren Sie zu Site-Einstellungen > Universal Scanning, um das universelle Scannen zu konfigurieren.

Universal Scanning nutzt WIA und TWAIN-Umleitung, damit jede Anwendung zum Scannen Hardware unterschiedlicher Technologien nutzen kann, die am Client-Gerät angeschlossen ist.

Universal Scanning gewährleistet, dass auf dem Server kein bestimmter Scanner-Treiber installiert werden muss.

Hinweis: Die Serverfunktion Desktopdarstellung ist erforderlich, damit WIA- und TWAIN-Scanning im RD-Sitzungshost möglich ist.

Standardmäßig wird der Universal Scanning-Treiber automatisch installiert, wenn der RAS-Farm ein Hostserver hinzugefügt wird und die Agent-Software darauf installiert ist.

Konfigurieren eines Musters für die Scanning-Umbenennung

Standardmäßig benennt Parallels Remote Application Server die Scanner nach folgendem Muster um: `%SCANNERNAME% für %USERNAME% über RAS`. Wenn beispielsweise eine Benutzerin namens Lois, die den SCANNER1 lokal installiert hat, sich mit einem Remotedesktop oder einer veröffentlichten Anwendung verbindet, wird ihr Scanner in „SCANNER1 für Lois über RAS“ umbenannt.

Wenn Sie das Muster für das Umbenennen von Druckern ändern möchten, geben Sie ein neues Muster in das Eingabefeld Scanner-Umbenennung / Muster ein. Für die Umbenennung können Sie folgende Variablen verwenden:

- `%SCANNERNAME%` – clientseitiger Scannername.
- `%USERNAME%` – Benutzername des mit dem Server verbundenen Benutzers.
- `%SESSIONID%` – ID der aktiven Sitzung.

Sie können ein anderes Muster für die Umbenennung spezifisch für jeden Server in der Liste festlegen.

Hinweis: Umgeleitete Scanner sind nur für den Administrator und den Benutzer zugänglich, der den Drucker umgeleitet.

Hinzufügen einer Scan-Anwendung

TWAIN-Anwendungen, die die Universal Scanning-Funktion verwenden, müssen der TWAIN-Konfiguration hinzugefügt werden. Auf diese Weise verwenden Sie den TWAIN-Treiber, damit wird das Einrichten für den Administrator vereinfacht.

So fügen Sie eine Anwendung der Liste der Scan-Anwendungen hinzu:

1. Wählen Sie die Kategorie TWAIN aus.
2. Klicken Sie im rechten Fensterbereich auf das Pluszeichen-Symbol und tippen Sie den Namen der ausführbaren Anwendung ein.

Hinweis: Einige Anwendungen verwenden unter Umständen andere oder mehrere Programmdateien. Achten Sie darauf, dass alle erforderlichen Programmdateien der Liste der Scan-Anwendungen hinzugefügt werden.

Um eine Scan-Anwendung aus der Liste zu entfernen, wählen Sie diese in der Liste aus und klicken auf das Minuszeichen-Symbol.

Hinweis: Wenn Sie eine Anwendung aus der Liste löschen, wird die Installation der Anwendung nicht beeinflusst.

KAPITEL 7

Infrastruktur

In diesem Kapitel

RD-Sitzungshosts 43
Virtual Desktop-Infrastruktur 59
Zertifikate 60
Gateways 67
Connection Brokers 85
Anbieter 91
Standardeinstellungen der Site 92

RD-Sitzungshosts

RD-Sitzungshosts werden verwendet, um auf dem Host veröffentlichte Ressourcen (Anwendungen, Desktops, Dokumente usw.) in einer RAS-Farm zu hosten.

Navigieren Sie zu Infrastruktur > RD-Sitzungshosts, um die RD-Sitzungshosts zu verwalten. Hier sind die bestehenden RD-Sitzungshosts aufgelistet. Evtl. Verwaltungsfunktionen (hinzufügen, entfernen, Ereignisse und Sitzungen anzeigen usw.) können ausgeführt werden, indem Sie die drei Punkte anklicken, oder über das Kontextmenü (durch Rechtsklicken) und in einigen Fällen auch über Aktionssymbole.

RD-Sitzungshost hinzufügen

Um den Benutzern die veröffentlichen Ressourcen verfügbar zu machen, muss auf einem RD-Sitzungshost die Rolle Remotedesktopdienste (RDS) installiert sein.

So fügen Sie einen RD-Sitzungshost zu einer Farm hinzu:

1. Navigieren Sie zu Infrastruktur > RD-Sitzungshosts.
2. Klicken Sie mit der rechten Maustaste auf die Liste und wählen Sie dann Hinzufügen aus (Sie können Hinzufügen auch auswählen, indem Sie auf die drei Punkte oder auf das Pluszeichen-Symbol klicken).
3. Wählen Sie einen Host (oder mehrere Hosts) aus der angezeigten Liste aus oder klicken Sie auf die Schaltfläche AD durchsuchen und suchen Sie dort nach einem Host.

4 Klicken Sie auf Weiter.

5 Spezifizieren Sie auf der nächsten Seite folgende Optionen:

- Firewall-Regeln hinzufügen. Fügen Sie in Windows auf dem Host die Firewall-Regeln hinzu, die Parallels RAS benötigt. Weitere Informationen finden Sie unter Port-Referenz.
- RDS-Rolle installieren. Installieren Sie die RDS-Rolle auf dem Host, wenn Sie nicht bereits installiert ist. Sie sollten diese Option immer auswählen.
- Desktopdarstellung aktivieren. Aktivieren Sie die Funktion „Desktopdarstellung“ in Windows auf dem Host. Diese Option ist nur aktiviert, wenn Sie „RDS-Rolle installieren“ (oben) ausgewählt haben. Diese Option gilt nur für Windows Server 2008 R1/R 2 und Windows 2012 R1/R2, auf denen die Funktion „Desktopdarstellung“ nicht standardmäßig aktiviert ist.
- Den Server bei Bedarf neu starten. Wenn nötig, starten Sie den Host automatisch neu. Sie können den Host auch manuell neu starten.
- Host(s) zum Hostpool hinzufügen. Den Host (oder die Hosts) einem Hostpool hinzufügen. Wählen Sie den gewünschten Hostpool in der Liste aus, die unter dieser Option angezeigt wird, um einen neuen Hostpool zu erstellen, indem Sie einen Namen eingeben, und dann auf Erstellen klicken. Weitere Informationen dazu, wie Sie einen Hostpool erstellen können, finden Sie unter RDSH-Hostpools (S. 58).

6 Klicken Sie auf Weiter.

7 Damit Endbenutzer auf veröffentlichte Ressourcen auf dem RD-Sitzungshost zugreifen können, müssen sie der Gruppe „Remotedesktopbenutzer“ in Windows auf dem Server hinzugefügt werden. Dies kann auf eine der folgenden Arten geschehen:

- Hinzufügen jedes Benutzers oder jeder Gruppe direkt auf dem Host mit den standardmäßigen Windows-Verwaltungstools.
- Hinzufügen von Benutzern oder Gruppen über Active Directory.
- Verwenden Sie die unten beschriebene Assistentenseite, die zu Ihrer Bequemlichkeit bereitgestellt wird.

Wenn Sie Ihre Benutzer bereits zur Gruppe „Remotedesktopbenutzer“ auf dem angegebenen Host hinzugefügt haben (oder wenn Sie aus irgendeinem Grund eine der anderen oben aufgeführten Methoden verwenden möchten), können Sie einfach auf Weiter klicken und diese Seite überspringen.

Um der Remotedesktop-Benutzergruppe über den Assistenten weitere Benutzer hinzuzufügen, klicken Sie auf Durchsuchen und geben Sie dann einen Benutzer oder eine Benutzergruppe an.

8 Überprüfen Sie die Einstellungen auf der nächsten Seite und klicken Sie auf Erstellen.

9 Wenn auf dem Host kein RAS RD Session Host Agent installiert ist, wird ein Dialogfeld angezeigt, in das Sie die Zugangsdaten für die Remote-Installation eingeben können. Geben Sie einen Benutzernamen und ein Passwort ein, die verwendet werden können, um die Agent-Software auf dem Host zu installieren. Klicken Sie auf Absenden und folgen Sie den Anweisungen auf dem Bildschirm.

10 Klicken Sie auf Fertig, wenn die Installation abgeschlossen ist. Hinweis: Wenn der Agent nicht installiert werden kann, können Sie der Farm trotzdem einen Host hinzufügen, Sie können diesen jedoch nicht verwenden. Sie können den Agent jederzeit zu einem späteren Zeitpunkt installieren.

Nach erfolgreicher Installation wird der Host in der Liste RD-Sitzungshosts aufgeführt.

Zusatzinformationen

Weitere Informationen darüber, wie Sie Ressourcen von einem RD-Sitzungshosts veröffentlichen können, finden Sie unter Veröffentlichung (S. 101).

So konfigurieren und verwalten Sie einen RD-Sitzungshost:

- Konfigurieren eines RD-Sitzungshosts (S. 45)
- Verwalten eines RD-Sitzungshosts (S. 53)

Konfigurieren eines RD-Sitzungshosts

So konfigurieren Sie einen RD-Sitzungshost:

1 Navigieren Sie zu Infrastruktur > RD-Sitzungshosts.

2 Klicken Sie auf einen Host in der Liste. Die Hostinformationen werden angezeigt.

3 In der Navigationsleiste klicken Sie unten auf Eigenschaften. Konfigurieren Sie den RD-Sitzungshost, wie unten beschrieben.

Verwendung von Standardwerten für Sites oder Hostpools

Die Eigenschaften des RD-Sitzungshosts werden in verschiedene Kategorien unterteilt und im mittleren Fensterbereich angezeigt. Jede Kategorie wartet mit eigenen Eigenschaften auf. Alle Kategorien außer Allgemeines und Scanvorgang verwenden einen gemeinsamen Link: Standardeinstellungen der Site oder Hostpool-Standardwerte, über die Sie die Standardeinstellungen abrufen können. Wenn Sie möchten, dass die Eigenschaften einer bestimmten Kategorie die Standardeinstellungen übernehmen, wählen Sie die Option

Standardeinstellungen erben aus. Wenn Sie dies tun, werden die Standardeinstellungen von einem der folgenden Elemente geerbt:

- Hostpool-Standardwerte, wenn der Host einem RD-Sitzungshost-Hostpool zugeordnet ist. Pools sind in Gruppieren und Klonen von RD-Sitzungshost beschrieben.
- Site-Standardwerte, wenn der Host keinem RD-Sitzungshost-Hostpool zugeordnet ist. Beachten Sie, dass ein Hostpool auch Site-Vorgaben erben kann, aber dies kann im Gruppeneigenschaften-Dialogfeld aufgehoben werden, wo Sie benutzerdefinierte Einstellungen für einen Hostpool festlegen können.

Klicken Sie auf den Link Hostpool-Standardwerte oder Standardeinstellungen der Site (je nachdem, was zutrifft), um das Fenster „Hostpool-Standardwerte“ oder „Standardeinstellungen der Site“ zu öffnen. Um die Standardeinstellungen zu ändern (falls erforderlich), klicken Sie auf Bearbeiten.

Allgemein

In der Navigationsleiste wählen Sie Allgemeines aus und geben dann Folgendes an:

- Host der Site aktivieren: Host aktivieren oder deaktivieren. Ein deaktivierter Host kann den Benutzern keine veröffentlichten Ressourcen zur Verfügung stellen. Wenn Sie einen Host deaktivieren, wird sein Name in der Hauptliste ausgegraut.
- Host: Geben Sie den Hostnamen an.
- Beschreibung: Gibt die Hostbeschreibung an.
- Direktadresse ändern: Wählen Sie diese Option, wenn Sie die direkte Adresse ändern müssen, die der Parallels Client benutzt, um eine direkte Verbindung mit dem RD-Sitzungshost herzustellen.

Agent-Einstellungen

Auf jedem RD-Sitzungshost in der Server-Farm ist ein RAS RD Session Host Agent installiert, über den die Kommunikation mit den anderen Parallels RAS-Komponenten abgewickelt wird. Mit der Kategorie Agent-Einstellungen wird der Agent konfiguriert.

Um die Standardeinstellungen zu verwenden, wählen Sie die Option Standardeinstellungen erben. Weiterführende Informationen finden Sie unter Standardwerte für Standorte oder Gruppen verwenden (S. 45). Um benutzerdefinierte Einstellungen für einen bestimmten Host festzulegen, wählen Sie die Option Standardeinstellungen erben ab und legen die Agent-Eigenschaften wie folgt fest:

Verweilen der Anwendungssitzung

Die Einstellungen in diesem Abschnitt gelten nur für Sitzungen, in denen keine Anwendungen laufen.

- Aktive Sitzung trennen nach: Gibt die Zeitdauer an, die jede Sitzung im Hintergrund verbunden bleibt, nachdem der Benutzer eine Remote-Anwendung geschlossen hat. Mit dieser Option können unnötige Verbindungswiederherstellungen mit dem Host vermieden werden.
- Getrennte Sitzung abmelden nach: Mit dieser Einstellung können Sie steuern, wie lange es dauert, bis eine Sitzung abgemeldet ist, nachdem sie als „getrennt“ markiert wurde.

Weitere Einstellungen

- Port. Legt eine andere Portnummer für die Remotedesktopverbindung fest, wenn auf dem Host ein nicht standardmäßiger Port konfiguriert ist.
- Session-Limit. Legt die maximale Anzahl von Sitzungen fest.
- URL-/E-Mail-Weiterleitung an Client erlauben. Wenn ein Benutzer versucht, eine URL oder einen HTML-Mailto-Link in einer Remote-Anwendung zu öffnen, kann der Link auf den Client-Computer umgeleitet und in einer lokalen Standardanwendung (einem Web-Browser oder E-Mail-Client) statt in einer Anwendung auf dem Remote-Host geöffnet werden. Mit dieser Option können Sie die Umleitung aktivieren oder deaktivieren. Sie können aus den folgenden Optionen auswählen:

  a Aktiviert – wählen Sie diese Option, um die Umleitung zu aktivieren, und wählen Sie dann die Option Windows Shell-URL-Namespaceobjekte unterstützen (unter dem Dropdownfeld). Hierbei handelt es sich um die Standkonfiguration der Umleitung, die in den meisten gängigen Szenarien funktioniert. Die Unterstützung von Shell-URL-Namespaceobjekten bedeutet, dass Parallels RAS Aktionen in veröffentlichten Anwendungen abfangen kann, die die Shell-Namespace-API zum Öffnen von Links verwenden, was in den meisten Anwendungen das Standardverhalten ist. Die Möglichkeit, die Unterstützung für Shell-URL-Namespace-Objekte zu deaktivieren, dient der Kompatibilität mit älteren Versionen von Parallels RAS. Sie können diese Option deaktivieren, wenn Sie das Verhalten einer älteren Version von Parallels RAS (RAS v16.2 oder früher) wünschen.

  b Aktiviert (registrierte Anwendung ersetzen) – diese Option verwendet eine alternative Methode der Umleitung eines Links. Hierbei werden auf Remotehost-Seite der Standard-Webbrowser und der Mail-Client durch „Dummy“-Anwendungen ersetzt. Auf diese Weise kann der Versuch, einen Link zu öffnen, abgefangen und auf den Client-Computer umgeleitet werden. Sie können diese Option ausprobieren, wenn die obige Standardoption mit Ihrer veröffentlichten Anwendung nicht funktioniert.

c Deaktiviert – diese Option deaktiviert die URL/E-Mail-Umleitung, sodass URL oder Mailto-Links immer auf dem Remote-Host geöffnet werden.

- Windows Shell-URL-Namespaceobjekte unterstützen:
- Ziehen und ablegen. Hier können Sie festlegen, wie das Ziehen und Ablegen in den Parallels Clients funktioniert. Sie können wählen zwischen „Deaktiviert“ (überhaupt kein Ziehen und Ablegen), „Nur Server zum Client“ (Ziehen und Ablegen zu einer lokalen Anwendung, aber nicht in die entgegengesetzte Richtung), „Nur Client zum Server“ (Ziehen und Ablegen nur zu einer entfernten Anwendung), „Bidirektional“ (Standard). Beachten Sie, dass sich diese Option seit Parallels RAS 17.1 geändert hat. In der Vergangenheit war es ein Kontrollkästchen, mit dem das Ziehen und Ablegen aktiviert oder deaktiviert werden konnte, was im Modus „Nur vom Client zum Server“ funktionierte. Beim Upgrade von einer älteren Version von Parallels RAS und wenn das Kontrollkästchen aktiviert war, ist die Option „Nur Client auf Server“ standardmäßig ausgewählt. Wenn die Option deaktiviert wurde, wird die Option „Deaktiviert“ gesetzt. Sie können sie auf jede der neuen verfügbaren Optionen ändern, wenn Sie es wünschen.

  Hinweis: Bei Redaktionsschluss dieser Dokumentation ist die Ziehen- und Ablegen-Funktion nur in Parallels Client für Windows und Parallels Client für Mac verfügbar.

- Bevorzugter Connection Broker. Wählen Sie einen Connection Broker aus, zu dem der RD-Sitzungshost eine Verbindung herstellen soll. Das ist hilfreich, wenn die Site-Komponenten in mehreren physischen Sites installiert sind, die über WAN miteinander kommunizieren. Sie können den Netzwerkdatenverkehr verringern, indem Sie einen geeigneteren RAS Connection Broker festlegen.
- 2XRemoteExec darf Befehle an den Client senden. Wählen Sie diese Option aus, um es einem auf dem Host laufenden Prozess zu erlauben, den Client anzuweisen, eine Anwendung auf der Clientseite bereitzustellen. Weitere Informationen finden Sie im Unterabschnitt Verwendung von RemoteExec weiter unten.
- RemoteApp verwenden (falls verfügbar). Aktivieren Sie diese Option, damit Remote-Anwendungen für Probleme in Verbindung mit der Shell genutzt werden können, wenn eine Anwendung nicht richtig angezeigt wird. Diese Funktion wird nur auf dem Parallels Client für Windows unterstützt.
- Anwendungsüberwachung aktivieren. Hier können Sie die Überwachung von Anwendungen auf dem Host aktivieren bzw. deaktivieren. Durch die Deaktivierung der Überwachung wird die WMI-Überwachung beendet, um die CPU-Auslastung auf dem Host und die Netzwerk-Auslastung während der Datenübertragung an RAS Connection Broker zu senken. Wenn diese Option aktiviert ist, werden die erfassten Informationen in einem entsprechenden RAS-Bereich angezeigt. Wenn die Option deaktiviert ist, werden die Informationen von diesem Host in keinem Bericht angezeigt.
- RDP-Transportprotokoll verwalten. Wählen Sie das Transportprotokoll aus, das für Verbindungen zwischen Parallels Client und einem Host verwendet werden soll.

- Dateiübertragungsbefehl zulassen (Web und Chrome-Clients): Aktiviert die Dateiübertragung in einer Remotesitzung. Wählen Sie die gewünschte Option aus der Dropdownliste aus. Weitere Details finden Sie unten unter Konfigurieren der Remote-Dateiübertragung.
- Speicherort für die Datenübertragung. Ein UNC-Pfad zu einem Ordner, der als Standard-Upload-Speicherort verwendet werden soll. Dieser Pfad wird auch als Standard-Quellort verwendet, wenn ein Benutzer versucht, eine Datei von einem Remotehost herunterzuladen. Sie können einen der vordefinierten Orte aus der Dropdownliste auswählen oder einen eigenen angeben.
  Standard-Windows-Umgebungsvariablen wie %USERNAME%, %USERDOMAIN%, %USERPROFILE%, können verwendet werden. Wenn der Ort nicht gefunden wird, wird der Standard-Speicherort für Downloads verwendet.
- Ändern des Speicherorts nicht erlauben. Dies verbietet dem Benutzer, den im Feld Ort angegebenen UNC-Pfad zu ändern. Wenn die Option aktiviert ist, kann der Benutzer beim Hoch- oder Herunterladen einer Datei keinen anderen Speicherort auswählen. Wenn die Option deaktiviert ist, kann der Benutzer einen anderen Ort angeben.
- Cache für Laufwerksumleitung aktivieren. Verbessert die Benutzererfahrung, indem das Durchsuchen von Dateien und die Navigation auf umgeleiteten Laufwerken deutlich schneller wird.

Verwenden von 2XRemoteExec

2XRemoteExec ist eine Funktion, die den Hosts die Möglichkeit gibt, Befehle an den Client zu senden. Dies erfolgt mithilfe des Befehlszeilendienstprogramms `2XRemoteExec.exe`. Die Optionen für die Befehlseingabe umfassen:

Parameter der Befehlseingabe	Beschreibung des Parameters
`-s`	Damit wird der 2XRemoteExec-Befehl im dialogfreien Modus ausgeführt. Ohne diesen Parameter zeigt der Befehl Meldungen aus der Anwendung an. Wenn Sie den Parameter setzen, werden die Meldungen nicht angezeigt.
`-t`	Dieser Parameter wird verwendet, um das Zeitlimit für den Start der Anwendung festzulegen. Das Zeitlimit muss ein Wert von 5000 ms bis 30.000 ms sein. Beachten Sie, dass der eingetragene Wert in Millisekunden gilt. Wenn das Zeitlimit abgelaufen ist, wird vom Befehl eine Fehlermeldung zurückgegeben. Beachten Sie, dass die Anwendung auf dem Client trotzdem gestartet sein kann.
`-?`	Zeigt eine Liste der Parameter, die von 2XRemoteExec verwendet werden, mit Hilfeanleitungen an.
`„Pfad zur Remote-Anwendung“`	Die Anwendung, die auf dem Client gemäß Anweisung vom Host gestartet wird.

Beispiele für 2XRemoteExec:

Der folgende Befehl zeigt ein Meldungsfeld an, in dem die verfügbaren Parameter beschrieben werden.

```
2XRemoteExec -?
```

Mit diesem Befehl wird der Windows-Editor auf dem Client ausgeführt.

```
2XRemoteExec C:\Windows\System32\Notepad.exe
```

In diesem Beispiel öffnet der Befehl die Datei `C:\readme.txt` im Windows-Editor auf dem Client. Es werden keine Meldungen angezeigt und 2XRemoteExec wartet 6 Sekunden bzw. bis zum Start der Anwendung.

```
2XRemoteExec C:\Windows\System32\Notepad.exe "C:\readme.txt"
```

Konfigurieren der Remote-Dateiübertragung

Parallels RAS bietet Endbenutzern die Möglichkeit, Dateien remote von und zu einem Remotehost zu übertragen.

Hinweis: Bei Redaktionsschluss dieses Handbuchs wurde die Dateiübertragung nur im Parallels Nutzerportal und im Parallels Client für Chrome unterstützt. Hinweis: Die bidirektionale Dateiübertragung wird nur im Parallels Nutzerportal unterstützt.

Um die Remote-Dateiübertragung so flexibel wie möglich zu gestalten, ermöglicht Parallels RAS Ihnen, die Dateiübertragung auf den drei folgenden drei Ebenen zu konfigurieren.

- RD-Sitzungshost; Anbieter oder Remote PC
- Nutzerportal
- Clientrichtlinie

Einstellungen für die Dateiübertragung, die Sie auf jeder Ebene festlegen, gelten in der oben angegebenen Reihenfolge. Wenn Sie die Dateiübertragung beispielsweise auf einem Nutzerportal aktivieren, aber auf einem RD-Sitzungshost deaktivieren, wird die Dateiübertragung für alle Benutzer deaktiviert, die sich über das angegebene Nutzerportal mit dem angegebenen RD-Sitzungshost verbinden. Als weiteres Beispiel können Sie die Dateiübertragung auf einem RD-Sitzungshost aktivieren und dann für eine bestimmte Client-Richtlinie (oder ein Nutzerportal) deaktivieren. Auf diese Weise können Sie steuern, welche Clients die Dateiübertragung verwenden können und welche nicht.

So konfigurieren Sie die Remote-Dateiübertragung:

1 Wählen Sie in der Dropdownliste Dateiübertragungsbefehl zulassen eine der folgenden Optionen aus:

- Deaktiviert: Die Remote-Dateiübertragung ist deaktiviert.
- Client zu Server: Überträgt Dateien nur von Client zu Server.
- Server zu Client: Überträgt Dateien nur von Server zu Client.
- Bidirektional: Überträgt Dateien in beiden Richtungen.

2 Geben Sie im Feld Speicherort für die Datenübertragung einen UNC-Pfad zu einem Ordner an, der als Standard-Upload-Speicherort verwendet werden soll. Dieser Pfad wird auch als Standard-Quellort verwendet, wenn ein Benutzer versucht, eine Datei von einem Remoteserver herunterzuladen. Standard-Windows-Umgebungsvariablen wie %USERNAME%, %USERDOMAIN%, %USERPROFILE%, können verwendet werden. Wenn der Ort nicht gefunden wird, wird der Standard-Speicherort für Downloads verwendet.

3 Die Option Ändern des Standorts nicht erlauben verbietet es dem Benutzer, den im Feld Ort angegebenen UNC-Pfad zu ändern. Wenn die Option aktiviert ist, kann der Benutzer beim Hoch- oder Herunterladen einer Datei keinen anderen Speicherort auswählen. Wenn die Option deaktiviert ist, kann der Benutzer einen anderen Ort angeben.

Wichtig: Bitte beachten Sie, dass die Option Ändern des Standorts nicht erlauben den Benutzer nicht daran hindern kann, direkt auf den angegebenen Remote-Standort zuzugreifen. So kann ein Benutzer beispielsweise versuchen, eine Datei hochzuladen, sich den UNC-Pfad des Standardspeichers (auf den er Zugriff hat) notieren, ihn dann im File Explorer öffnen und in einen beliebigen Ordner seines Profils kopieren. Um ein solches Szenario zu verhindern, müssen Sie zusätzliche Maßnahmen ergreifen, um andere Orte als den hier angegebenen zu kontrollieren.

Benutzerprofil

Wenn Sie Benutzerprofile für den Host basierend auf der FSLogix-Technologie konfigurieren möchten, wählen Sie bitte in der Technologie-Dropdownliste FSLogix aus und geben Sie die entsprechenden Einstellungen an. Eine vollständige Beschreibung der Konfiguration von FSLogix-Profilcontainern in Parallels RAS finden Sie unter FSLogix-Profilcontainer (S. 32).

Desktopzugriff

Die Kategorie Desktopzugriff ermöglicht es Ihnen, den Remotedesktopzugriff auf bestimmte Benutzer zu beschränken.

Um die Standardeinstellungen zu verwenden, wählen Sie die Option Standardeinstellungen erben. Siehe Unterabschnitt Verwenden der Standardeinstellungen oben.

Standardmäßig können alle Benutzer, die Zugriff auf Remote-Anwendungen auf einem RD-Sitzungshost haben, über eine Standard-RDP-Verbindung eine Verbindung mit einem Host

herstellen. Wenn Sie den Remotedesktopzugriff auf bestimmte Benutzer beschränken möchten, gehen Sie wie folgt vor:

1. Wählen Sie die Option Direkten Desktopzugriff auf die folgenden Benutzer beschränken aus. Wenn Sie die Option Standardeinstellungen erben ausgewählt haben, klicken Sie auf den Link Standardwerte bearbeiten, um die Standardkonfiguration anzuzeigen (und sie ggf. zu bearbeiten). Die restlichen Schritte gelten sowohl für das Dialogfeld Hosteigenschaften als auch für das Dialogfeld Standard-Hosteigenschaften.
2. Klicken Sie auf das Pluszeichen-Symbol.
3. Wählen Sie die gewünschten Benutzer aus. Um mehrere Benutzer hinzuzufügen, trennen Sie sie mit einem Semikolon.
4. Klicken Sie auf OK.

Die Benutzer in dieser Liste sind nach wie vor in der Lage, mit Parallels Client auf Remote-Anwendungen zuzugreifen, Remotedesktopzugriff auf diesen Server ist jedoch nicht möglich.

Beachten Sie bitte, dass Mitglieder der Administratorgruppe nach wie vor eine Verbindung mit dem Remotedesktop herstellen können, selbst wenn sie in dieser Liste enthalten sind.

Drucken und scannen

Drucken

In der Kategorie Drucken können Sie das Umbenennungsformat umgeleiteter Drucker konfigurieren. Das Format kann je nach Version und Sprache des verwendeten Hosts variieren.

Um die Standardeinstellungen zu verwenden, wählen Sie die Option Standardeinstellungen erben. Siehe Unterabschnitt Verwenden der Standardeinstellungen oben.

Die Dropdownliste RDP-Druckernamen-Format ermöglicht Ihnen die Auswahl eines Druckernamensformats speziell für den konfigurierten Host.

Wählen Sie die Option Session-Nummer aus Druckername entfernen aus, um die jeweilige Information vom Druckernamen auszuschließen.

Scannen

In der Ansicht Scanvorgang legen Sie fest, welche Imaging-Schnittstellen auf dem/den Host(s) aktiviert werden sollen. Wählen Sie aus: WIA, TWAIN oder beide.

Verwalten eines RD-Sitzungshosts

So führen Sie Verwaltungsaufgaben für RD-Sitzungshosts durch:

1. Navigieren Sie zu Infrastruktur > RD-Sitzungshosts.
2. Klicken Sie auf einen Host, um die Hosteigenschaften anzuzeigen.
3. Verwenden Sie die Navigationsleiste, um zwischen den einzelnen Ansichten hin- und her zu schalten, damit Sie weitere Informationen anzeigen und verschiedene Aktionen durchführen können. Diese Ansichten werden im Folgenden beschrieben.

Überblick

Die Ansicht Überblick zeigt folgende Informationen an:

- Der Abschnitt Informationen zeigt dieselben RD-Sitzungshost-Informationen an, wie diejenigen, die auf der Hauptliste RD-Sitzungshosts angezeigt werden. Hier sind sie aber in einer Ansicht zusammengefasst.
- Im Abschnitt Aktionen werden Aktionen aufgeführt, die Sie auf einem Host ausführen können (siehe unten). Bitte beachten Sie, dass Sie Aktionen auch in der Hauptliste RD-Sitzungshosts durchführen können, indem Sie einen Host auswählen, auf die drei Punkte klicken und eine Option auswählen.

Folgende Aktionen können Sie auf einem RD-Sitzungshost durchführen:

- Alle benachrichtigen: Sendet eine Nachricht an alle Benutzer, die mit dem Host verbunden sind.
- Alle trennen: Trennt alle aktuellen Benutzer vom Host.
- Alle Sitzungen abmelden: Alle aktuellen Sitzungen werden abgemeldet.
- Agent aktualisieren: Aktualisiert den RD Session Host Agent (falls erforderlich).
- Agent deaktivieren: Der Agent wird vorübergehend deaktiviert.

Das Untermenü Steuerung enthält folgende Elemente:

- Anmeldungen aktivieren: Aktiviert Anmeldungen aus Client-Sitzungen, aber nicht von der Konsole aus. Diese Option führt denselben Vorgang aus wie der Befehl `change logon /enable`.
- Anmeldungen deaktivieren: Deaktiviert nachfolgende Anmeldungen aus Client-Sitzungen, aber nicht von der Konsole aus. Aktuell angemeldete Benutzer sind davon nicht betroffen. Diese Option führt denselben Vorgang aus wie der Befehl `change logon /disable`.

- Drain: Deaktiviert Anmeldungen aus neuen Client-Sitzungen, lässt aber erneute Verbindungen mit bestehenden Sitzungen zu. Drain bleibt auch nach dem Neustart erhalten, bis der Administrator die Anmeldungen aktiviert.

  Beachten Sie, dass sich Administratoren, während sich ein Host im Drain-Modus befindet, immer noch an der physischen Konsole anmelden oder sich über die Befehlszeilenoption /admin oder /console für MSTSC aus der Ferne anmelden können. Dies ermöglicht Administratoren die Fernwartung des RDS-Hosts über Tools > Remotedesktop.
- Drain bis Neustart: Deaktiviert Anmeldungen aus neuen Client-Sitzungen, bis der Computer neu gestartet wird, lässt aber erneute Verbindungen mit bestehenden Sitzungen zu. Drain bleibt bis zum Neustart des Hosts aktiv. Diese Option führt denselben Vorgang aus wie der Befehl `change logon /drainuntilrestart`.
- Warten auf Neustart abbrechen (Scheduler): Warten auf Neustart wird abgebrochen.
- Deaktivierten Status abbrechen (Scheduler): Deaktivierter Status wird abgebrochen (Scheduler).
- RDS-Rolle installieren: Erlaubt es Ihnen, die RDS-Rolle auf dem Host zu installieren.
- Neustarten: Host wird neu gestartet.
- Ausschalten: Host wird herunterfahren.

Das Untermenü Protokolldateien enthält folgende Elemente:

- Konfigurieren: Erlaubt es Ihnen, die Protokollierung zu konfigurieren. Weitere Erklärungen zu den einzelnen Protokollierungsstufe finden Sie weiter unten.
- Abrufen: Ruft ein ZIP-Archiv mit den Protokolldateien am angegebenen Speicherort ab.
- Löschen: Damit werden alle bestehenden Protokolle gelöscht.

Folgende Protokollierungsstufen gibt es:

- Standard: Dies ist die Standard-Protokollierungsstufe, die nur die wichtigsten Ereignisse aufzeichnet. Wenn Sie nicht vom Parallels RAS-Support aufgefordert werden, eine der unten beschriebenen Protokollierungsstufen zu verwenden, sollten Sie immer diese verwenden.
- Erweitert: Diese Protokollierung beinhaltet mehr Informationen als die Standardprotokollierung, verlangsamt aber das System aufgrund der zusätzlichen Informationen, die es sammeln muss.
- Verbose: Die Verbose-Protokollierung beinhaltet noch mehr Informationen als die erweiterte Protokollierung und kann Ihr System erheblich verlangsamen.

Zur Vermeidung von Leistungseinbußen sollte die erweiterte und ausführliche Protokollierung nur für einen begrenzten Zeitraum aktiviert werden (genug, um die notwendigen Informationen für die Analyse zu sammeln). Sie können diesen Zeitraum mit der Option Anschließend wieder auf Standard-Ebene zurücksetzen einstellen. Der Standardwert ist 12 Stunden. In Einzelfällen

teilt Ihnen ein Parallels-Supporttechniker mit, ob dieser Zeitraum auf einen anderen Wert eingestellt werden sollte. Nach Ablauf dieser Zeitspanne wird die Protokollierungsstufe wieder auf den Standard zurückgesetzt.

Außerdem gibt es u. A. folgende Elemente:

- Dem Hostpool zuweisen: Weist den Host einem Hostpool zu.
- Aus dem Hostpool entfernen: Entfernt einen Host aus einem Hostpool.
- Aktualisieren: Aktualisiert die Hostinformationen, die auf dem Bildschirm angezeigt werden.
- Standardeinstellungen der Site: Öffnet die Ansicht RDSH-Standardeinstellungen der Site, in der Sie die Standardeinstellungen der Site anzeigen und konfigurieren können.
- Löschen: Löscht diesen Host aus der RAS-Farm.

Aktive Sitzungen (Active Sessions)

Um die aktive Sitzung für einen RD-Sitzungshost anzuzeigen, klicken Sie in der Navigationsleiste auf Aktive Sitzungen. Klicken Sie auf den Benutzernamen in der Liste, um detaillierte Sitzungsinformationen abzurufen. Dadurch wird die Ansicht Sitzungsinformationen geöffnet. Eine detaillierte Beschreibung der Sitzungsmetriken finden Sie unter Sitzungsinformationen (S. 93).

Um eine Aktion für eine Sitzung (oder mehrere Sitzungen) auszuführen, wählen Sie die entsprechende Aktion in der Liste aus und klicken dann auf die drei Punkte. Wählen Sie eines der folgenden Elemente aus:

- Sitzungsinformationen anzeigen: Dadurch wird die Ansicht Sitzungsinformationen geöffnet.
- Nachricht: Sendet eine Nachricht an den Sitzungseigentümer.
- Trennen: Trennt die Sitzung.
- Abmelden: Meldet die Sitzung ab.
- Ressourcen anzeigen: Dadurch wird die Ansicht mit den aktuell laufenden Ressourcen angezeigt.
- Laufende Prozesse anzeigen: Öffnet die Ansicht mit den aktuell laufenden Prozessen.
- Überwachungseinstellungen: Öffnet einen Dialog, in dem Sie Überwachungseinstellungen konfigurieren können, um Werte in Sitzungsmetriken für RD-Sitzungshosts hervorzuheben. In diesem Dialogfeld werden die verfügbaren Metriken aufgelistet, und Sie können für eine bestimmte Metrik die Schwellenwerte „Warnung“ und „Kritisch“ festlegen. Um einen Schwellenwert festzulegen, aktivieren Sie das Kontrollkästchen vor dem Namen einer Metrik und geben die gewünschten Werte an. Während des Betriebs der RAS-Farm wird bei Erreichen eines Schwellenwerts ein Sitzungsmetrikwert wie folgt hervorgehoben: Schwellenwert „Warnung“: orange; Schwellenwert „Kritisch“: rot.

Um die Werte für einen bestimmten Schwellenwert zurückzusetzen wählen Sie diesen aus und wählen dann im Drei-Punkt-Menü Zurücksetzen aus (oder klicken Sie mit der rechten Maustaste auf > Zurücksetzen). Sie können außerdem die Farbcodierung der Schwellenwerte für eine Metrik aktivieren oder deaktivieren. Dazu wählen Sie eine Metrik aus und wählen dann im Drei-Punkt-Menü Aktivieren oder Deaktivieren aus.

- Aktualisieren: Aktualisiert die Liste.
- Exportieren: Exportiert die Informationen in eine CSV-Datei.

Laufende Ressourcen

Um die laufenden Ressourcen für einen RD-Sitzungshosts anzuzeigen, klicken Sie in der Navigationsleiste auf Laufende Ressourcen. Klicken Sie auf den Ressourcennamen, um detaillierte Informationen abzurufen. Es öffnet sich eine Ansicht, in der die grundlegenden Ressourceninformationen (ID, Name, Ziel usw.) und die entsprechenden Sitzungsinformationen angezeigt werden. Detaillierte Informationen zu Sitzungsmetriken finden Sie unter Sitzungsinformationen (S. 93).

Um eine Aktion für eine Ressource auszuführen, wählen Sie die entsprechende Aktion in der Liste aus und klicken dann auf die drei Punkte. Wählen Sie eine der folgenden Optionen aus:

- Nachricht: Sendet eine Nachricht an den Sitzungseigentümer.
- Trennen: Trennt die Sitzung.
- Abmelden: Meldet die Sitzung ab.
- Laufende Prozesse anzeigen: Öffnet die Ansicht mit den aktuell laufenden Prozessen.
- Benutzersitzung anzeigen: Öffnet eine Ansicht mit Informationen über die Sitzung.
- Informationen anzeigen: Öffnet eine Ansicht mit Informationen über die Ressource.
- Überwachungseinstellungen: Siehe Beschreibung in Aktive Sitzungen (Active Sessions) (S. 55).
- Aktualisieren: Aktualisiert die Liste.
- Exportieren: Speichert die Liste in einer CSV-Datei.

Laufende Prozesse

Um die laufenden Prozesse für einen RD-Sitzungshosts anzuzeigen, klicken Sie in der Navigationsleiste auf Laufende Prozesse. Dadurch wird die Ansicht mit den aktuell laufenden Prozessen geöffnet.

Um einen oder mehrere Prozess(e) zu beenden, wählen Sie den/die entsprechenden Prozess(e) in der Liste aus, klicken Sie dann die drei Punkte an und wählen Prozesse beenden. Um die Liste zu aktualisieren, klicken Sie auf Aktualisieren.

Problembehandlung

Wählen Sie in der Navigationsleiste Problembehandlung aus, um Informationen und Aufgaben zur Problembehandlung anzuzeigen.

Die Daten, die in der Ansicht Problembehandlung angezeigt werden, werden aus dem RAS-Verwaltungsportal direkt vom RD-Sitzungshosts abgerufen, nicht vom RAS Connection Broker. Diese Ansicht kann Daten anzeigen, die für die Problembehandlung beim RAS RD Session Host Agent wichtig sind, auch wenn der Agent nicht vom RAS Connection Broker erreicht werden kann oder gerade bei einem anderen RAS Connection Broker registriert ist.

Folgende Daten werden angezeigt:

- Host: Der RD-Sitzungshostname.
- Agent: Agent-Status (z. B. „OK“).
- Version: Agent-Version.
- RDS-Rolle: Gibt an, ob eine RDS-Rolle im RD-Sitzungshosts aktiviert ist oder nicht.
- BS-Typ: Der auf dem Host installierte Betriebssystem-Typ.
- Status: Zeigt eine lange Version des Agent-Status an. Wenn der Agent „OK“ ist, wird dies angezeigt. Wenn es ein Problem gibt, wird in diesem Feld erklärt, welches Problem beim Agent auftritt. Nutzen Sie diese Informationen, um das Problem aus der Welt zu schaffen.

Sie können in der Ansicht Problembehandlung auch folgende Aktionen durchführen:

- Protokolle abrufen: Ruft die Host-Protokolle in einer einzigen ZIP-Datei ab.
- Protokolle konfigurieren: Erlaubt es Ihnen, eine Protokollierungsstufe für Parallels RAS-Komponenten anzugeben. Hinweis: Erweiterte und Verbose-Ebenen sollten nur für die Fehlersuche verwendet werden. Wenn Sie eine dieser Stufen auswählen, können Sie auch den Zeitraum festlegen, nach dem die Protokollstufe wieder auf „Standard“ zurückgesetzt wird.
- Protokolle löschen: Damit werden alle bestehenden Protokolle gelöscht.
- Agent neu starten: Damit wird der RAS RD Session Host Agent neu gestartet.
- Agent deinstallieren: Damit wird der Agent deinstalliert.
- Aktualisieren: Aktualisiert die Agent-Informationen.

RDSH-Gruppen

Wenn Sie Ressourcen in Parallels RAS veröffentlichen, müssen Sie einen oder mehrere Hosts angeben, auf denen sie gehostet werden. Mit Gruppen können Sie mehrere RDHS-Hostpools zusammenfassen und dann die Ressourcen aus dem Hostpool veröffentlichen, anstatt einzelne Server anzugeben.

Zu den wichtigsten Vorteilen einer Verwendung von RD-Sitzungshost-Hostpools gehören folgende:

- Sie vereinfachen die Verwaltung der veröffentlichten Ressourcen und sind in Umgebungen mit mehreren Hosts sehr empfehlenswert.
- Sie ermöglichen Ihnen die Verwendung von RD-Sitzungshosts, die aus einer Vorlage erstellt wurden, unter Verwendung der VDI-Infrastruktur. Mehr dazu später in diesem Abschnitt.

Beachten Sie, dass ein RD-Sitzungshost nur Mitglied eines Hostpools sein kann. Sie können nicht denselben Host mehreren Hostpools hinzufügen.

Einen Hostpool erstellen

So erstellen Sie einen RDSH-Hostpool:

1. Navigieren Sie zu Infrastruktur > RD-Sitzungshosts > Hostpools.
2. Klicken Sie auf die drei Punkte, wählen Sie Neuer Hostpool aus (oder klicken Sie auf das Pluszeichen-Symbol).
3. Tippen Sie einen Hostnamen ein und drücken Sie die Eingabetaste.
4. Klicken Sie auf den neuen Hostpool in der Liste, um den Bildschirm „Hostpool bearbeiten“ aufzurufen.
5. Klicken Sie im mittleren Fensterbereich auf Eigenschaften und konfigurieren Sie den Hostpool. Die Einstellungen hier ähneln denen bei der Einstellung eines einzelnen RD-Sitzungshosts. Siehe Konfigurieren eines RD-Sitzungshosts (S. 45).

Hostpool-Standardwerte verwenden

RD-Sitzungshosts, die einem Hostpool zugeordnet sind, haben verschiedene Einstellungen, die sie von den Hostpool-Standardwerten übernehmen können. Dies macht es einfacher, einen einzigen Satz von Einstellungen für alle Hosts zu konfigurieren, anstatt jeden Host einzeln einrichten zu müssen. Eine Site hat auch ihre eigenen Standardeinstellungen (Standardeinstellungen der Site). Darüber hinaus kann ein RD-Sitzungshost-Hostpool diese Standardwerte der Site erben. Dies gibt Ihnen die folgenden Auswahlmöglichkeiten beim Übernehmen der Standardeinstellungen an einen RD-Sitzungshost:

- Konfigurieren Sie die Standardeinstellungen der Site und lassen Sie den Hostpool diese Einstellungen erben. Die dem Hostpool zugeordneten RD-Sitzungshosts erben daher auch die Standardeinstellungen der Site. Dies ist das Standardszenario für einen neuen Hostpool.
- Konfigurieren Sie die Standardeinstellungen für einen bestimmten Hostpool. Auf diese Weise können Sie mehrere Hostpools einrichten, die jeweils ihre eigenen Hostpool-Standardwerte haben (anders als die Standardeinstellungen der Site). Die Hosts, die einem Hostpool zugeordnet sind, erben daher die Hostpool-Standardwerte.

Virtual Desktop-Infrastruktur

Mit Parallels RAS VDI (Virtual Desktop Infrastructure) können Sie durch Servervirtualisierung die Anzahl der physischen Server verringern, die erforderlich sind, um veröffentlichte Ressourcen zu hosten. Parallels RAS VDI unterstützt zahlreiche Virtualisierungstechnologien, darunter Hypervisor- und Cloud-basierte Plattformen.

Parallels RAS VDI enthält auch die Vorlagenfunktion, mit der Sie eine Vorlage aus einer vorkonfigurierten Gast-VM (virtuelle Maschine) zu erstellen und dann automatisch Hosts daraus zu klonen.

Bitte beachten Sie, dass zum Zeitpunkt der Erstellung dieses Dokuments die VDI-Funktionalität im Parallels RAS-Verwaltungsportal auf die Anzeige bestehender virtueller Desktops, die Neuerstellung von Hosts und die Durchführung von Schaltvorgängen beschränkt ist. Für andere VDI-Aufgaben verwenden Sie bitte die desktopbasierte Parallels RAS-Konsole.

Liste virtueller Desktops

Um die Liste der virtuellen Desktops anzuzeigen, die es in er Farm gibt, navigieren Sie zu Infrastruktur > Virtual Desktops.

Um in der Tabelle Virtual Desktops einzelne Spalten hinzuzufügen oder zu entfernen, klicken Sie auf das Zahnradsymbol und wählen die entsprechenden Spalten aus oder löschen diese.

Um einen Schaltvorgang durchzuführen, wählen Sie einen virtuellen Desktop und dann aus dem Drei-Punkt-Menü eine der folgenden Optionen aus:

- Starten
- Beenden
- Neustart – Der Neustartvorgang (ordnungsgemäß) hat ein Zeitlimit von 10 Minuten. Wenn der Vorgang während dieser Zeit nicht abgeschlossen werden kann, wird der Rücksetzvorgang (erzwungen) verwendet.

- Zurücksetzen
- Anhalten
- Aktualisieren
- Neu erstellen – Weitere Informationen dazu finden Sie weiter unten.

Einen Host neu erstellen

Wenn bei einem auf einer Vorlage basierenden Host ein Problem auftritt und sie unbrauchbar wird, müssen Sie diesen nicht löschen und einen neuen erstellen. Stattdessen können Sie ihn unter Beibehaltung seines Namens und seiner MAC-Adresse neu erstellen (um sicherzustellen, dass die VM die gleiche IP-Adresse vom DHCP-Server erhält). Auf diese Weise werden keine anderen Site-Einstellungen in Mitleidenschaft gezogen, die möglicherweise auf einem beschädigten Host basieren. Ein weiterer Grund für die Neuerstellung eines Hosts besteht darin, die an der Vorlage vorgenommenen Änderungen zu übernehmen (wenn Sie die Wartung verlassen, ohne den Befehl „Neu erstellen“ auszuführen). Beachten Sie, dass die Beibehaltung der MAC-Adresse nur auf ESXi, vCenter, Hyper-v und Hyper-v Failover Cluster unterstützt wird.

Hinweis: Wenn ein Host aus einer RD-Sitzungshost-Vorlage erstellt wurde und bereits einer RD-Sitzungshost-Hostpool zugeordnet war, kann sie nicht neu erstellt werden.

Wenn Sie einen Host neu erstellen:

- Bei dem Verfahren wird eine VM gelöscht und von derselben Vorlage eine neue erstellt.
- Der neue Host verwendet den gleichen Computer-Namen, der auch vorher verwendet wurde.
- Wenn ein Host ausgeführt wird, gehen jedoch alle nicht gespeicherten Daten aus dem Arbeitsspeicher verloren. Aus diesem Grund sollten sämtliche wichtigen Daten auf einem externen Datenträger gespeichert werden.

Siehe auch

Anbieter (S. 91)

Zertifikate

Das Parallels RAS-Verwaltungsportal enthält eine Zertifikatsverwaltungsoberfläche, mit der Sie alle Ihre SSL-Zertifikate an einem Ort verwalten können.

Zertifikate werden auf Site-Ebene verwaltet. Sobald ein Zertifikat der Site hinzugefügt wurde, kann es mit jedem RAS Secure Gateway oder HALB verwendet werden, das ebenfalls auf dieser Site vorhanden ist.

Navigieren Sie zu Infrastruktur > RD-Sitzungshosts, um die Zertifikate zu verwalten. Die Liste Zertifikate zeigt die bestehenden Zertifikate an. Wenn Sie Parallels RAS installieren, wird das selbstsignierte Zertifikat <Standard> automatisch erstellt, sodass Sie mindestens dieses Zertifikat in der Liste sehen. Das Standard-Zertifikat wird auch automatisch allen neuen RAS Secure Gateways und HALB zugewiesen.

In den folgenden Abschnitten werden die Aufgaben der Zertifikatsverwaltung detailliert beschrieben und zusätzliche Informationen und Anweisungen zum Zertifikat werden bereitgestellt.

Erstellen eines selbstsignierten Zertifikats

Um ein selbstsigniertes Zertifikat zu erzeugen, navigieren Sie zu Infrastruktur > Zertifikate. Klicken Sie auf die drei Punkte, wählen Sie Hinzufügen > Selbstsigniertes Zertifikat generieren aus und geben Sie folgende Optionen an:

- Name: Geben Sie einen Namen für dieses Zertifikat ein. Dieses Feld ist ein Pflichtfeld.
- Beschreibung: Eine optionale Beschreibung.
- Verwendung: Geben Sie an, ob das Zertifikat für RAS Secure Gateways oder HALB oder für beides verwendet werden soll. Diese Auswahl ist obligatorisch.
- Schlüsselgröße: Die Schlüsselgröße des Zertifikats in Bits. Hier können Sie aus den vordefinierten Werten wählen. Die Standardeinstellung ist 2048 Bit, die erforderliche Mindestlänge nach den aktuellen Industriestandards.
- Ungültig in: Das Ablaufdatum des Zertifikats.
- Länderkennung: Wählen Sie Ihr Land aus.
- Bundesland/Kanton: Ihr Bundesland oder Kanton.
- Stadt: Name der Stadt.
- Organisation: Der Name Ihrer Organisation.
- Organisationseinheit: Einheit der Organisation.
- E-Mail-Adresse: Ihre E-Mail-Adresse. Dieses Feld ist ein Pflichtfeld.
- Allgemeiner Name: Der Common Name (CN), auch bekannt als der Fully Qualified Domain Name (FQDN). Dieses Feld ist ein Pflichtfeld.

- Alternative Antragstellernamen: Geben Sie einen oder mehrere alternative Antragstellernamen (Subject Alternative Name – SAN) an. Hinweis: Da mobile Parallels Clients das Feld „Alternative Antragstellernamen“ nicht unterstützen, ist es am sichersten, einen allgemeinen festzulegen, den die meisten mobilen Geräte verwenden werden.

Klicken Sie auf Generieren, um das Zertifikat zu generieren. Danach erscheint das Zertifikat in der Liste Zertifikate, wobei in der Spalte Status die Option Selbstsigniert angezeigt wird.

So können Sie Zertifikateigenschaften anzeigen und ändern:

1. In der Ansicht Infrastruktur > Zertifikate klicken Sie auf den Namen des Zertifikats.
2. Rechts in der Ansicht überprüfen Sie im Abschnitt Informationen die Zertifikateigenschaften.
3. Im Abschnitt Aktionen können Sie das Zertifikat aktivieren oder deaktivieren. Siehe auch: Exportieren eines Zertifikats in eine Datei (S. 65). Wenn Sie das Zertifikat löschen möchten, klicken Sie auf Löschen.
4. Klicken Sie im mittleren Fensterbereich auf Eigenschaften, um einige der Zertifikateigenschaften zu ändern.
5. Klicken Sie links oben auf Bearbeiten, um die Einstellungen (falls erforderlich) zu ändern. Sie können den Namen und die Beschreibung des Zertifikats ändern und auch festlegen, ob das Zertifikat für Gateways, HALB oder beides verwendet werden soll.

Generieren einer Zertifikatsignaturanforderung (CSR)

So generieren Sie eine Zertifikatsignaturanforderung (CSR):

1. Navigieren Sie zu Infrastruktur > Zertifikate.
2. Klicken Sie auf die drei Punkte, wählen Sie Hinzufügen > Selbstsigniertes Zertifikat generieren aus und geben Sie erforderlichen Informationen ein. Die Informationen sind genau die gleichen wie diejenigen, wie unter Selbstsigniertes Zertifikat generieren (S. 61) beschrieben.
3. Nachdem Sie die Informationen eingegeben haben, klicken Sie auf Generieren. Die Ansicht „Zertifikat-Informationen“ öffnet sich.
4. Klicken Sie im mittleren Fensterbereich auf Zertifikat anfordern, um die angeforderten Daten anzuzeigen. Kopieren Sie diese Daten in einen Texteditor und speichern Sie die Datei für Ihre Unterlagen. In dieser Ansicht können Sie zu diesem Zeitpunkt auch einen öffentlichen Schlüssel importieren. Sie können die Anforderung jetzt bei einer Zertifizierungsstelle einreichen, den öffentlichen Schlüssel erhalten und ihn importieren, ohne die Ansicht zu schließen, oder Sie können dies später tun.

So übermitteln Sie die Anforderung an eine Zertifizierungsstelle und importieren einen öffentlichen Schlüssel:

1 Falls die Ansicht „Zertifikat anfordern“ geschlossen ist, öffnen Sie diese (klicken Sie in der Hauptliste auf die Anfrage und dann auf Zertifikat anfordern).

2 Kopieren Sie die Anforderung und laden Sie sie auf die Webseite der Zertifizierungsstelle hoch (oder senden Sie sie per E-Mail, in diesem Fall müssen Sie später zu dieser Ansicht zurückkehren).

3 Beziehen Sie die Zertifikatsdatei von der Zertifizierungsstelle.

4 Klicken Sie auf die Schaltfläche Öffentlichen Schlüssel importieren und schließen Sie die Zertifikatsregistrierung ab, indem Sie die Schlüsseldatei und die Zertifikatsdatei angeben.

Let's Encrypt-Zertifikate

Arbeiten mit Let's Encrypt-Zertifikaten

Let’s Encrypt ist eine globale Zertifizierungsstelle (CA). Diese Organisation ist nicht gewinnorientiert und verlangt keine Gebühren für ihre Zertifikate. Jedes Zertifikat ist 90 Tage lang gültig. Mit der RAS-Konsole können Sie Let's Encrypt-Zertifikate ausstellen, automatisch erneuern und widerrufen.

Let's Encrypt-Zertifikat ausstellen

So stellen Sie ein neues Let's Encrypt-Zertifikat aus:

1 Navigieren Sie zu Infrastruktur > Zertifikate.

2 Klicken Sie auf das Symbol [...] und wählen Sie dort die Option Let's Encrypt-Einstellungen aus.

3 Wählen Sie die Option Ich habe die Let's Encrypt EULA gelesen und akzeptiere sie aus.

4 Geben Sie in der Liste E-Mails zum Ablauf die E-Mail-Adressen an, die Benachrichtigungen von Let’s Encrypt erhalten sollen.

5 Alternativ ändern Sie die Zeit, zu der Zertifikate automatisch erneuert werden, im Feld Zertifikate vor Ablauf automatisch erneuern.

6 Navigieren Sie zurück zu Infrastruktur > Zertifikate.

7 Wählen Sie im Menü [...] Hinzufügen > Selbstsigniertes Zertifikat generieren aus und geben Sie folgende Optionen an:

- Name: Name des Zertifikats.
- Beschreibung: Beschreibung des Zertifikats.
- Verwendung: HALB und/oder Secure Gateway.
- Schlüsselgröße: Schlüsselgröße.

- Länderkennung: Länderkennung für Ihr Land.
- Bundesland/Kanton: Name Ihres Bundeslandes oder Ihrer Provinz.
- Stadt: Ihre Stadt.
- Organisation: Name Ihrer Organisation.
- Organisationseinheit: Name Ihrer Organisationseinheit.
- E-Mail-Adresse: E-Mail Adresse Ihrer Organisation.
- Allgemeiner Name: Gültiger Domänenname eines HALB oder Secure Gateways.
- Alternative Namen: Gültige Domänennamen von HALB oder Secure Gateways.

8 Klicken Sie auf Zertifikat ausstellen.

Manuelles Erneuern von Let's Encrypt-Zertifikaten

So erneuern Sie manuell ein Let's Encrypt-Zertifikat:

1 Navigieren Sie zu Infrastruktur > Zertifikate.

2 Wählen Sie das Let's Encrypt-Zertifikat, das Sie erneuern möchten, aus.

3 Wählen Sie Steuerungselement > Erneuern im Drei-Punkt-Menü [...] aus .

Widerrufen von Let's Encrypt-Zertifikaten

So widerrufen Sie ein Let's Encrypt-Zertifikat:

1 Navigieren Sie zu Infrastruktur > Zertifikate.

2 Wählen Sie das Let's Encrypt-Zertifikat, das Sie erneuern möchten, aus.

3 Wählen Sie Steuerungselement > Widerrufen im Drei-Punkt-Menü [...] aus. .

So fordert Parallels RAS Zertifikate von Let's Encrypt an.

Wenn Sie ein neues Let's Encrypt-Zertifikat mit Parallels RAS erstellen, wird folgender Prozess ausgeführt:

1 Der primäre Connection Broker von Parallels RAS, der die Lizenzierungsrolle hostet, stellt die erste Anfrage an den Let's Encrypt-Server, um ein Konto zu erstellen.

2 Die Kontoerstellung wird bestätigt. Parallels RAS erstellt eine CSR und sendet sie an den Let's Encrypt-Server.

3 Es wird eine Liste von Herausforderungen empfangen, und Connection Broker liest das vom Let's Encrypt-Server gesendete HTTP-Token.

4 Secure Gateway oder HALB ruft die Token vom Connection Broker ab.

5 Sobald dies geschehen ist, benachrichtigt Connection Broker den Let's Encrypt-Server.

6 Let's Encrypt startet den Verifizierungsprozess, indem es zum Secure Gateway oder HALB geht und die Verfügbarkeit des Tokens bestätigt.

7 Die Herausforderungen sind abgeschlossen, einschließlich der Bestätigung, dass die Secure Gateways oder HALB auf die genannte Domäne antworten können.

8 Unter der Annahme, dass die Herausforderung erfolgreich abgeschlossen wurde, fordert Parallels RAS ein Zertifikat an.

9 Ein gültiges Zertifikat wird vom Let's Encrypt-Server in den Connection Broker heruntergeladen.

10 Connection Broker verteilt das Zertifikat an die Secure Gateways oder HALB.

Ein Zertifikat aus einer Datei importieren

Um ein Zertifikat aus einer Datei zu importieren, klicken Sie auf die drei Punkte, wählen Sie Hinzufügen> Zertifikat importieren aus und geben Sie folgende Optionen an:

- Name: Geben Sie einen Namen für das Zertifikat ein.
- Beschreibung: Eine optionale Beschreibung.
- Verwendung: Geben Sie an, ob das Zertifikat für RAS Secure Gateways oder HALB oder für beides verwendet werden soll.
- Private Schlüsseldatei: Geben Sie eine Datei an, die den privaten Schlüssel enthält. Klicken Sie auf Durchsuchen, um nach der Datei zu suchen.
- Zertifikatsdatei: Wenn Sie eine private Schlüsseldatei (oben) angeben und eine passende Zertifikatsdatei haben, wird diese automatisch in dieses Feld eingefügt. Andernfalls geben Sie eine Zertifikatsdatei an.

Klicken Sie abschließend auf OK. Das Zertifikat wird jetzt in der Liste angezeigt, wobei in der Spalte Status die Option Importiert angezeigt wird.

Exportieren eines Zertifikats in eine Datei

Um ein Zertifikat in eine Datei zu exportieren, wählen Sie es aus der Liste aus, klicken Sie dann auf die drei Punkte und wählen Sie Zertifikat exportieren.

Sie können das Zertifikat später in einer anderen Farm oder an einer anderen Site importieren, indem Sie auf Zertifikat importieren klicken und die Zertifikatsdatei im Feld Private Schlüsseldatei angeben.

Ein Zertifikat für Gateways und HALB zuweisen

Nachdem Sie ein Zertifikat hinzugefügt haben, können Sie es einem RAS Secure Gateway, HALB oder beiden zuweisen, je nach dem Verwendungstyp, den Sie bei der Erstellung des Zertifikats angegeben haben. Mehr über die Option Nutzung des Zertifikats weiter unten.

Zertifikatnutzung

Die Zertifikatnutzung ist eine Option, die Ihnen zeigt, ob das Zertifikat für RAS Secure Gateways, HALB oder beides verfügbar sein soll. Siehe auch Generieren eines selbstsignierten Zertifikats (S. 61). Wenn Sie später SSL für ein RAS Secure Gateway oder HALB konfigurieren, müssen Sie ein SSL-Zertifikat angeben. Wenn Sie ein Zertifikat auswählen, sind die folgenden Optionen verfügbar, je nachdem, wie die Option Nutzung für ein bestimmtes Zertifikat konfiguriert ist:

- <Alle passenden Nutzungen>: Dies ist die Standardoption, die immer verfügbar ist. Das bedeutet, dass jedes Zertifikat verwendet wird, bei dem die Auswahl für Nutzung mit dem Objekttyp (Gateway oder HALB) übereinstimmt. Wenn Sie z. B. ein Gateway konfigurieren und ein Zertifikat haben, dessen Option Nutzung auf „Gateway“ eingestellt ist, wird dieses verwendet. Wenn bei einem Zertifikat sowohl Gateway- als auch HALB-Nutzungsoptionen ausgewählt wurden, kann es auch mit dem angegebenen Gateway verwendet werden. Dies funktioniert bei HALB auf die gleiche Weise, wenn Sie „Lastvert. für SSL-Arbeitslast“ konfigurieren. Bitte beachten Sie: Wenn Sie diese Option für ein Gateway oder HALB wählen, aber kein einziges passendes Zertifikat existiert, sehen Sie eine Warnung und müssen erst ein Zertifikat erstellen.
- Weitere Elemente in der Dropdownliste Zertifikate sind einzelne Zertifikate, die je nach den Einstellungen für Nutzung des Zertifikats vorhanden sind oder nicht. Wenn Sie z. B. „Lastvert. für SSL-Arbeitslast“ für HALB konfigurieren und ein Zertifikat mit der Option Nutzung auf „HALB“ gesetzt haben, erscheint das Zertifikat in der Dropdownliste. Andererseits werden Zertifikate, bei denen die Nutzung auf „Gateway“ eingestellt ist, nicht aufgelistet.

Wenn Sie z. B. nur ein Zertifikat benötigen, das Sie für alle Ihre Gateways verwenden möchten, müssen Sie ein Zertifikat erstellen und die Option Nutzung auf „Gateways“ setzen. Sie können dann jedes Gateway so konfigurieren, dass es dieses spezielle Zertifikat verwendet, oder Sie können die Standardauswahl <Alle passenden Nutzungen> beibehalten. Im letzteren Fall wird das Zertifikat automatisch von einem Gateway abgerufen. Genau das gleiche Szenario funktioniert auch für HALB.

Gateways

So weisen Sie einem RAS Secure Gateway ein Zertifikat zu:

1. Navigieren Sie zu Infrastruktur > Gateways.
2. Klicken Sie auf ein Gateway in der Liste.
3. Klicken Sie im mittleren Fensterbereich auf Eigenschaften .
4. Wählen Sie die Kategorie SSL/TLS aus.
5. Wählen Sie in der Dropdownliste Zertifikate das von Ihnen erstellte Zertifikat aus.

Beachten Sie, dass Sie auch die Option <Alle passenden Nutzungen> verwenden können. Dann wird jedes Zertifikat verwendet, das die Verwendung auf Gateway oder Gateway und HALB eingestellt hat.

HALB

Beachten Sie, dass zum Zeitpunkt der Erstellung dieses Handbuchs HALB nicht im RAS-Verwaltungsportal verwaltet werden kann. Verwenden Sie bitte die desktopbasierte RAS-Konsole.

Gateways

RAS Secure Gateway transportiert alle Parallels RAS-Daten durch einen Tunnel über einen einzelnen Port. Es bietet auch sichere Verbindungen und ist der Verbindungspunkt des Benutzers mit Parallels RAS.

In einer Einzelmandant-Umgebung müssen Sie mindestens ein RAS Secure Gateway installieren, damit Parallels RAS funktioniert. Sie können einer RAS-Site zusätzliche Gateways hinzufügen, um mehr Benutzer zu unterstützen, Lastausgleichverbindungen herzustellen und Redundanz zu gewährleisten.

Nachstehend wird beschrieben, wie RAS Secure Gateway mit den Verbindungsanforderungen von Benutzern umgeht:

1. RAS Secure Gateway empfängt die Anforderung für eine Benutzerverbindung.
2. Anschließend leitet es die Anforderung an den RAS Connection Broker weiter, bei dem es registriert ist (standardmäßig die Einstellung „Bevorzugter Connection Broker“).
3. Ein RAS Connection Broker führt Lastverteilungsprüfungen und eine Sicherheitsnachschau in Active Directory durch, um die Sicherheitsberechtigungen zu erhalten.
4. Wenn der Benutzer, der eine veröffentlichte Ressource anfordert, ausreichende Zugriffsberechtigungen hat, sendet der RAS Connection Broker eine Antwort an das Gateway zurück und übermittelt damit Details über den RD-Sitzungshost, mit dem sich der Benutzer verbinden kann.

5 Je nach Verbindungsmodus verbindet sich der Client entweder über das Gateway oder trennt die Verbindung vom Gateway und verbindet sich dann direkt mit dem RD-Sitzungshost-Server.

Betriebsmodus von RAS Secure Gateways

Ein RAS Secure Gateway kann in einem der folgenden Modi betrieben werden:

- Normaler Modus: RAS Secure Gateway empfängt Verbindungsanforderungen von Benutzern und prüft über RAS Connection Broker, ob der Benutzer, der die Anforderung gestellt hat, eine Zugriffsberechtigung hat. Gateways, die in diesem Modus arbeiten, können eine größere Anzahl von Anforderungen unterstützen und verbessern die Redundanz.
- Weiterleitungsmodus: RAS Secure Gateway leitet Verbindungsanforderungen von Benutzern an ein vorkonfiguriertes Gateway weiter. Gateways im Weiterleitungsmodus sind sinnvoll, wenn kaskadierende Firewalls benutzt werden, um WAN-Bindungen von LAN-Verbindungen zu trennen und eine Trennung der WAN-Segmente zu ermöglichen, wenn Probleme auftreten und das LAN nicht unterbrochen werden soll.

Hinweis: Zum Konfigurieren des Weiterleitungsmodus muss in einer RAS-Serverfarm mehr als ein RAS Secure Gateway installiert worden sein.

Planung der Hochverfügbarkeit

Wenn Sie RAS Secure Gateways zu einer Site hinzufügen, sollte die N+1-Redundanz konfiguriert werden, um einen unterbrechungsfreien Dienst für Ihre Benutzer zu gewährleisten. Dies ist eine allgemeine Regel, die auch für andere Parallels RAS-Komponenten gilt, wie z. B. Connection Broker oder RD-Sitzungshosts.

Gateway hinzufügen

So fügen Sie ein RAS Secure Gateway hinzu:

1 Navigieren Sie zu Infrastruktur > Secure Gateways.

2 Klicken Sie im rechten Fensterbereich im Drei-Punkt-Menü auf Hinzufügen. Der Assistent Gateway – Neu hinzufügen wird geöffnet.

3 Geben Sie den FQDN oder die IP-Adresse ein oder klicken Sie auf AD durchsuchen, um einen Server aus der Liste auszuwählen. Um die IP-Adresse auf FQDN oder vice versa aufzulösen, klicken Sie auf IP auflösen oder auf Namen auflösen.

4 Klicken Sie auf Weiter.

5 Wählen Sie im Dropdownmenü Modus den Gateway-Modus aus („Normal“ oder „Weiterleitung“).

6 Wenn Sie im vorherigen Schritt den Modus Weiterleitung ausgewählt haben, müssen Sie jetzt in der Dropdownliste Weiterleiten an das Ziel-Gateway auswählen. Sie können auch eine spezifische IP-Adresse aus der Dropdownliste Auf IP auswählen, wenn der Gateway-Server mehr als eine IP-Adresse hat.

7 Geben Sie eine optionale Beschreibung für dieses Gateway ein.

8 Wählen Sie die Option Nutzerportal aktivieren aus, um die Unterstützung für das RAS Nutzerportal zu aktivieren (ein browser-basierter Client, der verwendet werden kann, um sich mit Parallels RAS zu verbinden und veröffentlichte Ressourcen zu starten).

9 Wählen Sie Firewall-Regeln aktivieren, um automatisch die Firewall auf dem Server zu konfigurieren, auf dem das Gateway gehostet wird.

10 Klicken Sie auf Weiter.

11 Überprüfen Sie die Einstellungen und klicken Sie auf Erstellen, um der Website das Gateway hinzuzufügen.

Zusatzinformationen

Hier erfahren Sie, wie Sie ein RAS Secure Gateway hinzufügen können:

- Gateway konfigurieren (S. 69)
- Gateway verwalten (S. 84)

Gateway konfigurieren

Konfiguration eines RAS Secure Gateways:

1 Navigieren Sie zu Infrastruktur > Secure Gateways.

2 Klicken Sie auf ein Gateway in der Liste. Die Gateway-Informationen werden angezeigt.

3 Klicken Sie im mittleren Fensterbereich auf Eigenschaften.

Konfigurieren Sie die Gateway-Eigenschaften, wie in den nachfolgenden Abschnitten beschrieben.

Allgemein

Wählen Sie die Option RAS Secure Gateway in Website aktivieren aus oder deaktivieren Sie diese.

- Host: Wählen Sie, falls erforderlich, einen anderen Host aus.
- Beschreibung: Geben Sie eine optionale Beschreibung ein oder ändern Sie die vorhandene.
- Öffentliche Adresse: Geben Sie eine öffentliche Adresse für den Gateway-Server ein.

Festlegen von IP-Adressen für Clientverbindungen

Geben Sie folgenden IP-Optionen an:

- IP-Version verwenden: Wählen Sie die zu verwendende(n) IP-Version(en) aus. RAS Secure Gateway erkennt sowohl IPv4 als auch IPv6. Standardmäßig wird IPv4 verwendet.
- IP(s): Geben Sie eine oder mehrere durch ein Semikolon getrennte IP-Adressen an, oder klicken Sie auf Auflösen, um die IP-Adresse automatisch aufzulösen. Dies sind die auf dem Gateway-Server verfügbaren Adressen. Um IP-Adressen anzugeben, die für Client-Verbindungen verwendet werden sollen, verwenden Sie den Abschnitt An IP binden (siehe unten).
- An IP binden: In diesem Abschnitt können Sie angeben, an welcher IP-Adresse (oder an welchen Adressen) das Gateway auf Client-Verbindungen lauschen soll. Sie können eine bestimmte Adresse oder Alle verfügbaren Adressen auswählen, wobei in diesem Fall alle im Feld IP(s) angegebenen IP-Adressen verwendet werden.
- Systempuffer entfernen für: Diese Option kann verwendet werden, wenn die Verbindung zwischen dem Gateway und dem Parallels Client eine hohe Latenzzeit hat (wie z. B. das Internet). Diese Option optimiert den Datenverkehr und verbessert die Erfahrung auf der Parallels Client-Seite. Sie können eine oder mehrere bestimmte Adressen, alle verfügbaren Adressen oder keine auswählen. Diese Option verzögert das interne Socket, um die Leistung des externen Sockets anzupassen. Wenn das interne Netzwerk schnell und das externe langsam ist, erkennt RDP den schnellen internen Socket und sendet viele Daten. Das Problem ist, dass diese Daten nicht schnell genug vom Gateway zum Client gesendet werden können, was zu einer schlechten Benutzererfahrung führt. Wenn Sie diese Option aktivieren, wird der Datenaustausch optimiert.

Modus

Ein RAS Secure Gateway kann in einem der folgenden Modi betrieben werden:

- Normaler Modus: RAS Secure Gateway empfängt Verbindungsanforderungen von Benutzern und prüft über RAS Connection Broker, ob der Benutzer, der die Anforderung gestellt hat, eine Zugriffsberechtigung hat. Gateways, die in diesem Modus arbeiten, können eine größere Anzahl von Anforderungen unterstützen und verbessern die Redundanz.
- Weiterleitungsmodus: RAS Secure Gateway leitet Verbindungsanforderungen von Benutzern an ein vorkonfiguriertes Gateway weiter. Gateways im Weiterleitungsmodus sind sinnvoll, wenn kaskadierende Firewalls benutzt werden, um WAN-Bindungen von LAN-Verbindungen zu trennen und eine Trennung der WAN-Segmente zu ermöglichen, wenn Probleme auftreten und das LAN nicht unterbrochen werden soll.

Hinweis: Zum Konfigurieren des Weiterleitungsmodus muss in einer RAS-Serverfarm mehr als ein RAS Secure Gateway installiert worden sein.

Um die Standardeinstellungen der Site zu verwenden, klicken Sie auf die Option Standardeinstellungen erben. Wenn Sie Ihre eigenen Einstellungen festlegen möchten, deaktivieren Sie diese Option.

Einrichten des Normalmodus

Zum Einrichten des Normalmodus wählen Sie in der Dropdownliste Gateway-Modus die Option Normal.

Die Dropdownliste Bevorzugter Connection Broker ermöglicht Ihnen die Angabe eines RAS Connection Broker, mit dem sich das Gateway verbinden soll. Das ist hilfreich, wenn die Site-Komponenten in mehreren physischen Sites installiert sind, die über WAN miteinander kommunizieren. Sie können den Netzwerkdatenverkehr verringern, indem Sie einen geeigneteren RAS Connection Broker festlegen. Damit das Gateway einen Connection Broker automatisch auswählt, wählen Sie die Option Automatisch.

Mit der Option Anforderungen an HTTP-Server weiterleiten können Sie Anforderungen weiterleiten, die nicht zum RAS Secure Gateway gehören (Gateways verarbeiten HTML5-Datenverkehr, Wyse und URL-Schema). Wenn Sie mehrere Server eingeben, trennen Sie sie mit Strichpunkten. Ein HTTP-Server kann mit einer IPv6-Adresse angegeben werden, sofern erforderlich. Beachten Sie, dass ein HTTP-Server die gleiche IP-Version unterstützen muss wie der anfordernde Browser.

Einrichten des Weiterleitungsmodus

Zum Einrichten des Weiterleitungsmodus wählen Sie in der Dropdownliste Gateway-Modus die Option Weiterleitung und geben Sie eine oder mehrere Gateway(s) an. Ein Gateway im Weiterleitungsmodus leitet alle Verbindungsanforderungen von Benutzern an ein vorkonfiguriertes Gateway weiter. Gateways im Weiterleitungsmodus sind sinnvoll, wenn kaskadierende Firewalls benutzt werden, um WAN-Bindungen von LAN-Verbindungen zu trennen und eine Trennung der WAN-Segmente zu ermöglichen, wenn Probleme auftreten und das LAN nicht unterbrochen werden soll.

Netzwerk

Über die Kategorie Netzwerk können die Netzwerkoptionen für RAS Secure Gateway konfiguriert werden.

Um die Standardeinstellungen der Site zu verwenden, klicken Sie auf die Option Standardeinstellungen erben. Wenn Sie Ihre eigenen Einstellungen festlegen möchten, deaktivieren Sie diese Option und legen Folgendes fest:

- RAS Secure Gateway-Port: Standardmäßig wartet das RAS Secure Gateway auf den TCP-Port 80, um den gesamten RAS-Verkehr von Parallels zu tunneln. Um den Port zu ändern, geben Sie einen neuen Port ein.
- RDP-Port: Der RDP-Port 3389 wird für Clients verwendet, die Desktop-Sitzungen mit einfachem Lastausgleich erfordern. Verbindungen mit diesem Port unterstützen KEINE veröffentlichten Ressourcen. Um den RDP-Port an einem Gateway zu ändern, wählen Sie die Option RDP-Port und geben Sie einen neuen Port an. Wenn Sie Ihren eigenen Port einrichten, stellen Sie sicher, dass dieser Port nicht mit der Standardeinstellung für den „Port des RD-Sitzungshosts“ in Konflikt steht.

  Hinweis: Wenn der RDP-Port geändert wurde, müssen die Benutzer die Portnummer an ihre Verbindungszeichenfolge im Remotedesktop-Client anhängen (z. B. [IP-Adresse]:[Port]).

- RAS Secure Gateway-Adresse übertragen: Diese Option kann verwendet werden, um die Übertragung der Gateway-Adresse einzuschalten, sodass Parallels Clients ihre primären Gateways automatisch finden können. Diese Option ist standardmäßig aktiviert.
- RDP-UDP-Tunnelling aktivieren: Wählen Sie diese Option (Standardeinstellung), um UDP-Tunnelling auf Windows-Geräten zu aktivieren. Um UDP-Tunnelling zu deaktivieren, entfernen Sie das Häkchen für die Option.
- Geräte-Manager-Port: Wählen Sie diese Option, um die Verwaltung von Windows-Geräten zu ermöglichen. Diese Option ist standardmäßig aktiviert.
- RDP DOS Attack- Filter aktivieren: Wenn diese Option ausgewählt ist, weist sie Ketten unvollständiger Sitzungen von derselben IP-Adresse zurück. Beispiel: Wenn ein Parallels Client mehrere aufeinanderfolgende Sitzungen beginnt und jede Sitzung darauf wartet, dass der Benutzer Anmeldedaten eingibt, verweigert Parallels RAS weitere Versuche. Diese Option ist standardmäßig aktiviert.

SSL/TLS

Der Datenverkehr zwischen Parallels RAS-Nutzern und einem RAS Secure Gateway kann verschlüsselt werden. In der Kategorie SSL/TLS können Sie Datenverschlüsselungsoptionen konfigurieren.

Um die Standardeinstellungen der Site zu verwenden, klicken Sie auf die Option Standardeinstellungen erben. Wenn Sie Ihre eigenen Einstellungen festlegen möchten, deaktivieren Sie diese Option.

HSTS

Im Abschnitt HSTS können Sie die HTTP Strict Transport Security (HSTS) erzwingen, einen Mechanismus, der einen Webbrowser dazu bringt, mit dem Webserver nur über sichere HTTPS-Verbindungen zu kommunizieren. Wenn HSTS für ein RAS Secure Gateway

durchgesetzt wird, sind alle Webanforderungen an es gezwungen, HTTPS zu verwenden. Das betrifft insbesondere das Nutzerportal, das normalerweise nur HTTPS-Anfragen akzeptiert.

- Strenge HTTP-Transportsicherheit (HSTS) durchsetzen: Aktiviert oder deaktiviert HSTS für das Gateway.
- Max. Alter: Gibt das maximale Alter für HSTS in Monaten an, d. h. die Zeit, in der der Webbrowser nur über HTTPS mit dem Gateway kommunizieren kann. Der Standardwert (und empfohlene) Wert beträgt 12 Monate. Akzeptable Werte sind 4 bis 120 Monate.
- Subdomains einbeziehen: Gibt an, ob Subdomains eingefügt werden sollen (falls anwendbar).
- Vorab laden: Aktiviert oder deaktiviert das Vorab-Laden von HSTS. Dies ist ein Mechanismus, bei dem eine Liste von Hosts, die die Verwendung von SSL/TLS auf ihrer Site erzwingen möchten, in einem Webbrowser fest kodiert wird. Die Liste wird von Google erstellt und von den Browsern Chrome, Firefox, Safari und Edge verwendet. Wenn HSTS Preload verwendet wird, versucht ein Webbrowser nicht, eine Anforderung über HTTP zu senden, sondern verwendet jedes Mal HTTPS. Bitte lesen Sie auch den wichtigen Hinweis unten.

Hinweis: Um HSTS Preload zu verwenden, müssen Sie Ihren Domainnamen für die Aufnahme in die HSTS Preload-Liste von Chrome einreichen. Ihre Domain wird in allen Webbrowsern, die die Liste verwenden, fest kodiert. Wichtig: Die Aufnahme in die Preload-Liste kann nicht ohne weiteres rückgängig gemacht werden. Sie sollten die Aufnahme nur dann beantragen, wenn Sie sicher sind, dass Sie HTTPS für Ihre gesamte Site und alle ihre Subdomains langfristig (in der Regel 1-2 Jahre) unterstützen können.

Beachten Sie auch die folgenden Anforderungen:

- Ihre Site muss über ein gültiges SSL-Zertifikat verfügen.
- Alle Subdomains (falls vorhanden) müssen in Ihrem SSL-Zertifikat enthalten sein. Erwägen Sie, ein Wildcard-Zertifikat zu bestellen.

Verschlüsselung

Standardmäßig wird einem RAS Secure Gateway bei der Installation des Gateways ein selbstsigniertes Zertifikat zugewiesen. Jedem RAS Secure Gateway muss ein Zertifikat zugewiesen werden und das Zertifikat sollte den vertrauenswürdigen Stammzertifizierungsstellen auf der Client-Seite hinzugefügt werden, um Sicherheitswarnungen zu vermeiden.

SSL-Zertifikate werden auf Site-Ebene erstellt. Sobald ein Zertifikat erstellt ist, kann es einem RAS Secure Gateway zugewiesen werden. Informationen zum Erstellen und Verwalten von Zertifikaten finden Sie unter Zertifikate (S. 60).

So konfigurieren Sie die Verschlüsselung:

1. Wählen Sie die Option SSL aktivieren für Port und geben Sie eine Portnummer an (Standardeinstellung ist 443).
2. Wählen Sie in der Dropdownliste Akzeptierte SSL-Versionen aus.
3. Wählen Sie im Feld Verschlüsselungsstärke eine gewünschte Verschlüsselungsstärke aus.
4. Geben Sie im Feld Verschlüsselung die Verschlüsselung an. Eine stärkere Chiffre ermöglicht eine stärkere Verschlüsselung, wodurch mehr Aufwand erforderlich ist, um sie zu knacken.
5. Die Option Verschlüsselungen entsprechend Serverpräferenz verwenden ist standardmäßig aktiviert. Sie können Client-Einstellungen verwenden, indem Sie diese Option deaktivieren.
6. Wählen Sie in der Dropdownliste Zertifikate das gewünschte Zertifikat aus. Die Option <Alle übereinstimmenden Verwendungen> verwendet jedes Zertifikat, das für die Verwendung durch Gateways konfiguriert ist. Wenn Sie ein Zertifikat erstellen, geben Sie die Eigenschaft „Verwendung“ an, in der Sie „Gateway“, „HALB“ oder beides auswählen können. Wenn bei dieser Eigenschaft die Option „Gateway“ ausgewählt ist, kann sie mit einem Gateway verwendet werden. Hinweis: Wenn Sie diese Option wählen, aber kein einziges passendes Zertifikat vorhanden ist, wird eine Warnung angezeigt und Sie zuerst ein Zertifikat erstellen müssen.

Zusatzinformationen

Client- und Server-Konfiguration (S. 74)

Client- und Server-Konfiguration

Verschlüsseln der Parallels Client-Verbindung

Standardmäßig ist die einzige Art Verschlüsselung eine Verbindung zwischen einem Gateway und Backend-Servern. Um eine Verbindung zwischen Parallels Client und einem Gateway zu verschlüsseln, müssen Sie auch die Verbindungseigenschaften auf der Client-Seite konfigurieren. Öffnen Sie dazu in Parallels Client die Verbindungseigenschaften und stellen Sie den Verbindungsmodus auf Gateway SSL ein.

Um die Konfiguration von Parallels Client zu vereinfachen, wird empfohlen, ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters oder einer Unternehmenszertifizierungsstelle (CA) zu verwenden. Wenn ein Zertifikat einer Unternehmenszertifizierungsstelle verwendet wird, erhalten Windows-Clients aus Active Directory ein Stamm- oder Zwischenzertifikat einer Unternehmenszertifizierungsstelle. Client-Geräte auf anderen Plattformen müssen manuell konfiguriert werden. Wenn ein Zertifikat eines Drittanbieters von einer bekannten vertrauenswürdigen Zertifizierungsstelle verwendet

wird, vertraut das Client-Gerät den Aktualisierungen der vertrauenswürdigen Zertifizierungsstelle für die Plattform.

Konfiguration von Parallels Clients

Wenn das Zertifikat selbstsigniert ist oder von einer Unternehmenszertifizierungsstelle ausgestellt wurde, müssen Parallels Clients wie folgt beschrieben konfiguriert werden.

1. Exportieren Sie das Zertifikat im Base-64 kodierten X.509 (.CER)-Format.
2. Öffnen Sie das exportierte Zertifikat in einem Texteditor, wie z. B. Notepad oder WordPad, und kopieren Sie den Inhalt in die Zwischenablage.

Fügen Sie das Zertifikat dann clientseitig der Liste der vertrauenswürdigen Zertifizierungsstellen hinzu und erlauben Sie Parallels Client, sich über SSL mit einem Zertifikat von einer Unternehmenszertifizierungsstelle zu verbinden.

1. Auf der Client-Seite sollte sich im Verzeichnis „C:\Programmdateien\Parallels\Remote Application Server Client\“ eine Datei mit dem Namen `trusted.pem` befinden. Diese Datei enthält Zertifikate bekannter vertrauenswürdiger Stellen.
2. Fügen Sie den Inhalt des exportierten Zertifikats (im Anhang der Liste der anderen Zertifikate) ein.

Sichern von RDP-UDP-Verbindungen

Ein Parallels Client kommuniziert normalerweise mit einem RAS Secure Gateway über eine TCP-Verbindung. Jüngere Windows-Clients verwenden eventuell auch eine UDP-Verbindung, um die WAN-Leistung zu verbessern. Um UDP-Verbindungen mit SSL zu schützen, muss DTLS verwendet werden.

So verwenden Sie DTLS auf einem RAS Secure Gateway:

1. Stellen Sie sicher, dass in der Kategorie SSL/TLS die Option SSL aktivieren für Port ausgewählt ist.
2. Stellen Sie sicher, dass in der Kategorie Netzwerk die Option RDP-UDP-Tunnelling aktivieren ausgewählt ist.

Die Parallels Clients müssen für die Verwendung des Modus SSL-Verbindung konfiguriert sein. Diese Option kann clientseitig unter Verbindungseinstellungen > Verbindungsmodus eingestellt werden.

Nachdem die zuvor genannten Optionen korrekt eingestellt wurden, werden sowohl TCP- als auch UDP-Verbindungen über SSL getunnelt.

SSL-Serverkonfiguration

Bei der Konfiguration von RAS Secure Gateway für die Verwendung von SSL-Verschlüsselung sollten Sie darauf achten, wie der SSL-Server konfiguriert ist, um mögliche Fallen und Sicherheitsprobleme zu vermeiden. Insbesondere sollten die folgenden SSL-Komponenten bewertet werden, um festzustellen, wie gut die Konfiguration ist:

- Das Zertifikat, das gültig und vertrauenswürdig sein soll.
- Das Protokoll, der Schlüsselaustausch und die Verschlüsselung sollten unterstützt werden.

Die Bewertung ist ohne spezifische Kenntnisse über SSL möglicherweise nicht einfach durchzuführen. Aus diesem Grund empfehlen wir Ihnen, den SSL-Server-Test zu verwenden, der in den Qualys SSL Labs erhältlich ist. Dies ist ein kostenloser Online-Dienst, der eine Analyse der Konfiguration eines SSL-Webservers im öffentlichen Internet durchführt. Um den Test auf einem RAS Secure Gateway durchzuführen, müssen Sie es möglicherweise vorübergehend in das öffentliche Internet verschieben.

Der Test ist unter der folgenden URL verfügbar: https://www.ssllabs.com/ssltest/

Sie können ein Papier von Qualys SSL Labs, das die bei der Bewertung verwendete Methodik beschreibt, unter folgender URL lesen:
https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide.

Nutzerportal

Das Parallels-Nutzerportal ist in RAS Secure Gateway integriert. Es erlaubt dem Benutzer, eine Verbindung zu Parallels RAS herzustellen und veröffentlichte Ressourcen über einen Webbrowser zu öffnen.

Hinweis: Um das Nutzerportal zu verwenden, muss SSL auf einem RAS Secure Gateway aktiviert sein. Wenn Sie den Client aktivieren, achten Sie darauf, dass SSL in der Kategorie SLL/TLS oder auf Ihrem Netzwerklastausgleich aktiviert ist. Beachten Sie auch: Die Kategorie Nutzerportal ist nur verfügbar, wenn der Gateway-Modus auf Normal eingestellt ist.

Informationen zur Konfiguration der Nutzerportal-URL und zum Zugriff auf den Client über einen Webbrowser finden Sie im Abschnitt Web (S. 80).

- Um die Standardeinstellungen der Website auf der Registerkarte Nutzerportal zu verwenden, klicken Sie auf die Option Standardeinstellungen erben. Wenn Sie Ihre eigenen Einstellungen festlegen möchten, deaktivieren Sie diese Option.
- Um das RAS-Nutzerportal zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie die Option Nutzerportal aktivieren.

Client

Im Abschnitt Client können Sie Methoden zum Starten von Anwendungen und andere Nutzerportal-Einstellungen festlegen.

- Sitzungen starten mit: Diese Option gibt an, welcher Parallels Client verwendet wird, um eine veröffentlichte Ressource zu öffnen. Dies kann das Nutzerportal oder ein plattformspezifischer Parallels Client sein. Im Vergleich zum Web Client enthält der plattformspezifische Parallels Client eine größere Anzahl an Funktionen und bietet Endanwendern eine bessere allgemeine Benutzererfahrung. Wählen Sie eine der folgenden Optionen:
  - **a** Nur Browser: Benutzer können Remote-Anwendungen und -Desktops nur mit Web Client ausführen. Verwenden Sie diese Option, wenn Sie nicht möchten, dass Ihre Benutzer einen plattformspezifischen Parallels Client installieren.
  - **b** Nur Parallels Client: Benutzer können Remote-Anwendungen und -Desktops nur in Parallels Client ausführen. Wenn sich ein Benutzer über Parallels Web Client mit Parallels RAS verbindet, wird er aufgefordert, den plattformspezifischen Parallels Client zu installieren, bevor er Remote-Anwendungen und -Desktops starten kann. Dem Benutzer wird eine Meldung für den Parallels Client-Download anzeigt. Nachdem der Benutzer Parallels Client installiert hat, kann er immer noch eine Remote-Anwendung oder einen Desktop in Parallels Web Client starten, diese bzw. dieser wird dann aber stattdessen in Parallels Client geöffnet.
  - **c** Parallels Client mit Failback zum Browser: Remote-Anwendungen und Desktops können sowohl in Parallels Client als auch in einem Browser (HTML5) gestartet werden. Parallels Client ist die primäre Methode; Parallels Web Client wird als Backup verwendet, wenn eine veröffentlichte Ressource aus irgendeinem Grund nicht in Parallels Client gestartet werden kann. Der Benutzer wird informiert, wenn Parallels Client nicht verwendet werden kann. Er hat dann stattdessen die Möglichkeit, ihn im Browser zu öffnen.
- Den Benutzern erlauben, eine Startmethode auszuwählen: Wenn diese Option ausgewählt ist, können die Benutzer entscheiden, ob sie Remote-Anwendungen in einem Browser oder in Parallels Client öffnen. Sie können diese Option aktivieren, wenn die Option Sitzung starten mit (oben) auf Parallels Client und Failback zum Browser (d. h. beide Methoden sind erlaubt) gesetzt wurde.
- Öffnen von Anwendungen in einer neuen Registerkarte erlauben: Wenn diese Option ausgewählt ist, können Benutzer Remote-Anwendungen in einer neuen Registerkarte in ihrem Web-Browser öffnen.

Zugriff auf den Lastausgleich

Der Abschnitt Zugriff auf Netzwerklastausgleich ist für Bereitstellungsszenarien vorgesehen, bei denen Frontend-Lastausgleiche von Drittanbietern wie Amazon Web Services (AWS) Elastic

Load Balancers (ELBs) verwendet werden. Es ermöglicht Ihnen, einen alternativen Hostnamen und eine alternative Portnummer zu konfigurieren, die vom Network Load Balancer (NLB) verwendet werden. Dies ist notwendig, um Hostnamen und Ports zu trennen, auf denen TCP- und HTTPS-Kommunikation durchgeführt wird, da der AWS Load Balancer nicht beide spezifischen Protokolle über den gleichen Port unterstützt.

Folgende Optionen stehen zur Verfügung:

- Anderen Hostnamen verwenden: Wählen Sie diese Option und geben Sie einen alternativen Hostnamen an. Wenn der alternative Hostname aktiviert ist, verwenden alle plattformspezifischen Parallels Clients diesen Hostnamen, um sich mit der RAS-Serverfarm oder der Site zu verbinden.
- Anderen Port verwenden: Wählen Sie diese Option und geben Sie eine alternative Portnummer an. Der Port darf nicht von anderen Komponenten der RAS-Serverfarm oder der Site verwendet werden. Um die Portnummer auf den Standardwert zurückzusetzen, klicken Sie auf Standard. Wenn der alternative Port aktiviert ist, verwenden alle plattformspezifischen Parallels Clients diesen Port, um sich mit der RAS-Serverfarm oder der Site zu verbinden. Beachten Sie, dass RDP-Sitzungen im Web Client weiterhin eine Verbindung zum Standard-SSL-Port (443) herstellen.

Hinweis: Bitte beachten Sie, dass die Verwendung eines alternativen Hosts oder Ports in einer mandantenfähigen Umgebung nicht geeignet ist, da der Mandantenmakler RAS Secure Gateways zwischen den Mandanten gemeinsam genutzt werden, was unterschiedliche Konfigurationen erfordern würde.

Darüber hinaus unterstützt der AWS Application Load Balancer (ALB), der den vom Parallels Web Client benötigten HTTP/s-Verkehr verarbeitet, nur bestimmte Cookies, die normalerweise automatisch generiert werden. Wenn ein Load Balancer zum ersten Mal eine Anforderung von einem Client erhält, leitet er die Anforderung an ein Ziel weiter und erzeugt ein Cookie namens `AWSALB`, das Informationen über das ausgewählte Ziel kodiert. Der Load Balancer verschlüsselt dann das Cookie und nimmt es in die Antwort an den Client auf. Wenn Sticky Sessions aktiviert sind, verwendet der Load Balancer das vom Client empfangene Cookie, um den Datenverkehr an das gleiche Ziel weiterzuleiten, vorausgesetzt, das Ziel ist erfolgreich registriert und gilt als gesund. Standardmäßig verwendet Parallels RAS sein eigenes ASP.NET-Cookie mit dem Namen `_SessionId`. In diesem Fall müssen Sie das Cookie jedoch anpassen und das erwähnte AWS-Cookie für Sticky-Sitzungen angeben. Dies kann über das Feld Web-Cookie im Nutzerportal > Unterkategorie Web konfiguriert werden.

Beschränkungen

Der Abschnitt Beschränkungen wird verwendet, um die folgenden Nutzerportal-Funktionen zuzulassen oder einzuschränken:

- Anmeldeformat von Prä-Windows 2000 verwenden: Aktiviert das Legacy-Anmeldeformat (vor Windows 2000).
- Einbettung des Parallels-Nutzerportals in andere Webseiten zulassen: Wenn diese Option ausgewählt ist, kann die Parallels-Nutzerportal-Webseite in andere Webseiten eingebettet werden. Beachten Sie, dass sich daraus ein potenzielles Sicherheitsrisiko durch Clickjacking ergibt.
- Dateiübertragungsbefehl: Aktiviert die Dateiübertragung in einer Remotesitzung. Wählen Sie die gewünschte Option aus der Dropdownliste aus. Weitere Informationen finden Sie unter Konfigurieren der Remote-Dateiübertragung weiter unten.
- Zwischenablage-Umleitung: Wählen Sie eine Zwischenablage-Option aus, die in einer Remotesitzung erlaubt werden soll. Wählen Sie aus: Nur Client zu Server (kopieren und einfügen nur vom Client zum Server), Nur Server zu Client (kopieren und einfügen nur vom Server zum Client), Bidirektional (kopieren und einfügen in beide Richtungen).
- Ursprungsübergreifende Ressourcenfreigabe (CORS) erlauben: Aktiviert ursprungsübergreifende Ressourcenfreigabe (CORS = cross-origin resource sharing): Um CORS zu aktivieren, wählen Sie diese Option aus und geben dann in dem sich öffnenden Dialogfeld eine oder mehrere Domänen an, für die der Zugriff auf Ressourcen erlaubt werden soll. Wenn Sie keine Domänen angeben, wird die Option automatisch deaktiviert. Geben Sie im Feld Browser-Cache-Zeit an, wie lange der Browser des Endbenutzers eine Ressource zwischenspeichern soll.

Konfigurieren der Remote-Dateiübertragung

Parallels RAS bietet Endbenutzern die Möglichkeit, Dateien remote von und zu einem Remoteserver zu übertragen.

Hinweis: Bei Redaktionsschluss dieses Handbuchs wurde die Dateiübertragung nur im Parallels Web Client und im Parallels Client für Chrome unterstützt. Hinweis: Bidirektionale Dateiübertragung wird nur in Parallels Web Client unterstützt.

Um die Remote-Dateiübertragung so flexibel wie möglich zu gestalten, ermöglicht Parallels RAS Ihnen, die Dateiübertragung auf den drei folgenden drei Ebenen zu konfigurieren.

- RD-Sitzungshost; Anbieter oder Remote PC
- Nutzerportal
- Clientrichtlinie

Einstellungen für die Dateiübertragung, die Sie auf jeder Ebene festlegen, gelten in der oben angegebenen Reihenfolge. Wenn Sie die Dateiübertragung beispielsweise auf einem Nutzerportal aktivieren, aber auf einem RD-Sitzungshost deaktivieren, wird die Dateiübertragung für alle Benutzer deaktiviert, die sich über das angegebene Nutzerportal mit dem angegebenen

RD-Sitzungshost verbinden. Als weiteres Beispiel können Sie die Dateiübertragung auf einem RD-Sitzungshost aktivieren und dann für eine bestimmte Client-Richtlinie (oder ein Nutzerportal) deaktivieren. Auf diese Weise können Sie steuern, welche Clients die Dateiübertragung verwenden können und welche nicht.

Um die Remote-Dateiübertragung für ein Nutzerportal zu konfigurieren, wählen Sie eine der folgenden Optionen in der Dropdownliste Dateiübertragungsbefehl aus:

- Deaktiviert: Die Remote-Dateiübertragung ist deaktiviert.
- Client zu Server: Überträgt Dateien nur von Client zu Server.
- Server zu Client: Überträgt Dateien nur von Server zu Client.
- Bidirektional: Überträgt Dateien in beiden Richtungen.

Web

Hinweis: Die Unterkategorie Web ist nur verfügbar, wenn der Gateway-Modus auf normal eingestellt ist.

In der Kategorie Web können Sie Einstellungen vornehmen, die für die Lastverteilung in bestimmten Szenarien erforderlich sind. Hier können Sie eine Umleitungs-URL für Webanforderungen und einen Sitzungs-Cookie-Namen angeben, um die Persistenz zwischen einem Client und einem Server zu erhalten.

Umleitungs-URL

Die ursprüngliche Webanfrage kann das Gateway auf eine der beiden folgenden Arten erreichen:

- Die Anforderung wird über das lokale Netzwerk unter Verwendung der IP-Adresse oder des FQDN direkt an das Gateway gesendet. Zum Beispiel https://192.168.10.10.
- Die Anfrage wird an ein HALB-Gerät gesendet, das dieses und andere Gateways in der Serverfarm ausgleicht. Das HALB-Gerät ist häufig dem Internet zugewandt (d. h. in der DMZ), sodass sein DNS-Name in der ursprünglichen Anforderungs-URL verwendet werden kann. Zum Beispiel: https://ras.msp.com. Das HALB-Gerät verteilt dann die Anforderung an ein Gateway.

Wenn das Gateway die Webanforderung empfängt, nimmt es die in der Kategorie Web angegebene URL und sendet sie zur Weiterleitung an den Webbrowser zurück.

Technisch gesehen können Sie hier eine beliebige URL eingeben, und die ursprüngliche Webanfrage wird auf diese URL umgeleitet. Der Hauptzweck dieses Feldes besteht jedoch

darin, den Endbenutzern einen einfachen Zugang zum Nutzerportal von ihren Webbrowsern aus zu ermöglichen. Funktionsweise:

1. Ein Benutzer gibt den Load Balancer-DNS-Namen in einem Webbrowser ein. Zum Beispiel: https://ras.msp.com.
2. Der Load Balancer empfängt die Anforderung und verteilt sie zur Verarbeitung an das am wenigsten ausgelastete RAS Secure Gateway.
3. Das Gateway empfängt die Original-URL und ersetzt sie durch die im Feld Standard-URL angegebene URL. Siehe folgenden Unterabschnitt Standard-URL-Format.
4. Die ersetzte URL wird dann an den Webbrowser zurückgeschickt, der sie zum Öffnen der Nutzerportal-Anmeldeseite verwendet.

Standard-URL-Format

Das Standard-URL-Format ist das folgende:

```
https://%hostname%/userportal
```

- Die Variable `%hostname%` wird automatisch durch den Namen des Servers ersetzt, der die ursprüngliche Anfrage erhalten hat, in unserem Beispiel der Load Balancer-DNS-Name. Wenn Sie möchten, können Sie die Variable durch einen bestimmten Hostnamen oder eine IP-Adresse (z. B. dieses oder ein anderes Gateway) ersetzen. Zum Beispiel `https://192.168.5.5/userportal`. Wenn Sie dies tun, werden die Webanforderungen immer an den angegebenen Host weitergeleitet und dort wird das Nutzerportal geöffnet. Die Hardcodierung eines Hosts mag nicht sehr praktisch sein, aber Sie können dies dennoch tun.
- Das `Nutzerportal` ist eine Konstante und ist der Pfad zur Nutzerportal-Anmeldeseite.

In unserem Beispiel lautet die resultierende URL, die der Webbrowser für den Zugriff auf das Nutzerportal verwenden wird, wie folgt:

```
https://ras.msp.com/userportal
```

Tatsache ist, dass ein Benutzer von Anfang an einfach die obige URL verwenden könnte, aber dank der Umleitungsfunktion brauchen Benutzer nur den DNS-Namen des Servers (oder den FQDN bzw. die IP-Adresse im lokalen Netzwerk) anstelle der gesamten URL einzugeben.

Öffnen eines bestimmten Nutzerportal-Schemas

„Nutzerportal-Schemas“ ist eine Funktion, mit der Sie das Aussehen des Nutzerportals für verschiedene Benutzergruppen individuell gestalten können.

Die Standard-URL der Webanfrage öffnet das Standardschema. Um ein bestimmtes Schema zu öffnen, fügen Sie den Namen des Schemas am Ende der URL wie folgt hinzu:

```
https://%hostname%/userportal/?theme=<theme-name>
```

wobei `<Schemaname>` der Name eines Schemas ohne Klammern oder Anführungszeichen ist.

Damit Benutzer ein bestimmtes Thema öffnen können, muss die URL, die sie in einem Webbrowser eingeben, den Namen des Themas enthalten, aber in diesem Fall ist das Format so einfach wie das folgende:

```
https://<Servername>/<Schemaname>
```

Wenn Sie unser Load-Balancer-DNS-Namensbeispiel von oben verwenden, kann die URL wie folgt aussehen:

```
https://ras.msp.com/Theme-E1
```

Weitere Informationen finden Sie unter Nutzerportal-Schemaeinstellung > URLs.

Nutzerportal öffnen

Die Schaltfläche Nutzerportal öffnen verwendet die angegebene Gateway-Adresse und öffnet das Nutzerportal auf diesem Gateway in einer neuen Registerkarte. Sie können diese Schaltfläche verwenden, um Ihre Bereitstellung zu testen.

Web-Cookie

Das Feld „Web-Cookie“ wird zur Angabe eines Sitzungs-Cookie-Namens verwendet. Die RAS-HTML5-Sitzungspersistenz wird normalerweise durch die IP-Adresse des Benutzers festgelegt (Quelladressierung). Wenn Sie die Quelladressierung in Ihrer Umgebung nicht verwenden können (z. B. weil Ihre Sicherheitsrichtlinien dies nicht erlauben), können Sie das Sitzungs-Cookie verwenden, um die Persistenz zwischen einem Client und einem Server aufrechtzuerhalten. Dazu müssen Sie einen Load Balancer einrichten, der ein Sitzungs-Cookie für die Persistenz verwenden kann. Der Standard-Cookie-Name ist ASP.NET_SessionId.

Wenn Sie einen Drittanbieter-Lastenausgleich, wie z. B. Amazon Web Services (AWS) verwenden, müssen Sie einen eigenen Cookie-Namen angeben. Im Falle von AWS gilt: Wenn ein Load Balancer zum ersten Mal eine Anforderung von einem Client erhält, leitet er die Anforderung an ein Ziel weiter und erzeugt ein Cookie namens `AWSALB`, das Informationen über das ausgewählte Ziel kodiert. Der Load Balancer verschlüsselt dann das Cookie und nimmt es in die Antwort an den Client auf. Wenn Sticky Sessions aktiviert sind, verwendet der Load Balancer

das vom Client empfangene Cookie, um den Datenverkehr an das gleiche Ziel weiterzuleiten, vorausgesetzt, das Ziel ist erfolgreich registriert und gilt als gesund.

Wyse

Um Anwendungen aus Parallels RAS mit Wyse thinOS auf Thin Clients zu veröffentlichen, wählen Sie die Option Wyse ThinOS-Unterstützung aktivieren auf der Registerkarte Wyse.

Hinweis: Die Kategorie „Wyse“ ist nur verfügbar, wenn der Gateway-Modus auf „normal“ eingestellt ist.

Wenn Sie diese Option aktivieren, fungiert das RAS Secure Gateway als Wyse-Makler. Sie müssen dafür Sorge tragen, dass die DHCP-Option 188 auf Ihrem DHCP-Server auf die IP-Adresse dieses Gateways für Thin-Clients festgelegt ist, die über dieses Gateway hochfahren. Nachdem der DHCP-Server konfiguriert wurde, klicken Sie auf die Schaltfläche Testen, um die DHCP-Servereinstellungen zu prüfen.

Die Option Keine Warnung bei nicht überprüftem Server-Zertifikat kann ausgewählt (aktiviert) werden, wenn ein Wyse-Gerät bei der Verbindung mit einem RAS Secure Gateway eine SSL-Warnung anzeigt, weil der Hostname nicht mit dem Zertifikat übereinstimmt. Wenn die Option ausgewählt ist, sendet das Gateway den Wyse-Clients die folgenden Parameter in der Datei wnos.ini: SecurityPolicy=low TLSCheckCN=no, womit SSL-Prüfungen deaktiviert werden. Beachten Sie, dass die Option nicht erforderlich ist, wenn ein Zertifikat die folgenden Eigenschaften hat:

- Der CNAME ist auf den FQDN des RAS Secure Gateway gesetzt.
- Der SAN ist auf die IP-Adresse des RAS Secure Gateway gesetzt.

Beachten Sie, dass bei Verwendung einer benutzerdefinierten wnos.ini im Ordner "C:\Programme (x86)\Parallels\ApplicationServer\AppData\wnos" auf dem Gateway das Gateway die SSL-Prüfparameter nicht sendet.

Sicherheit

Sie können den Benutzerzugriff auf ein Gateway basierend auf einer MAC-Adresse erlauben oder verweigern. Dies kann über die Registerkarte Sicherheit im Dialogfeld RAS Secure Gateway-Eigenschaften erfolgen.

Um die Standardeinstellungen der Site zu verwenden, klicken Sie auf die Option Standardeinstellungen erben. Wenn Sie Ihre eigenen Einstellungen festlegen möchten, deaktivieren Sie diese Option.

Um eine Liste der zulässigen und nicht zulässigen MAC-Adressen zu konfigurieren, klicken Sie auf die Registerkarte Sicherheit und wählen Sie eine der folgenden Optionen:

- Alle MAC-Adressen zulassen außer. Alle Geräte im Netzwerk dürfen sich mit dem Gateway verbinden, mit Ausnahme derer, die in dieser Liste enthalten sind. Klicken Sie auf Aufgaben > Hinzufügen, um ein Gerät auszuwählen oder eine MAC-Adresse anzugeben.
- Nur folgende MAC-Adressen zulassen. Nur die Geräte mit den in dieser Liste aufgeführten MAC-Adressen dürfen eine Verbindung zum Gateway herstellen. Klicken Sie auf Aufgaben > Hinzufügen, um ein Gerät auszuwählen oder eine MAC-Adresse anzugeben.

Die Filterung der Gateway-MAC-Adressen basiert auf ARP, sodass sich Client und Server im selben Netzwerk befinden müssen, damit die Filterung funktioniert. Sie funktioniert nicht über Netzwerkgrenzen hinaus.

Gateways verwalten

So führen Sie RAS Secure Gateway-Verwaltungsaufgaben durch:

1. Navigieren Sie zu Infrastruktur > Secure Gateways.
2. Von hier aus können Sie entweder ein Gateway auswählen und auf die drei Punkte klicken, um eine Verwaltungsaufgabe durchzuführen. Sie können aber auch auf ein Gateway klicken, um eine Ansicht zu öffnen, die Details zum Gateway angibt. Hier können Sie dieselben Aufgaben durchführen. Diese Aufgaben werden nachstehend beschrieben.

Steuerungselement

Mit dieser Option können Sie das Gateway aktivieren/deaktivieren.

Protokolle

Ein RAS Secure Gateway wird überwacht und es werden Protokolle mit relevanten Informationen erstellt. Um die Protokollierung zu konfigurieren, klicken Sie auf eine der folgenden Optionen:

- Konfigurieren: Erlaubt es Ihnen, die Protokollierung zu konfigurieren. Weitere Erklärungen zu den einzelnen Protokollierungsstufe finden Sie weiter unten.
- Abrufen: Ruft ein ZIP-Archiv mit den Protokolldateien am angegebenen Speicherort ab.
- Löschen: Damit werden alle bestehenden Protokolle gelöscht.

Folgende Protokollierungsstufen gibt es:

- Standard: Dies ist die Standard-Protokollierungsstufe, die nur die wichtigsten Ereignisse aufzeichnet. Wenn Sie nicht vom Parallels RAS-Support aufgefordert werden, eine der unten beschriebenen Protokollierungsstufen zu verwenden, sollten Sie immer diese verwenden.

- Erweitert: Diese Protokollierung beinhaltet mehr Informationen als die Standardprotokollierung, verlangsamt aber das System aufgrund der zusätzlichen Informationen, die es sammeln muss.
- Verbose: Die Verbose-Protokollierung beinhaltet noch mehr Informationen als die erweiterte Protokollierung und kann Ihr System erheblich verlangsamen.

Zur Vermeidung von Leistungseinbußen sollte die erweiterte und ausführliche Protokollierung nur für einen begrenzten Zeitraum aktiviert werden (genug, um die notwendigen Informationen für die Analyse zu sammeln). Sie können diesen Zeitraum mit der Option Anschließend wieder auf Standard-Ebene zurücksetzen einstellen. Der Standardwert ist 12 Stunden. In Einzelfällen teilt Ihnen ein Parallels-Supporttechniker mit, ob dieser Zeitraum auf einen anderen Wert eingestellt werden sollte. Nach Ablauf dieser Zeitspanne wird die Protokollierungsstufe wieder auf den Standard zurückgesetzt.

Weitere Aktionen

- Aktualisieren: Aktualisiert die angezeigten Gateway-Informationen.
- Standardeinstellungen der Site: Öffnet die Ansicht „Standardeinstellungen der Site“.
- Löschen: Entfernt das Gateway aus der Farm.

Connection Brokers

RAS Connection Broker bietet den Lastausgleich von veröffentlichten Anwendungen und Desktops. Ein RAS Connection Broker wird automatisch auf einem Server installiert, auf dem Sie Parallels RAS installieren, und wird als primärer Connection Broker festgelegt. Jede Site muss über einen primären RAS Connection Broker verfügen, kann aber auch über sekundäre Connection Broker verfügen. Der Zweck eines sekundären Connection Broker ist es, sicherzustellen, dass die Benutzer keine Unterbrechung des Dienstes aufgrund eines möglichen Ausfalls des primären RAS Connection Broker erleben.

Konfigurieren eines RAS Connection Brokers

Um die auf einer Site installierten RAS Connection Broker anzuzeigen, navigieren Sie in der RAS-Konsole zu Infrastruktur > Connection Broker.

Auf einer Site muss mindestens der primäre Connection Broker installiert sein. Dieser wird in der Spalte Priorität als solcher gekennzeichnet. Außerdem können Sie auch sekundäre Agents als Redundanz hinzufügen (S. 87).

Um die Konfiguration eines Connection Brokers zu ändern, klicken Sie in der Liste darauf und dann im mittleren Fensterbereich auf Eigenschaften. Klicken Sie auf Bearbeiten und geben Sie folgende Optionen an:

- Aktivieren: Der Connection Broker kann damit aktiviert oder deaktiviert werden.
- IP: Hier wird die IP-Adresse des Servers angegeben.
- Alternative IPs: Hier werden alternative IP-Adressen angegeben, die durch ein Semikolon voneinander getrennt werden. Diese Adresse wird verwendet, wenn RAS Secure Gateways mit der im Feld IP angegebenen Adresse keine Verbindung zum RAS Connection Broker herstellen können. Dies kann passieren, wenn beispielsweise Gateways aus einem Netzwerk, das dem Active Directory nicht hinzugefügt wurde, versuchen, eine Verbindung herzustellen.
- Standby: Wenn ausgewählt, wird ein sekundärer Connection Broker in den Standby-Modus versetzt. Das bedeutet, dass sich Agents mit diesem Connection Broker erst verbinden, wenn ein anderer Connection Broker offline geht. Diese Option wird automatisch für jeden neuen sekundären Connection Broker aktiviert, der zusätzlich zu den drei bereits vorhandenen Agents eingerichtet wird. Es wird nicht empfohlen, mehr als drei aktive Connection Broker zu haben, da dies die Systemleistung beeinträchtigen kann. Mit dieser Option können Sie mehr als drei Agents haben, die sich jedoch im Standby-Modus befinden, bis sie benötigt werden. Weitere Informationen finden Sie unter Sekundäre Connection Broker hinzufügen (S. 87.

Wenn Sie die Änderungen vorgenommen haben, klicken Sie auf Speichern und dann auf Alle Änderungen übernehmen.

Das Drei-Punkt-Menü in der Hauptansicht Connection Brokers weist folgende Elemente auf:

- Hinzufügen: Fügt der Site einen RAS Connection Broker hinzu. Im folgenden Abschnitt finden Sie Informationen zum Hinzufügen von sekundären Connection Broker.
- Agent aktualisieren: Agent wird aktualisiert.
- Agent aktivieren/deaktivieren: Aktiviert oder deaktiviert den Agent.
- Protokolle: Darüber können Sie die Protokollierung verwalten.
- Auf primär hochstufen: Stuft einen sekundären Connection Broker auf primär hoch.
- Priorität hochstufen: Erhöht die Priorität eines sekundären Connection Brokers (verschiebt ihn in der Prioritätsliste nach oben).
- Priorität herabstufen: Vermindert die Priorität eines sekundären Connection Broker (verschiebt ihn in der Prioritätsliste nach unten).
- Aktualisieren. Aktualisiert die Liste Connection Broker.

- Löschen. Löscht einen sekundären Connection Broker von der Site. Um den aktuellen primären Connection Broker löschen zu können, müssen Sie zuerst einen sekundären Connection Broker zu einem primären machen.

Zusatzinformationen

- Sekundären Connection Broker hinzufügen (S. 87)
- RAS Connection Broker verwalten (S. 90)

Sekundären Connection Broker hinzufügen

Ein sekundärer Connection Broker wird zu einer Site hinzugefügt, um Redundanz zu gewährleisten. Wenn der primäre Connection Broker ausfällt, steht der sekundäre Connection Broker weiterhin zur Verfügung, um die Anforderungen zu bearbeiten. Connection Broker arbeiten aktiv/aktiv, um eine hohe Verfügbarkeit zu gewährleisten. Bei einem Ausfall des Connection Broker ist der nächste Agent immer bereit, die Last zu verarbeiten. Im Allgemeinen sollte der N+1-Redundanzansatz pro Site angewendet werden. Beachten Sie, dass Sie für die automatische Hochstufung nicht mehr als drei Connection Broker haben sollten (die automatische Verbindungsherstellung wird später in diesem Abschnitt beschrieben).

Wenn Sie einen weiteren sekundären Connection Broker installiert haben, werden die Laufzeitdaten auf jeden Agent repliziert. Wenn also ein Dienst ausfällt, wird die Ausfallzeit auf ein Minimum reduziert. Darüber hinaus wird jeder aktive Connection Broker für Authentifizierungszwecke sowohl mit dem AD als auch mit jedem verwendeten Second-Level-Authentifizierungsanbieter verwendet.

Der primäre Connection Broker führt dieselben Aufgaben wie der sekundäre Connection Broker aus, hat aber zusätzliche Verantwortlichkeiten. Es verwaltet bestimmte Prozesse, die von einem einzigen Connection Broker verwaltet werden müssen. In der folgenden Tabelle sind die vom primären Connection Broker und vom sekundären Connection Broker verwalteten Prozesse aufgeführt:

Prozess	Primäre Connection Broker	Sekundäre Connection Broker
PAs überwachen (Zähler)	Ja	Ja
RD-Sitzungshosts überwachen (Zähler)	Ja	Ja
Anbieter überwachen (Zähler)	Ja	Ja
RDS-Sitzungen überwachen (Neuverbindung)	Ja	Ja
Bereitgestellte RDS-Anwendungen	Ja	Ja

überwachen		
VDI-Sitzung überwachen (Verbindungswiederherstellung)	Ja	Ja
Systemeinstellungen verwalten	Ja	Nein
Lizenzinformationen und Taktfrequenz senden	Ja	Nein
CEP-Informationen verarbeiten und versenden	Ja	Nein
Informationen an den Reporting Server senden	Ja	Nein
RDS-Aufgabenplan verwalten	Ja	Nein
Reporting-Engine-Informationen	Ja	Zukünftige Versionen
Shadowing	Ja	Zukünftige Versionen
E-Mail-Benachrichtigungen senden	Ja	Nein

Im folgenden Beispiel wird gezeigt, wie die Lastverteilung auf mehrere Connection Broker funktioniert:

- Angenommen, es sind zwei Connection Broker vorhanden: PA1 (primär) und PA2 (sekundär).
- Angenommen, es sind 10 RD-Sitzungshosts vorhanden: RDS1, RDS2 ... RDS10

Die sich daraus ergebende Last wird wie folgt verteilt:

- RDS1–RDS5 verwendet PA1 als bevorzugten Connection Broker.
- RDS6–RDS10 verwendet PA2 als bevorzugten Connection Broker.

Planung für sekundäre Connection Broker

RAS Connection Broker an derselben Site kommunizieren miteinander und teilen sich die Last. Da von einem Agent zum anderen große Datenmengen übertragen werden, muss ein zuverlässiger Highspeed-Kommunikationskanal gewährleistet sein (beispielsweise kann für die Kommunikation der Connection Broker ein Subnetzwerk konfiguriert werden).

Wenn Sie einer Site einen sekundären Connection Broker hinzufügen, müssen Sie seine IP-Adresse angeben. Stellen Sie sicher, dass die IP-Adressen aller Agents zum gleichen Netzwerksegment gehören. Für ihre Kommunikation untereinander verwenden Connection Broker Port TCP 20030.

Es gibt keine physische Beschränkung im Hinblick auf die Anzahl der Connection Broker, die Sie einer Site hinzufügen können. Die besten Ergebnisse werden jedoch mit nur zwei bis drei Agents erzielt. Das Drei-Agent-Szenario ist sehr empfehlenswert, insbesondere wenn Sie Anbieter haben und eine hohe Verfügbarkeit für VDI ermöglichen wollen. Wenn Sie einer Site mehr als zwei sekundäre Connection Broker hinzufügen, kann dies die entgegengesetzte Wirkung haben und die Systemleistung sogar verschlechtern. Beachten Sie, dass dies nicht für sekundäre Connection Broker im Standby-Modus gilt, was unter Konfigurieren von RAS Connection Broker beschrieben ist.

Hinzufügen eines sekundären RAS Connection Broker zu einer Site

So fügen Sie einen sekundären Connection Broker hinzu:

1. Navigieren Sie zu Infrastruktur > Connection Brokers.
2. Wählen Sie im Drei-Punkt-Menü Hinzufügen aus (oder klicken Sie auf das Pluszeichen-Symbol). Der Assistent Neu hinzufügen wird geöffnet.
3. Geben Sie auf der Seite Host die folgenden Optionen an:
   - Hostname: FDQN des Hosts, auf dem der sekundäre Connection Broker gehostet wird. Klicken Sie auf IP-Adresse auflösen, um die IP-Adresse des Hosts automatisch zu erhalten.
   - IP-Adresse: Die Host-IP-Adresse: Klicken Sie auf Name auflösen, um die FQDN des Hosts automatisch zu erhalten.
4. Geben Sie auf der Seite Agent-Einstellungen die folgenden Optionen an:
   - Alternative IPs: Hier werden alternative IP-Adressen angegeben, die durch ein Semikolon voneinander getrennt werden. Diese Adressen werden verwendet, wenn RAS Secure Gateways sich mit RAS Connection Broker nicht über dessen FQDN oder die auf der vorherigen Seite angegebene Adresse verbinden können. Dies kann passieren, wenn beispielsweise Gateways aus einem anderen Netzwerk, das dem Active Directory nicht hinzugefügt wurde, versuchen, eine Verbindung herzustellen.
   - Beschreibung: Hier können Sie optional eine Beschreibung hinzufügen.
   - Firewall-Regeln aktivieren: Wählen Sie diese Option, um automatisch die Firewall auf dem Host zu konfigurieren.
   - Host neu starten, falls erforderlich: Dadurch wird der Host automatisch nach der Installation neu gestartet, falls diese erforderlich ist.
   - Gateway mit Connection Broker installieren: Wählen Sie diese Option, wenn Sie auch auf dem angegebenen Host ein RAS Secure Gateway installieren möchten. Wenn Sie diese Option auswählen, können Sie auch die Option HTML5-Gateway aktivieren auswählen, um das Nutzerportal automatisch auf dem Gateway zu aktivieren.

5 Überprüfen Sie die Einstellungen auf der Seite Zusammenfassung und klicken Sie dann auf Erstellen.

Folgen Sie jetzt den Anweisungen auf dem Bildschirm, um der Farm den Connection Broker hinzuzufügen.

Weitere Informationen:

RAS Connection Broker verwalten (S. 90)

RAS Connection Broker verwalten

So führen Sie RAS Connection Broker-Verwaltungsaufgaben durch:

1 Navigieren Sie zu Infrastruktur > Connection Brokers.

2 Wählen Sie einen Connection Broker auf der Liste aus und klicken Sie dann auf das Drei-Punkt-Menü.

3 Im Menü wählen Sie eine der unten beschriebenen Optionen aus.

Neu

Siehe Sekundären Connection Broker hinzufügen.

Agent aktualisieren, Agent aktivieren/deaktivieren

Connection Broker aktualisieren, aktivieren oder deaktivieren.

Protokolle

Um die Protokollierung zu konfigurieren, wählen Sie eine der folgenden Optionen aus:

- Konfigurieren: Erlaubt es Ihnen, die Protokollierung zu konfigurieren. Weitere Erklärungen zu den einzelnen Protokollierungsstufe finden Sie weiter unten.
- Abrufen: Ruft ein ZIP-Archiv mit den Protokolldateien am angegebenen Speicherort ab.
- Löschen: Damit werden alle bestehenden Protokolle gelöscht.

Folgende Protokollierungsstufen gibt es:

- Standard: Dies ist die Standard-Protokollierungsstufe, die nur die wichtigsten Ereignisse aufzeichnet. Wenn Sie nicht vom Parallels RAS-Support aufgefordert werden, eine der unten beschriebenen Protokollierungsstufen zu verwenden, sollten Sie immer diese verwenden.

- Erweitert: Diese Protokollierung beinhaltet mehr Informationen als die Standardprotokollierung, verlangsamt aber das System aufgrund der zusätzlichen Informationen, die es sammeln muss.
- Verbose: Die Verbose-Protokollierung beinhaltet noch mehr Informationen als die erweiterte Protokollierung und kann Ihr System erheblich verlangsamen.

Zur Vermeidung von Leistungseinbußen sollte die erweiterte und ausführliche Protokollierung nur für einen begrenzten Zeitraum aktiviert werden (genug, um die notwendigen Informationen für die Analyse zu sammeln). Sie können diesen Zeitraum mit der Option Anschließend wieder auf Standard-Ebene zurücksetzen einstellen. Der Standardwert ist 12 Stunden. In Einzelfällen teilt Ihnen ein Parallels-Supporttechniker mit, ob dieser Zeitraum auf einen anderen Wert eingestellt werden sollte. Nach Ablauf dieser Zeitspanne wird die Protokollierungsstufe wieder auf den Standard zurückgesetzt.

Auf primär hochstufen

Die Option ist nur für sekundäre Connection Broker aktiviert. Falls der primäre Connection Broker nicht funktioniert und nicht wiederhergestellt werden kann, können Sie einen sekundären Connection Broker zum primären hochstufen:

Priorität hochstufen / Priorität herabstufen

Die Option ist nur für sekundäre Connection Broker aktiviert. Jedem sekundären Connection Broker wird eine Priorität zugewiesen. Um die Priorität zu ändern, wählen Sie Priorität hochstufen oder Priorität herabstufen aus. Der Connection Broker wird dann in der Hauptliste weiter oben oder weiter unten angezeigt. Je höher der Agent in der Liste steht, desto höher ist auch seine Priorität.

Aktualisieren

Aktualisiert die aktuelle Ansicht.

Löschen

Entfernt den Connection Broker aus der Farm.

Anbieter

Anbieter sind Hypervisoren oder Cloud-basierte Virtualisierungslösungen, die zu einer RAS-Farm hinzugefügt werden können, um virtuelle Maschinen als Virtual Desktops zu nutzen.

Bitte beachten Sie, dass zum Zeitpunkt der Erstellung dieses Dokuments die Anbieter-Funktionalität im Parallels RAS-Verwaltungsportal auf die Anzeige verfügbarer Anbieter, Hosts und die Durchführung aktiver Sitzungen beschränkt ist. Für andere Anbieter-Aufgaben verwenden Sie bitte die Desktop-basierte Parallels RAS-Konsole.

Anbieterliste

Um die Liste der Anbieter anzuzeigen navigieren Sie zu Infrastruktur > Anbieter.

Um in der Tabelle Anbieter einzelne Spalten hinzuzufügen oder zu entfernen klicken Sie auf das Zahnradsymbol und wählen die entsprechenden Spalten aus oder löschen diese.

Um eine Aufgabe durchzuführen, wählen Sie einen Anbieter auf der Liste, klicken Sie dann auf die drei Punkte und wählen Sie eine der folgenden Optionen aus:

- Gehostete VDI-Desktops anzeigen: Öffnet die Hostliste (S. 59), auf die ein Filter angewandt wurde, um nur die Hosts anzuzeigen, die diesem Anbieter zugewiesen sind.
- Aktive Sitzungen anzeigen: Öffnet die Sitzungsliste (S. 93), auf die ein Filter angewandt wurde, um nur die Sitzungen anzuzeigen, die diesem Anbieter zugewiesen sind.

Standardeinstellungen der Site

In der Kategorie Standardeinstellungen der Site können Sie Standardeinstellungen für verschiedene RAS-Komponenten und -Dienste konfigurieren. Zum Zeitpunkt der Erstellung dieses Dokuments können Sie folgende Standardeinstellungen für die Site konfigurieren:

- Veröffentlichung – siehe Standardeinstellungen der Site (Veröffentlichung) (S. 112).
- Gateways – siehe Gateway konfigurieren (S. 69).
- RD-Sitzungshosts und Hostpools – siehe Agent-Einstellungen (S. 46).
- Multifaktor-Authentifizierung – siehe Multifaktor-Authentifizierung (S. 25).

Wenn Sie einer RAS-Farm eine Komponente hinzufügen oder wenn Sie eine Ressource veröffentlichen, werden die Standardeinstellungen der Site verwendet, damit Sie die Werte nicht jedes Mal manuell eingeben müssen. Sie können diese Standardeinstellungen aber jederzeit mit Ihren eigenen Werten überschreiben.

Um die Standardeinstellungen der Site anzuzeigen, klicken Sie auf eine beliebige der verfügbaren Kategorien. Um die Standardeinstellungen der Site zu ändern, klicken Sie in der Ansicht „Standardeinstellungen der Site“ auf Bearbeiten.

KAPITEL 8

Sitzungen

In diesem Kapitel

Überblick 93
Sitzungsinformationen 93
Benutzersitzungen 98
Laufende Ressourcen 99

Überblick

In der Kategorie Sitzung werden Benutzersitzungen für alle verfügbaren Hosttypen angezeigt, einschließlich RD-Sitzungshosts und VDI. Hier können Sie alle laufenden Sitzungen einsehen, unabhängig vom Typ des Servers, auf dem die Sitzung stattfindet.

Wenn Sie die Kategorie Sitzung auswählen, werden die folgenden beiden Elemente in der Navigationsleiste Sitzungen angezeigt:

- Benutzersitzungen: Zeigt Benutzersitzungen für alle verfügbaren Hosttypen an.
- Laufende Ressourcen: Listet die derzeit laufenden veröffentlichten Ressourcen (Anwendungen und Desktops) von allen Hosts auf.

Beachten Sie, dass möglicherweise einige der Spalten in der Liste nicht sofort befüllt werden, wenn Sie die Kategorie Sitzungen oder eine der Registerkarten Aktive Sitzung öffnen. Das liegt daran, dass es ein wenig dauert, diese Werte zu berechnen. Einige Beispiele für solche Spalten sind Anmeldedauer, UX Evaluator, Latenz. Warten Sie einfach einige Sekunden, dann erscheinen die Werte in der Liste.

Sitzungsinformationen

Um Benutzersitzungen anzuzeigen, navigieren Sie zu Sitzungen > Benutzersitzungen. In der Liste werden Benutzersitzungen für alle verfügbaren Hosttypen angezeigt, einschließlich RD-Sitzungshosts und VDI.

Um Tabellenspalten ein- oder auszublenden, klicken Sie auf das Zahnradsymbol und wählen Sie die gewünschten Spalten aus oder löschen Sie diese.

Um Sitzungsdetails anzuzeigen, wählen Sie eine Sitzung aus und klicken auf den Benutzernamen. Dadurch wird die Ansicht Sitzungsinformationen geöffnet und die Sitzungsinformationen angezeigt.

Es werden die folgenden Gruppen angezeigt:

- Sitzungseinrichtung: Enthält allgemeine Sitzungsinformationen.
- Sitzungsdetails: Zeigt den aktuellen Sitzungsstatus, die Anmeldezeit, die Größe der Eingangs- und Ausgangsdaten und allgemeinen Sitzungsinformationen an.
- Benutzererfahrung: Zeigt Kennzahlen an, die verwendet werden können, um die Benutzererfahrung zu evaluieren.
- Anmeldungsdetails: Zeigt Anmeldungskennzahlen an, die verwendet werden können, um den Anmeldeprozess zu evaluieren.
- Verbindungsdetails: Zeigt die Verbindungs- und Authentifizierungsinformationen an.
- Client-Details: Zeigt Informationen über das Benutzergerät und den Parallels Client-Typ und die Version an.

Parallels RAS 18 führt über 25 neue Sitzungsdetail-Kennzahlen ein. In der Tabelle unten erhalten Sie einen Überblick über diese neuen und einige bereits vorher vorhandene wichtige Kennzahlen.

Hinweis: Für einige der angezeigten neuen Metriken ist Parallels Client erforderlich.

Sitzungseinrichtung

Messgröße	Beschreibung
Sitzungshost*	Name des Sitzungshosts
Quelle*	Nur Kategorie Sitzungen. Host-Typ: RDSH (auch wenn es über VDI läuft), VDI, RemotePC (nur über VDI), Virtueller Desktop auf Azure.

* Neu ab Parallels RAS 18.1

Sitzungsdetails

Messgröße	Beschreibung
Sitzungsstatus	Aktiv, Leerlauf, getrennt usw.
Anmeldezeit	Uhrzeit und Datum des Sitzungsaufbaus
Sitzungslänge	Zeitdauer der Sitzung

Leerlaufzeit	Zeit, in der die Sitzung untätig war
Eingehende Daten*	Menge der vom Client erhaltenen Daten
Ausgehende Daten*	Menge der an den Client gesendeten Daten
Auflösung	Sitzungsauflösung
Farbtiefe	Farbtiefe der Sitzung
Bandbreitennutzung*	Vom Client verwendete Bandbreite

* Neu ab Parallels RAS 18.0

Benutzererfahrung

Messgröße	Beschreibung
Auswertung der Benutzererfahrung	Hierbei handelt es sich um das beim Client gemessene Zeitintervall zwischen dem ersten Schritt (Benutzeraktion) und dem letzten Schritt (grafische Darstellung der Antwort).
Qualität der Verbindung*	Bewertung der Verbindungsqualität (schlecht – ausgezeichnet)
Latenz*	Netzwerklatenz
Transportprotokoll*	TCP oder UDP (über RDP)
Verfügbare Bandbreite*	Verfügbarkeit von Bandbreite aus der Sicht des Clients
Verbindungswiederherstellungen*	Anzahl der Verbindungswiederherstellungen, die bei der aktuellen Sitzung von Beginn an aufgetreten sind (ohne nicht ordnungsgemäße)
Letzte Verbindungswiederherstellungen*	Anzahl der Verbindungswiederherstellungen, die bei der aktuellen Gerätesitzung aufgetreten sind (ohne nicht ordnungsgemäße)
Ursache für die Trennung der Verbindung*	Der Grund für die Verbindungsunterbrechung der letzten Sitzung

* Neue Funktionen in Parallels RAS 18.0

Anmeldungsdetails

Messgröße	Beschreibung
Anmeldedauer*	Anmeldedauer ohne das Warten auf die Benutzerschnittstelle.
Aufschlüsselung der Anmeldedauer*	Dauer für Aufbau der Verbindung Dauer der Authentifizierung Host-Vorbereitung (inkl. Lastenausgleichsalgorithmus) Ladedauer für das Benutzerprofil Suche nach RAS-Richtlinien Verarbeitung der Gruppenrichtlinie Laden des Desktops Anderes
Benutzerprofil*	Verwendete Benutzerprofil-Methode: FSLogix, Benutzerprofil-Datenträger oder andere (enthält auch zusätzliche Informationen wie etwa Fehlercode).

* Neu ab Parallels RAS 18.0

Verbindungsdetails

Messgröße	Beschreibung
Verbindungsmodus	Vom Client verwendeter Verbindungsmodus (z. B. GW SSL).
Authentifizierungstyp	Vom Client verwendeter Authentifizierungstyp (z. B. Zugangsdaten).
MFA-Anbieter	Vom Client verwendeter MFA-Anbieter, falls anwendbar.
Flow	Listet alle Hosts auf, die die Verbindung auf dem Weg zum Ressourcenhost durchläuft (HALB, Gateway, Sitzungshost).

Client-Details

Messgröße	Beschreibung
Gerätename	Name des Geräts, von dem aus die Sitzung aufgebaut wurde
IP-Adresse	Private IP-Adresse des Clients
Client-Betriebssystem*	Das Betriebssystem, auf dem der Client läuft
Version des Client-Betriebssystems*	Die Betriebssystemversion, auf der der Client läuft
Client-Version*	Die verwendete RAS Client-Version

* Neu ab Parallels RAS 18.0

Sitzungsinformationen exportieren

Um die Sitzungsinformationen in eine CSV-Datei zu exportieren, klicken Sie in der Navigationsleiste auf Exportieren und geben Sie den Speicherort und den Dateinamen an.

Sie können Sitzungsinformationen auch aus der Hauptsitzungsliste exportieren, indem Sie im Drei-Punkt-Menü Exportieren anklicken. Beachten Sie, dass abhängig davon, was in der Liste ausgewählt wurde, Folgendes exportiert wird:

- Eine einzelne Sitzung: Die Informationen über diese Sitzung werden exportiert.
- Mehrere Sitzungen: Die Informationen über alle ausgewählten Sitzungen werden exportiert.
- Nichts wurde ausgewählt: Die Informationen über alle aktuellen Sitzungen werden exportiert. Die exportierte CSV-Datei enthält die exportierten Sitzungsdetails und die Exportinformationen im folgenden Format:

Sitzungsdetails (%Servertyp% wie RD-Sitzungshosts) aus der Parallels RAS-Serverfarm %Serverfarm-Name% und der Site %Site-Name%, exportiert von %Administrator% am %Datum% um %Uhrzeit%

Benutzersitzungen

Um eine Benutzersitzung (oder mehrere Sitzungen gleichzeitig) zu verwalten, wählen Sie eine oder mehrere Sitzungen und dann eine der folgenden Aktionen aus:

- Sitzungsinformationen anzeigen: Dadurch wird die Ansicht Sitzungsinformationen geöffnet (S. 93). Diese Option ist nur verfügbar, wenn eine einzelne Sitzung ausgewählt wurde.
- Nachricht: Öffnet das Dialogfeld Nachricht senden, in das Sie eine Nachricht eingeben und an den oder die Sitzungseigentümer versenden können.
- Trennen: Trennt die ausgewählte(n) Sitzung(en).
- Abmelden: Meldet die Sitzung(en) ab.
- Ressourcen anzeigen: Wechselt zur Ansicht Laufende Ressourcen (S. 99).
- Laufende Prozesse anzeigen: Öffnet eine Ansicht, in der die laufenden Prozesse für die ausgewählte Sitzung aufgelistet werden. Diese Option ist nur verfügbar, wenn eine einzelne Sitzung ausgewählt wurde. Siehe unten: Laufende Prozesse anzeigen.
- Überwachungseinstellungen: Öffnet einen Dialog, in dem Sie Überwachungseinstellungen konfigurieren können, um Werte in Sitzungsmetriken für RD-Sitzungshosts hervorzuheben. In diesem Dialogfeld werden die verfügbaren Metriken aufgelistet, und Sie können für eine bestimmte Metrik die Schwellenwerte „Warnung“ und „Kritisch“ festlegen. Um einen Schwellenwert festzulegen, aktivieren Sie das Kontrollkästchen vor dem Namen einer Metrik und geben die gewünschten Werte an. Während des Betriebs der RAS-Farm wird bei Erreichen eines Schwellenwerts ein Sitzungsmetrikwert wie folgt hervorgehoben: Schwellenwert „Warnung“: orange; Schwellenwert „Kritisch“: rot.

  Um die Werte für einen bestimmten Schwellenwert zurückzusetzen wählen Sie diesen aus und wählen dann im Drei-Punkt-Menü Zurücksetzen aus (oder klicken Sie mit der rechten Maustaste auf > Zurücksetzen). Sie können außerdem die Farbcodierung der Schwellenwerte für eine Metrik aktivieren oder deaktivieren. Dazu wählen Sie eine Metrik aus und wählen dann im Drei-Punkt-Menü Aktivieren oder Deaktivieren aus.
- Aktualisieren: Aktualisiert die Liste.
- Exportieren: Exportiert die Sitzungsinformationen in eine CSV-Datei. Siehe Sitzungsinformationen (S. 93).

Laufende Prozesse

Die Menüoption Laufende Prozesse anzeigen öffnet die Ansicht Laufende Prozesse für den Sitzungshost, auf den ein Filter angewandt wurde, um nur die Prozesse für die ausgewählte Sitzung anzuzeigen.

Indem Sie die drei Punkte anklicken, können Sie die folgenden Aktionen auf einen Prozess anwenden:

- Prozess beenden. Beendet den ausgewählten Prozess.
- Aktualisieren. Aktualisiert die Liste.

Laufende Ressourcen

Um eine Liste der veröffentlichten Ressourcen anzuzeigen, die aktuell auf einem Host laufen, navigieren Sie zu Sitzungen > Laufende Ressourcen.

Einige der wichtigen Spalten in der Liste sind:

- Veröffentlichter Name: Der Name der veröffentlichten Ressource (wie er in der Kategorie Veröffentlichung angezeigt wird).
- ID: Die ID der veröffentlichten Ressource (wie sie in der Kategorie Veröffentlichung angezeigt wird).
- Beschreibung: Beschreibung der veröffentlichten Ressource:
- Name des Prozesses: Der entsprechende Name des Prozesses.
- Benutzer: Sitzungseigentümer.
- Sitzungs-ID: Sitzungs-ID.
- Sitzungshost: Name des Sitzungshosts.
- Quelle: Sitzungsquelle (RDSH, VDI).

Um eine Aufgabe für eine Ressource auszuführen, wählen Sie die entsprechende Aktion in der Liste aus und klicken dann auf die drei Punkte. Einige der Aufgaben:

- Nachricht: Sendet eine Nachricht an den Sitzungseigentümer.
- Trennen: Trennt die Sitzung.
- Abmelden: Meldet die Sitzung ab.
- Laufende Prozesse anzeigen: Öffnet die Ansicht Laufende Prozesse für den Sitzungshost, auf den ein PID-Filter angewandt wurde.
- Benutzersitzung anzeigen: Öffnet die Ansicht Sitzungsinformationen (S. 93).
- Informationen anzeigen: Zeigt die Ressourcenzusammenfassung und die Sitzungsinformationen an. Die Sitzungsinformationen umfassen dieselben Metriken wie in Sitzungsinformationen (S. 93) beschrieben.

- Überwachungseinstellungen: Siehe Beschreibung der Menüoption Überwachungseinstellungen im Thema Benutzersitzungen (S. 98).
- Aktualisieren: Aktualisiert die Liste.
- Exportieren: Exportiert die Ressourceninformationen in eine CSV-Datei.

Klicken Sie auf den Ressourcennamen, um detaillierte Informationen über die veröffentlichte Ressource abzurufen. Es öffnet sich eine Ansicht, in der die grundlegenden veröffentlichten Ressourceninformationen (ID, Name, Ziel usw.) und die entsprechenden Sitzungsinformationen angezeigt werden. Eine detaillierte Beschreibung der Sitzungsmetriken finden Sie unter Sitzungsinformationen (S. 93). Wenn Sie auf den Ressourcennamen klicken, wird die Kategorie Veröffentlichung geöffnet, in der die veröffentlichte Ressource konfiguriert wird. Die Elemente in der Navigationsleiste führen dieselben Aktionen wie über die oben beschriebenen entsprechenden Menüoptionen durch.

KAPITEL 9

Veröffentlichung

Die Veröffentlichung beschreibt den Prozess, bei dem eine Ressource in Parallels RAS für die Endbenutzer verfügbar gemacht wird. Zu den Ressourcen, die in RAS-Verwaltungsportal veröffentlicht werden können, gehören:

- App
- Desktop
- Dokumente
- Ordner im Dateisystem

Die Veröffentlichung wird in der Kategorie Veröffentlichung im RAS-Verwaltungsportal durchgeführt.

Wenn Sie die Kategorie Veröffentlichung auswählen, werden die veröffentlichten Ressourcen im mittleren Fensterbereich angezeigt. Wenn Sie eine Ressource auswählen, wird die Informationen im rechten Fensterbereich angezeigt. Wenn eine Ressource in einem Ordner platziert wird, müssen Sie zunächst den Ordner erweitern und dann die Ressource auswählen. Um eine bestehende veröffentlichte Ressource zu ändern, klicken Sie auf die Schaltfläche Bearbeiten in der rechten oberen Ecke des rechten Fensterbereichs.

Um Aufgaben zur Veröffentlichung durchzuführen, verwenden Sie die Menüleiste oben im mittleren Fensterbereich. Von hier aus können Sie eine neue Ressource veröffentlichen, einen Ordner hinzufügen (z. B., um Ressourcen desselben Typs zu gruppieren), eine Ressource duplizieren, aktivieren oder deaktivieren, die Liste sortieren oder einige andere Aufgaben durchführen.

In diesem Kapitel

Veröffentlichen einer Anwendung 102
Veröffentlichen eines Desktops 103
Veröffentlichen eines Dokuments 105
Veröffentlichen eines Ordners im Dateisystem 105
Verwalten veröffentlichter Ressourcen 106

Veröffentlichen einer Anwendung

So veröffentlichen Sie eine Anwendung:

1. Wählen Sie im RAS-Verwaltungsportal die Kategorie Veröffentlichung aus.
2. Wählen Sie im mittleren Fensterbereich das Pluszeichen-Symbol (oder wählen Sie im Drei-Punkt-Menü Hinzufügen aus). Der Veröffentlichungsassistent wird geöffnet.
3. Wählen Sie auf der Seite Veröffentlichungstyp Anwendung aus und klicken Sie dann auf Weiter.
4. Wählen Sie auf der Seite Sites eine oder mehrere Sites (falls verfügbar), von denen aus die Anwendung verfügbar sein soll.
5. Klicken Sie auf Weiter.
6. Wählen Sie auf der Seite Veröffentlichen über eine der folgenden Optionen aus:
   - Alle Server der Site: Veröffentlichen Sie die Anwendung von allen Hosts aus, die auf dieser Site verfügbar sind.
   - Server-Hostpools: Geben Sie einen oder mehrere Hostpools an, von denen aus Sie die Anwendung veröffentlichen wollen.
   - Einzelne Server: Geben Sie einen oder mehrere spezifische einzelne Hosts an.
7. Klicken Sie auf Weiter.
8. Wählen Sie auf der Seite Anwendungstyp eine der folgenden Optionen aus:
   - Aus installierter und vordefinierter Anwendung auswählen: Wählen Sie diese Option aus, um von einer vorinstallierten und Standard-Windows-Anwendung aus auszuwählen.
   - Einzelne Anwendung manuell hinzufügen: Wählen Sie diese Option, um alle Anwendungseinstellungen selbst zu konfigurieren.
9. Klicken Sie auf Weiter.
10. Je nach dem von Ihnen auf der vorherigen Seite ausgewählten Anwendungstyp wird die nächste Seite folgendermaßen angezeigt:
    - Aus installierter und vordefinierter Anwendung auswählen: Diese Seite zeigt eine Liste der vorinstallierten Anwendungen und Anwendungsgruppen an. Sie können eine gesamte Gruppe oder einzelne Anwendungen auswählen. Wenn Sie fertig sind, klicken Sie auf Weiter und folgen den Anweisungen auf dem Bildschirm, um den Assistenten abzuschließen und die Anwendung(en) zu veröffentlichen. Sie können den Rest dieses Abschnitts überspringen.

- Einzelne Anwendung manuell hinzufügen: Diese Seite wird geöffnet und Sie müssen die Anwendungseinstellungen selbst eingeben. Lesen Sie weiter.

11 Wenn Sie Einzelne Anwendung manuell hinzufügen ausgewählt haben, öffnet sich eine Seite, auf der Sie die Anwendung, wie unten beschrieben, konfigurieren müssen.

Geben Sie im Abschnitt Zielanwendung Folgendes an:

- Ziel: Der ausführbare Dateiname und Pfad der Anwendung.
- Starten in: Den Pfad, den die Anwendung als aktuelles Verzeichnis verwenden sollte (Standardmäßig der ausführbare Pfad).
- Parameter: Startparameter der Anwendung (wenn vorhanden).

Geben Sie im Abschnitt Veröffentlichte Ressourcen-Einstellungen Folgendes an:

- Name: Tippen Sie einen Namen für die Anwendung ein.
- Beschreibung: Geben Sie eine optionale Beschreibung ein.
- Fenstermodus: Wählen Sie aus: „Normal“, „Maximiert“ oder „Minimiert“.
- Bei Anmeldung automatisch starten: Wählen Sie diese Option, wenn eine Anwendung starten soll, sobald sich ein Benutzer anmeldet. Diese Option funktioniert nur auf Desktop-Versionen von Parallels Client.
- Vom Sitzungsvorabstart ausschließen: Der Antrag wird in den Szenarien vor dem Start der Sitzung nicht berücksichtigt.
- Symbol: Klicken Sie auf „Durchsuchen“ und wählen Sie ein Symbol für die Anwendung aus. Symbol ändern. Ändern Sie das Anwendungssymbol (optional).

12 Geben Sie auf der nächsten Seite den Anfangsstatus der Ressource an. Wählen Sie eine der folgenden Optionen aus:

- Aktiviert: Endbenutzer können die Ressource starten.
- Deaktiviert: Die Ressource wird in Parallels Client nicht angezeigt.
- In Wartung: Die Ressource wird in Parallels Client angezeigt, aber die Benutzer können sie nicht starten. Wenn eine Ressource in Wartung ist und ein Benutzer versucht, sie zu starten, wird eine Meldung angezeigt. Um die Meldung anzupassen, klicken Sie auf die Schaltfläche Konfigurieren. Weitere Informationen finden Sie unter Standardeinstellungen der Site (Publishing) (S. 112).

13 Klicken Sie auf Weiter und dann auf Fertigstellen , um die Anwendung zu veröffentlichen.

Veröffentlichen eines Desktops

So veröffentlichen Sie einen Desktop:

1. Wählen Sie im RAS-Verwaltungsportal die Kategorie Veröffentlichung aus.
2. Wählen Sie im mittleren Fensterbereich das Pluszeichen-Symbol (oder wählen Sie im Drei-Punkt-Menü Hinzufügen aus). Der Veröffentlichungsassistent wird geöffnet.
3. Wählen Sie auf der Seite Veröffentlichungstyp Desktop aus und klicken Sie dann auf Weiter.
4. Wählen Sie auf der Seite Sites eine oder mehrere Sites (falls verfügbar), von denen aus die Anwendung verfügbar sein soll.
5. Klicken Sie auf Weiter.
6. Wählen Sie auf der Seite Veröffentlichen über eine der folgenden Optionen aus:
   - Alle Server der Site: Veröffentlichen Sie die Anwendung von allen Hosts aus, die auf dieser Site verfügbar sind.
   - Server-Hostpools: Geben Sie einen oder mehrere Hostpools an, von denen aus Sie die Anwendung veröffentlichen wollen.
   - Einzelne Server: Geben Sie einen oder mehrere spezifische einzelne Hosts an.
7. Klicken Sie auf Weiter.
8. Geben Sie auf der Seite Desktop die folgenden Optionen an:

   Geben Sie im Abschnitt Veröffentlichte Ressourcen-Einstellungen Folgendes an:

   - Name: Geben Sie einen Namen für diesen Desktop ein.
   - Beschreibung: Geben Sie eine optionale Beschreibung ein.
   - Mit Verwaltungssitzung verbinden: Wählen Sie diese Option, wenn Sie möchten, dass sich Benutzer mit der Verwaltungssitzung verbinden.
   - Bei Anmeldung automatisch starten: Wählen Sie diese Option, wenn ein Desktop geöffnet werden soll, sobald sich ein Benutzer anmeldet.
   - Vom Sitzungsvorabstart ausschließen: Der Desktop wird in den Szenarien vor dem Start der Sitzung nicht berücksichtigt.
   - Symbol: Wählen Sie ein Symbol für die Anwendung aus.

   Geben Sie im Abschnitt Desktop-Sitzungseinstellungen Folgendes an:

   - Desktop-Größe: Geben Sie die gewünschte Größe an. Sie können aus vorhandenen Optionen und Bildschirmauflösungen auswählen oder benutzerdefinierte Eingaben machen. Um eine benutzerdefinierte Breite und Höhe festzulegen, wählen Sie Benutzerdefiniert aus und geben Sie die gewünschten Werte in den entsprechenden Feldern ein.
   - Mehrere Bildschirme: Wählen Sie aus, ob die Unterstützung für mehrere Bildschirme aktiviert bzw. ob die Client-Einstellungen verwendet werden sollen.

9 Geben Sie auf der nächsten Seite den Anfangsstatus der Ressource an. Wählen Sie eine der folgenden Optionen aus:

- Aktiviert: Endbenutzer können die Ressource starten.
- Deaktiviert: Die Ressource wird in Parallels Client nicht angezeigt.
- In Wartung: Die Ressource wird in Parallels Client angezeigt, aber die Benutzer können sie nicht starten. Wenn eine Ressource in Wartung ist und ein Benutzer versucht, sie zu starten, wird eine Meldung angezeigt. Um die Meldung anzupassen, klicken Sie auf die Schaltfläche Konfigurieren. Weitere Informationen finden Sie unter Standardeinstellungen der Site (Publishing) (S. 112).

10 Klicken Sie auf Weiter und dann auf Fertigstellen , um den Desktop zu veröffentlichen.

Veröffentlichen eines Dokuments

Die Veröffentlichung eines Dokuments ähnelt der Veröffentlichung einer Anwendung, aber statt einer ausführbaren Anwendung geben Sie den Dateinamen und den Pfad des Dokuments ein. Weitere Informationen siehe Veröffentlichen einer Anwendung (S. 102).

Veröffentlichen eines Ordners im Dateisystem

So veröffentlichen Sie einen Ordner im Dateisystem:

1 Wählen Sie im RAS-Verwaltungsportal die Kategorie Veröffentlichung aus.

2 Wählen Sie im mittleren Fensterbereich das Pluszeichen-Symbol (oder wählen Sie im Drei-Punkt-Menü Hinzufügen aus). Der Veröffentlichungsassistent wird geöffnet.

3 Wählen Sie auf der Seite Veröffentlichungstyp die Option Ordner im Dateisystem aus und klicken Sie auf Weiter.

4 Wählen Sie auf der Seite Sites eine oder mehrere Sites (falls verfügbar), von denen aus die Anwendung verfügbar sein soll.

5 Klicken Sie auf Weiter.

6 Wählen Sie auf der Seite Veröffentlichen über eine der folgenden Optionen aus:

- Alle Server der Site: Veröffentlichen Sie die Anwendung von allen Hosts aus, die auf dieser Site verfügbar sind.
- Server-Hostpools: Geben Sie einen oder mehrere Hostpools an, von denen aus Sie die Anwendung veröffentlichen wollen.
- Einzelne Server: Geben Sie einen oder mehrere spezifische einzelne Hosts an.

7 Klicken Sie auf Weiter.

8 Geben Sie auf der Seite Ordner die folgenden Optionen an:

- Name: Geben Sie einen Namen für diesen Ordner ein.
- Beschreibung: Geben Sie eine optionale Beschreibung ein.
- Fenstermodus: Wählen Sie aus: „Normal“, „Maximiert“ oder „Minimiert“.
- UNC-Pfad: Geben Sie den UNC-Pfad des Ordners ein, den Sie veröffentlichen möchten.
- Symbol: Wählen Sie ein Ordnersymbol aus.

9 Geben Sie auf der nächsten Seite den Anfangsstatus der Ressource (des Ordners) an. Wählen Sie eine der folgenden Optionen aus:

- Aktiviert: Endbenutzer können die Ressource öffnen.
- Deaktiviert: Die Ressource wird in Parallels Client nicht angezeigt.
- In Wartung: Die Ressource wird in Parallels Client angezeigt, aber die Benutzer können sie nicht verwenden. Wenn eine Ressource in Wartung ist und ein Benutzer versucht, sie zu öffnen, wird eine Meldung angezeigt. Um die Meldung anzupassen, klicken Sie auf die Schaltfläche Konfigurieren. Weitere Informationen finden Sie unter Standardeinstellungen der Site (Publishing) (S. 112).

10 Klicken Sie auf Weiter und dann auf Fertigstellen , um den Ordner zu veröffentlichen.

Verwalten veröffentlichter Ressourcen

Um veröffentlichte Ressourcen anzuzeigen, wählen Sie im RAS-Verwaltungsportal die Kategorie Veröffentlichen aus.

Der Fensterbereich Veröffentlichung listet die aktuell veröffentlichten Ressourcen auf. Sie können die Liste neu anordnen, indem Sie ein Element auf die gewünschte Zeile ziehen.

Klicken Sie auf die drei Punkte, um allgemeine Verwaltungsaufgaben durchzuführen. Das Menü hat folgende Optionen:

- Hinzufügen: Öffnet den Veröffentlichungsassistenten. Das Pluszeichen-Symbol ist das entsprechende Toolbar-Element für diese Menüoption.
- Duplizieren: Erstellt eine Kopie einer ausgewählten Ressource.
- Neuer Ordner: Erstellt einen Ordner in der Liste Veröffentlichung. Dies ist ein virtueller Ordner, der nur verwendet wird, um Ressourcen in der Anwendungsliste zu gruppieren. Der Ordner wird in der Anwendungsliste in Parallels Client angezeigt. Das Ordner-Symbol ist das entsprechende Toolbar-Element für diese Menüoption.

- Aktualisieren: Aktualisiert die angezeigte Informationen.
- Status festlegen: Aktiviert/deaktiviert eine Ressource oder versetzt sie in den Wartungsmodus. Eine deaktivierte Ressource ist für Endbenutzer nicht verfügbar. Eine in Wartung versetzte Ressource wird in der Liste auf Clientseite angezeigt, kann aber nicht verwendet werden. Wenn der Status einer Ressource zu „Deaktiviert“ oder „In Wartung“ geändert wird, wird der Ressourcenname in der Liste ausgegraut und der aktuelle Status in Klammern angezeigt.
- Nach oben: Bewegt eine veröffentlichte Ressource auf der Liste weiter nach oben. Das ändern nichts an der Ressourcen-ID usw.
- Nach unten: Bewegt eine veröffentlichte Ressource auf der Liste weiter nach unten.
- Sortieren: Damit werden Ressourcen alphabetisch sortiert. Damit diese Aktionsoption aktiviert wird, müssen Sie den Knoten Veröffentlichte Ressourcen (den obersten) oder einen Ordner mit einzelnen Elementen auswählen.
- Löschen: Löscht eine veröffentlichte Ressource. Damit wird nur die veröffentlichte Ressource aus der Serverfarm entfernt. Die eigentliche Anwendung wird davon nicht berührt.

Zusatzinformationen

In den folgenden Abschnitten wird beschrieben, wie man einzelne veröffentlichte Ressourcen unterschiedlicher Art verwaltet.

Verwalten veröffentlichter Anwendungen

Wenn Sie eine Anwendung über einen Assistenten veröffentlichen, legen Sie mehrere Anwendungsparameter wie Name, Fahrt zur ausführbaren Datei usw. fest. Sie können diese Optionen ändern, nachdem die Anwendung veröffentlicht wurde.

Um eine veröffentlichte Anwendung zu ändern, wählen Sie diese im Bereich Veröffentlichte Ressourcen aus und klicken dann auf im rechten Fensterbereich auf Bearbeiten, um die Einstellungen zu ändern. Ändern Sie die Anwendungseigenschaften, wie unten beschrieben.

Beachten Sie, dass die Einstellungen hier dieselben sind wie diejenigen im Anwendungsveröffentlichungsassistenten. Weitere Details über individuell Einstellungen finden Sie auch unter Veröffentlichen einer Anwendung (S. 102). Die Beschreibungen unten konzentrieren sich auf Einstellungen, die nicht im Assistenten verfügbar sind und nur hier geändert werden können.

App

Die meisten Einstellungen hier sind dieselben wie diejenigen, die im Anwendungsveröffentlichungsassistenten beschrieben sind. Die neuen Optionsmöglichkeiten lauten Per Server-Einstellungen. Wenn die Anwendung von mehreren Servern veröffentlicht wird, können Sie die folgenden Anwendungseigenschaften einzeln für jeden Server festlegen:

- Ziel
- Starten in
- Parameter

Ein Beispiel: Sie können die oben beschriebenen Eigenschaften ändern, wenn auf verschiedenen Servern die Anwendung in verschiedenen Ordnern installiert ist, damit die Werte in den Feldern Ziel und Starten in auf jedem Server gültig sind.

Filterung

Die Optionen der Kategorie Filterung sind im Veröffentlichungsassistenten nicht verfügbar und können nur hier geändert werden. Die Kategorie wird üblicherweise für veröffentlichte Ressourcen aller Typen verwendet. Umfassende Informationen dazu finden Sie unter Verwenden von Filterregeln (S. 114).

Routing

Nähere Informationen finden Sie unter Bevorzugtes Routing konfigurieren (S. 115).

Verknüpfungen

In dieser Ansicht können Sie konfigurieren, wo eine Tastenkombination auf einem Benutzergerät konfiguriert werden soll. Diese Einstellungen werden von den Site-Standardeinstellungen übernommen, können aber für eine bestimmte Anwendung angepasst werden. Weitere Details finden Sie unter Standardeinstellungen der Site (Publishing) (S. 112).

Dateierweiterung

Diese Kategorie erlaubt es Ihnen, die Dateierweiterungszuordnung für die Anwendung zu ändern. Um einen Eintrag hinzuzufügen, zu entfernen oder zu ändern, wählen Sie die Option Dateierweiterungen zuordnen. Um der Liste eine neue Dateierweiterung hinzuzufügen, klicken Sie auf die drei Punkte, wählen Sie dann Hinzufügen aus und geben Sie die gewünschte Dateierweiterung an. Um eine bestehende Zuordnung zu ändern, wählen Sie die

Dateierweiterung in der Liste aus, klicken Sie auf die drei Punkte und wählen Sie dann die Option Eigenschaften aus.

Lizenz

Siehe Standardeinstellungen der Site (Publishing) (S. 112).

Anzeige

Siehe Standardeinstellungen der Site (Publishing) (S. 112).

Wenn Sie Änderungen vorgenommen haben, klicken Sie auf den Button Speichern oder Abbrechen, um sie zu entfernen.

Verwalten veröffentlichter Desktops

Um einen veröffentlichten Desktop zu ändern, wählen Sie ihn in der Ansicht Veröffentlichung aus. Verwenden Sie die Navigationsleiste im mittleren Fensterbereich, um die Desktopeinstellungen anzuzeigen und zu ändern. Klicken Sie auf die Schaltfläche Bearbeiten, um die Einstellungen zu bearbeiten.

Überblick

In dieser Ansicht werden weitere Navigationsleistenelemente mit kurzen Beschreibungen angezeigt. Sie können auf die Elemente hier oder in der Navigationsleiste klicken.

Veröffentlichen von

Listet Hosts oder Hostpools auf, von denen aus der Desktop veröffentlicht wird. Verwenden Sie die Dropdownliste Veröffentlichen über, um zwischen einzelnen Hosts oder Hostpools hin- und her zu schalten. Hosts oder Hostpools nach Bedarf auswählen oder löschen.

Desktop

In dieser Ansicht werden die veröffentlichten Desktop-Einstellungen angezeigt. Eine Beschreibung zur Konfiguration dieser Einstellungen finden Sie unter Desktop veröffentlichen (S. 103).

Filterung

Die Einstellungen der Kategorie Filterung sind im Veröffentlichungsassistenten nicht verfügbar und können nur hier geändert werden. Die Einstellungen werden üblicherweise für veröffentlichte Ressourcen aller Typen verwendet. Umfassende Informationen dazu finden Sie unter Verwenden von Filterregeln (S. 114).

Routing

Nähere Informationen finden Sie unter Bevorzugtes Routing konfigurieren (S. 115).

Verknüpfungen

In dieser Ansicht können Sie konfigurieren, wo ein Tastenkombination für einen veröffentlichten Desktop auf einem Benutzergerät konfiguriert werden soll. Diese Einstellungen werden von den Site-Standardeinstellungen übernommen, können aber für eine bestimmte veröffentlichte Ressource angepasst werden. Weitere Details finden Sie unter Standardeinstellungen der Site (Publishing) (S. 112).

Wenn Sie Änderungen vorgenommen haben, klicken Sie auf den Button Speichern oder Abbrechen, um sie zu entfernen.

Verwalten von Ordnern

Ordner werden verwendet, um veröffentlichte Ressourcen zu organisieren und Filteroptionen zu ermöglichen.

Es gibt zwei Arten von Ordnern, die Sie erstellen können:

- Ordner für Administrationszwecke. Ordner dieser Art sind für Parallels RAS-Administratoren vorgesehen. Sie werden benutzt, um veröffentlichte Ressourcen im RAS-Verwaltungsportal logisch zu organisieren, erscheinen aber nicht im Parallels Client-Launchpad auf Benutzergeräten. Diese Ordner werden verwendet, damit Administratoren veröffentlichte Ressourcen wirksamer verwalten können.
- Normale Ordner. Diese Ordner sind den oben beschriebenen Ordnern für Administrationszwecke ähnlich, werden aber im Launchpad auf Benutzergeräten nicht angezeigt. Sie verwenden diese Ordner in der Regel, um veröffentlichte Ressourcen nach Typen zusammenzufassen (Office-Anwendungen, bestimmte Geschäftsanwendungen, Dienstprogramme usw.).

Erstellen eines Ordners

So erstellen Sie einen neuen Ordner:

1. Wählen Sie die Kategorie Veröffentlichung aus.
2. In der Navigationsleiste Veröffentlichung klicken Sie auf das Drei-Punkt-Menü und wählen die Option Neuer Ordner aus (oder klicken Sie auf den Ordner mit dem Pluszeichen-Symbol).
3. Wählen Sie eine Site aus, von der aus der Ordner veröffentlicht werden soll. Klicken Sie auf Weiter.
4. Geben Sie einen Namen und optional eine Beschreibung ein.
5. Wählen Sie, falls erforderlich, die Option Für Administrationszwecke verwenden aus (siehe Erklärung weiter oben).
6. Wählen Sie ein Symbol aus oder verwenden Sie das standardmäßig vorgegebene.
7. Klicken Sie auf Weiter.
8. Geben Sie auf der nächsten Seite den Anfangsstatus der Ressource (des Ordners) an. Wählen Sie eine der folgenden Optionen aus:
   - Aktiviert: Endbenutzer können den Ordner sehen und die darin enthaltenen veröffentlichten Ressourcen starten.
   - Deaktiviert: Der Ordner wird in Parallels Client nicht angezeigt.
   - In Wartung: Der Ordner wird in Parallels Client angezeigt, aber die Benutzer können die darin enthaltenen Ressourcen nicht starten. Wenn der Ordner Unterordner hat, erben diese den Status des übergeordneten Ordners, was bedeutet, dass keine der Ressourcen, die in einem der Ordner in der Hierarchie enthalten sind, für Benutzer zugänglich sind. Wenn ein Ordner in Wartung ist und ein Benutzer versucht, eine Ressource aus ihm zu starten, wird eine Meldung angezeigt. Um die Meldung anzupassen, klicken Sie auf die Schaltfläche Konfigurieren. Weitere Informationen finden Sie unter Standardeinstellungen der Site (Publishing) (S. 112).
9. Klicken Sie auf Fertigstellen, um den Ordner zu erstellen.

Hinzufügen von veröffentlichten Ressourcen zu einem Ordner

Um einem Ordner eine veröffentlichte Ressource hinzuzufügen, klicken Sie darauf und verwenden dann die Optionen Nach oben oder Nach unten, um die Ressource unter dem Ordnersymbol zu platzieren.

Standardeinstellungen der Site (Publishing)

So konfigurieren Sie Standardeinstellungen der Site für veröffentlichte Ressourcen:

1 Navigieren Sie zu Infrastruktur > Standardeinstellungen der Site.

2 Klicken Sie auf Veröffentlichung.

3 Bearbeiten Sie, falls erforderlich, die Standardeinstellungen, wie unten beschrieben.

Verknüpfungen

In dieser Ansicht können Sie konfigurieren, wo eine Tastenkombination auf einem Benutzergerät konfiguriert werden soll. Beachten Sie, dass Verknüpfungen nicht auf allen Betriebssystemen verfügbar sind.

Folgende Optionen stehen Ihnen für die Erstellung von Verknüpfungen zur Verfügung:

- Verknüpfung auf Desktop erstellen: Wenn diese Option ausgewählt wird, wird eine Verknüpfung auf dem Benutzerdesktop erstellt.
- Verknüpfung in Ordner „Start“ erstellen: Erstellt eine Verknüpfung im Ordner „Start.
- Im Feld „Bearbeiten“ können Sie den Namen des Ordners eingeben, in dem die Verknüpfung erstellt werden soll. Die standardmäßige (und einzig verfügbare) %Groups%-Variable fügt zusätzliche Unterordner hinzu, wenn sie auf dem Host-Server erscheinen, auf dem die veröffentlichte Ressource gehostet wird. Wenn sich die Ressource beispielsweise unter „Myapps“ > „Spiele“ auf dem Host-Server befindet, wird dem Pfad die gleiche Ordnerstruktur hinzugefügt. Beachten Sie, dass Sie keine benutzerdefinierten Variablen verwenden können.
- Verknüpfung in Ordner „Autostart“ erstellen: Die Anwendungsverknüpfung wird dem Ordner „Autostart“ hinzugefügt und automatisch beim Hochfahren des Computers gestartet.

Lizenz

Konfigurieren Sie die folgenden Optionen, um die Nutzung der Anwendungslizenzen besser überwachen zu können:

- Session-Sharing deaktivieren: Wenn diese Option aktiviert ist, können Sie damit eine veröffentlichte Anwendung für eine Sitzung isolieren. Wenn dieselbe Anwendung mehr als einmal gestartet wird, teilen sich die Instanzen der Anwendung dieselben Sitzungen. Eine andere Anwendung wird jedoch in einer eigenen Sitzung gestartet.
- Einzelne Instanz pro Benutzer: Wenn diese Option aktiviert ist, kann ein Benutzer nur eine einzelne Instanz der Anwendung aufrufen.

- Concurrent-Lizenzen: Verwenden Sie diese Option, um die maximale Anzahl von gleichzeitigen Instanzen festzulegen, die eine Anwendung ausführen kann. Wenn die Lizenz der Anwendung beispielsweise nur das Ausführen von zehn Instanzen der Anwendung erlaubt, legen Sie die Option Concurrent-Lizenzen mit zehn fest, damit die Benutzer keine weiteren Instanzen aufrufen können, sobald diese Zahl erreicht ist.
- Aktion bei Lizenz-Überschreitung. In diesem Dropdown-Menü können Sie eine Aktion festlegen, die bei Überschreiten eines Lizenzierungslimits durchgeführt werden soll.

Anzeige

Konfigurieren Sie die folgenden Optionen:

- Warten Sie, bis alle RAS-Universaldrucker umgeleitet wurden, bevor Sie die Anwendung anzeigen. Aktivieren Sie diese Option, um zu warten, bis die Drucker umgeleitet werden, bevor die Anwendung geladen wird. Sie können auch die maximale Wartezeit (in Sekunden) für die Umleitung der Universaldrucker angeben. Beachten Sie, dass die Umleitung eines Druckers einige Zeit in Anspruch nehmen kann. Um Verwirrung zu vermeiden, wird dem Benutzer ein Fortschrittsbalken angezeigt, während die Drucker umgeleitet werden.
- Maximale Wartezeit (Sekunden):
- Farbtiefe: Wählen Sie eine Farbtiefe für die Anwendung aus.
- Anwendung maximiert starten, wenn mobile Clients verwendet werden. Diese Option gilt nur für Parallels Client, der auf mobilen Geräten ausgeführt wird. Wenn die Option ausgewählt ist, startet die Anwendung auf einem mobilen Gerät im maximierten Zustand. Dies bietet den Benutzern die beste Erfahrung bei der Arbeit mit einer Remote-Anwendung. Diese Option bietet dem RAS-Administrator eine einfache Möglichkeit, eine Anwendung immer zu maximieren, ohne zusätzliche Schritte zu unternehmen.

Wartungsmeldung

Auf der Ansicht Wartungsmeldung können Sie eine Meldung angeben, die den Benutzern angezeigt wird, wenn sie versuchen, eine veröffentlichte Ressource während der Wartung zu starten. Wenn sich eine Ressource in der Wartung befindet, wird sie zwar in Parallels Client angezeigt, ist aber ausgegraut (im Nutzerportal wird dies im Ressourcennamen angegeben). Wenn ein Benutzer versucht, die Ressource zu öffnen, wird die Meldung angezeigt, die Sie hier festlegen. Wenn Sie eine Meldung geändert haben, aber die Standardmeldung wiederherstellen möchten, wählen Sie eine Meldung in der gewünschten Sprache aus und klicken Sie auf die Schaltfläche Zurücksetzen.

Wenn Sie die Änderungen der Standardeinstellungen der Site abgeschlossen haben, klicken Sie auf Speichern.

Verwenden von Filterregeln

Mit Filterregeln können Sie steuern, wer Zugriff auf eine bestimmte veröffentlichte Ressource hat. Jede Regel besteht aus einem oder mehreren Kriterien für den Abgleich mit Benutzer-Verbindungen. Jedes Kriterium besteht wiederum aus einem oder mehreren spezifischen Objekten, die abgeglichen werden können.

Sie können die folgenden Objekte abgleichen:

- Benutzer, eine Gruppe, zu der der Benutzer gehört, oder der Computer, von dem aus der Benutzer eine Verbindung herstellt.
- Das Secure Gateway, mit dem sich der Benutzer verbindet.
- Name des Client-Geräts.
- Betriebssystem des Client-Geräts.
- Design.
- IP-Adresse.
- Hardware-ID. Das Format einer Hardware-ID hängt vom Betriebssystem des Clients ab.

Beachten Sie bitte folgende Hinweise zu den Regeln:

- Die Kriterien werden mit dem AND-Operator verknüpft. Wenn eine Regel beispielsweise ein Kriterium enthält, das auf bestimmte IP-Adressen zutrifft, und ein Kriterium, das auf die Betriebssysteme der Client-Geräte zutrifft, wird die Regel angewendet, wenn eine Benutzer-Verbindung mit einer der IP-Adressen UND einem der Client-Betriebssysteme übereinstimmt.
- Die Kriterien werden mit dem OR-Operator verknüpft. Wenn Sie z. B. nur ein Kriterium für passende Client-Geräte-Betriebssysteme erstellen, wird die Regel angewendet, wenn eines der Betriebssysteme mit der Clientverbindung übereinstimmt.
- Die Regeln werden von oben nach unten mit einer Benutzer-Verbindung verglichen. Darum hängt die Priorität einer Regel von ihrem Platz in der Regelliste ab. Parallels RAS wird die erste Regel anwenden, die der Benutzer-Verbindung entspricht.
- Wenn keine andere Regel zutrifft, wir die Standardregel angewandt. Sie können sie entweder auf Zulassen oder Ablehnen einstellen (siehe unten), aber für diese Regel sind keine anderen Kriterien verfügbar.

So erstellen Sie eine neue Regel:

1 Navigieren Sie zu Veröffentlichung.

2 Klicken Sie auf die Ressource, für die Sie eine Regel erstellen möchten.

3 Klicken Sie im mittleren Fensterbereich auf Filterung.

4 Klicken Sie auf Bearbeiten.

5 Klicken Sie auf Plus-Symbol.

6 Geben Sie den Namen und optional eine Beschreibung der Regel ein.

7 Geben Sie die Kriterien für die Regel an. Folgende Steuerelemente sind verfügbar:

- Erlauben: gibt an, dass die Ressource zugänglich sein muss, wenn eine Benutzer-Verbindung den Kriterien entspricht. Klicken Sie auf Erlauben, um die Option auf Ablehnen zu ändern.
- Ablehnen: gibt an, dass die Ressource nicht zugänglich sein darf, wenn eine Benutzer-Verbindung den Kriterien entspricht. Klicken Sie auf Ablehnen, wenn, um die Option auf Erlauben, wenn zu ändern.
- (+): fügt ein neues Kriterium hinzu. Wenn Sie ein Secure Gateway, einen Client-Gerätenamen, ein Client-Gerätebetriebssystem, ein Design, eine IP-Adresse oder eine Hardware-ID abgleichen möchten, klicken Sie auf (+).
- (X): Löscht ein bestimmtes Objekt aus dem Abgleich. Wenn Sie z. B. die IP-Adresse 198.51.100.1 aus dem Abgleich entfernen möchten, klicken Sie daneben auf (X).
- Ist: gibt an, dass die Ressource zugänglich sein muss (oder unzugänglich, durch Erlauben und Ablehnen), wenn eine Benutzer-Verbindung den Kriterien entspricht. Klicken Sie auf „Ist“, um dieses Steuerungselement auf Ist nicht zu ändern. Dieses Steuerungselement wird angezeigt, wenn mindestens ein Objekt hinzugefügt wurde.
- Ist nicht: gibt an, dass die Ressource nicht zugänglich sein darf (oder zugänglich, durch Erlauben und Ablehnen), wenn eine Benutzer-Verbindung den Kriterien nicht entspricht. Klicken Sie auf „Ist nicht“, um dieses Steuerungselement auf Ist zu ändern. Dieses Steuerungselement wird angezeigt, wenn mindestens ein Objekt hinzugefügt wurde.

Sie können die Kriterien aktivieren/deaktivieren, indem Sie links daneben auf den Schalter klicken.

8 Klicken Sie zum Abschluss auf Speichern.

Bevorzugtes Routing konfigurieren

Überblick

Bevorzugtes Routing ist eine nützliche Funktion, wenn sich Parallels RAS-Benutzer mit unterschiedlichen geografischen Standorten mit derselben Parallels RAS-Serverfarm/-Site verbinden. Die Verwendung einer gemeinsamen Zugriffsebene (RAS Secure Gateway, HALB oder ein Load Balancer eines Drittanbieters) ist nicht optimal, wenn sich eine Ressource in einem anderen Rechenzentrum in derselben RAS Serverfarm/Site befindet. Die Lösung besteht

darin, einen bevorzugten Server der Zugriffsebene für eine bestimmte veröffentlichte Ressource zu konfigurieren. In diesem Fall würde jeder Benutzer eine Verbindung zu einem Standard-Secure Gateway herstellen, aber nach vom Administrator festgelegten Proximity-Regeln umgeleitet werden. In der Regel bietet die Verwendung des Secure Gateway, das dem Sitzungshost am nächsten liegt, eine bessere Benutzererfahrung, einen geringeren internen Netzwerkverkehr und damit verbundene Kosten sowie eine bessere Nutzung der Ressourcen.

Hinweis: Das bevorzugte Routing gilt nicht für veröffentlichte Objekte von Azure Virtual Desktop.

So funktioniert das bevorzugte Routing:

1. Parallels Client stellt eine Verbindung mit einem Secure Gateway unter Verwendung einer Standardauthentifizierung her.
2. Über den RAS Connection Broker wird die bevorzugte Route der Ressource (sofern konfiguriert) ermittelt.
3. Parallels Client erhält die bevorzugte öffentliche Adresse, um die Ressource zu starten.
4. Parallels Client versucht dann, die Ressource über die umgeleitete Adresse zu starten und greift auf das ursprüngliche Gateway zurück, wenn dies nicht gelingt.

Bevorzugtes Routing konfigurieren

Um bevorzugtes Routing zu konfigurieren, müssen Sie zunächst eine oder mehrere benutzerdefinierte öffentliche Serveradressen für eine Site angeben. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie im RAS-Verwaltungsportal die Kategorie Site-Einstellungen aus.
2. Im Menü Verbindungen wählen Sie Adressen aus.
3. Klicken Sie auf das Pluszeichen-Symbol und in dem Dialogfeld, das sich jetzt öffnet, geben Sie einen Namen für diese benutzerdefinierte Adresse, optional eine Beschreibung, eine öffentliche Adresse, den Port und SSL-Port (es wird empfohlen, für das Benutzersitzungsrouting einen SSL-Port zu verwenden) ein.

Sobald eine oder mehrere benutzerdefinierte Serveradressen konfiguriert wurden, können Sie eine solche Adresse für eine veröffentlichte Ressource wie folgt angeben:

1. Wählen Sie die Kategorie Veröffentlichung aus.
2. Wählen Sie eine veröffentlichte Ressource aus.
3. Klicken Sie im mittleren Fensterbereich auf Routing.
4. Im Bereich „Bearbeiten“ klicken Sie auf Bearbeiten.
5. Wählen Sie die Option Bevorzugtes Routing aktivieren.

6 Klicken Sie auf das Pluszeichen-Symbol.

7 Wählen Sie aus der Liste eine benutzerdefinierte Adresse aus, die Sie als bevorzugte Route für diese veröffentlichte Ressource verwenden möchten.

KAPITEL 10

Überwachung

In diesem Kapitel

Überblick 118
Installieren von RAS Performance Monitor 119
Überwachung im RAS-Verwaltungsportal aktivieren 120
Anzeigen von Leistungskennzahlen 121
Konfigurieren der Sicherheit für RAS Performance Monitor 123

Überblick

Die Kategorie Überwachung bietet Ihnen Zugang zu RAS Performance Monitor, ein browserbasiertes Dashboard, das Administratoren bei der Analyse von Engpässen und der Ressourcennutzung einer Parallels RAS-Bereitstellung unterstützt. Das Dashboard bietet eine visuelle Darstellung der Leistungskennzahlen, die in der Parallels RAS Konsole oder in einem Webbrowser angezeigt werden können.

Komponenten

Parallels RAS Performance Monitor besteht aus den folgenden Komponenten:

- InfluxDB-Datenbank – eine Datenbank zum Speichern von Systemperformancedaten.
- Grafana-Dashboard – ein browserbasiertes Dashboard, auf dem Leistungskennzahlen eingezeichnet werden.
- Telegraf-Dienst – ein Dienst, der Leistungsdaten auf einem Server sammelt, auf dem er installiert ist. Der Dienst wird automatisch installiert, wenn Sie einen Server einer Parallels RAS-Serverfarm hinzufügen und einen entsprechenden RHS Agent darauf einrichten (beispielsweise RAS Secure Gateway Agent, RD Session Host Agent, Remote PC Agent usw.).

Funktionsweise:

Der Telegraf-Dienst wird standardmäßig gestoppt und sammelt daher keine Daten. Um den Dienst auf jeden Server in der Farm zu starten, muss die Funktion für die Leistungsüberwachung auf der Parallels RAS-Konsole und/oder Parallels-Verwaltungsportal konfiguriert und aktiviert sein. Nachdem er aktiviert wurde, beginnt der Telegraf-Dienst mit der

Sammlung einer vordefinierten Gruppe von Leistungskennzahlen in einem festgelegten Zeitintervall (10 Sekunden). Danach sendet er die gesammelten Daten an die InfluxDB-Datenbank zum Speichern. Um Leistungskennzahlen anzuzeigen, benutzt der Parallels RAS-Administrator die Kategorie Überwachung des Parallels RAS-Verwaltungsportals, das die visuelle Darstellung der Leistungszähler in Echtzeit anzeigt.

Die Leistungskennzahlen werden im Dashboard nach Typ (Sitzung, CPU, Arbeitsspeicher, Festplatte usw.) gruppiert, sodass der Administrator jede Gruppe von Kennzahlen getrennt einsehen kann. Der Administrator kann auch auswählen, ob Leistungskennzahlen für einen oder mehrere spezifische Server oder für alle Server in der Farm oder auf der Site angezeigt werden. Zusätzlich kann der Administrator eine bestimmte Site auswählen, für die die Daten angezeigt werden sollen.

Installieren von RAS Performance Monitor

Voraussetzungen

Parallels RAS Performance Monitor ist eine separate Komponente von Parallels RAS mit eigenem Installationsprogramm. Er kann auf einem dedizierten Server oder auf einem Server installiert werden, der eine der Parallels RAS-Komponenten hostet. Wenn Sie das Installationsprogramm ausführen, werden die InfluxDB-Datenbank und der Grafana Dashboard-Dienst automatisch installiert. Weitere Informationen finden Sie im untenstehenden Unterabschnitt Installation.

Die folgenden Firewall-Regeln (offene Ports) werden automatisch auf dem Server hinzugefügt, auf dem Sie Parallels RAS Performance Monitor installieren:

- TCP Port 8086 (wird von der InfluxDB-Datenbank verwendet).
- TCP Port 3000 (wird vom Grafana-Performance-Dashboard verwendet).

Installation

So installieren Sie Parallels RAS Performance Monitor:

1. Laden Sie das Parallels RAS Performance Monitor-Installationsprogramm von https://www.parallels.com/de/products/ras/download/links/ herunter.
2. Führen Sie den Installationsassistenten (die Datei RASPerformanceMonitor.msi) aus und befolgen Sie die Anweisungen auf dem Bildschirm.
3. Schließen Sie den Assistenten, wenn Sie fertig sind.

Überwachung im RAS-Verwaltungsportal aktivieren

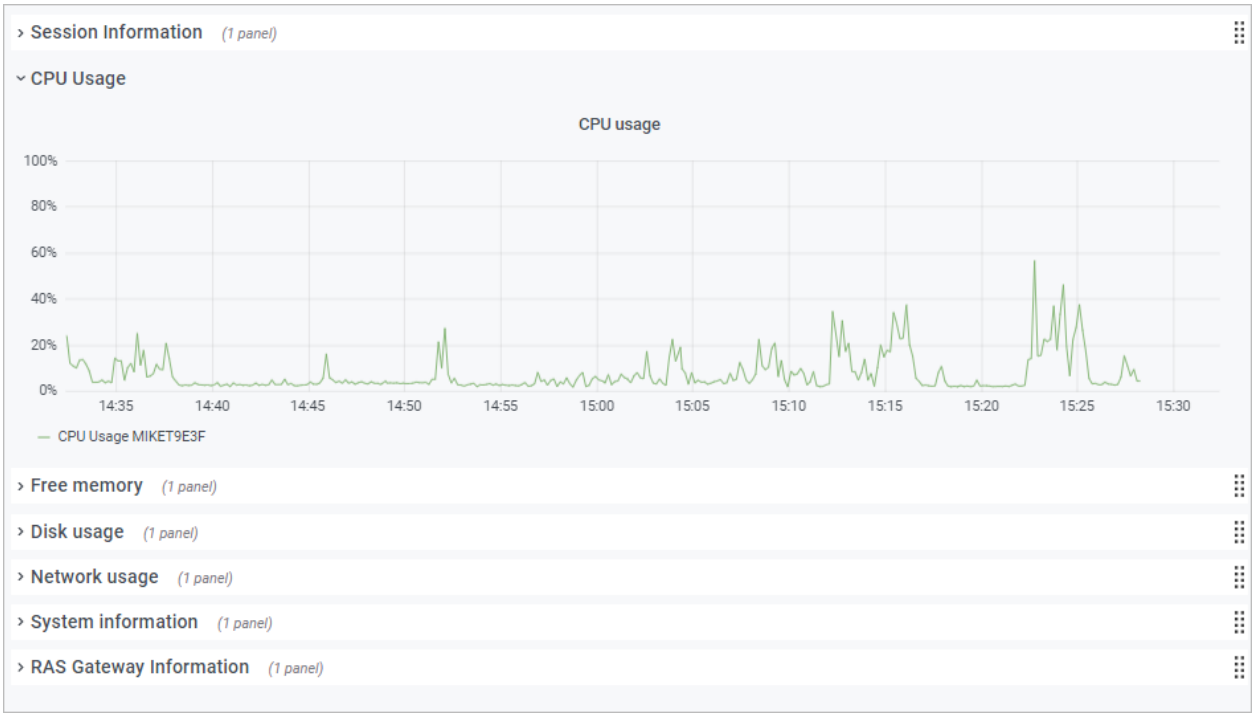
Hinweis: Um RAS Performance Monitor im Verwaltungsportal zu aktivieren, müssen Sie Root-Administrator einer RAS-Farm sein.

So aktivieren Sie RAS Performance Monitor:

1. Wählen Sie im Verwaltungsportal in der Seitenleiste die Kategorie Überwachung aus.
2. Klicken Sie im rechten Fensterausschnitt auf den Link Farm-Einstellungen. Die Kategorie Farm-Einstellungen wird geöffnet, die Unterkategorie Überwachung ist ausgewählt.
3. Klicken Sie im oberen Fensterbereich auf die Schaltfläche Bearbeiten.
4. Wählen Sie die Option RAS Performance Monitor aktivieren aus.
5. Geben Sie Verbindungseinstellungen für den Server an, auf dem die RAS Performance Monitor-Datenbank gehostet wird:
   - Server: Geben Sie den FQDN oder die IP-Adresse des Servers an, auf dem Sie die InfluxDB-Datenbank und das Grafana-Dashboard installiert haben.
   - Port: Der Standardport ist 8086. Sie können diesen bei Bedarf ändern.
6. Klicken Sie auf Speichern.

Anzeigen von Leistungskennzahlen

Wählen Sie in der Seitenleiste die Kategorie Überwachung, um die Leistungskennzahlen anzuzeigen. Im rechten Fensterbereich wird das Leistungskennzahlendashboard angezeigt.



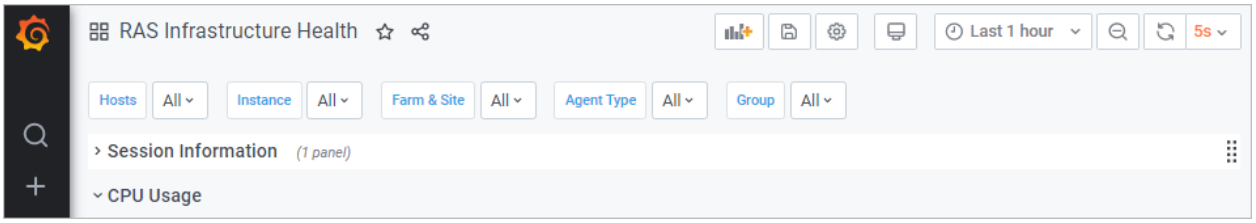
Um die Kennzahlen eines bestimmten Typs anzuzeigen, erweitern Sie die gewünschte Kategorie in den Hauptbereich des Dashboards. Die Kategorien sind:

- Sitzungsinformationen. Zeigt die Informationen über aktive Sitzungen und getrennte Sitzungen an.
- CPU-Auslastung. CPU-Zähler.
- Freier Arbeitsspeicher. Zähler für den physischen Speicher.
- Festplattennutzung. Zähler für Festplatten-I/O.
- Netzwerk-Auslastung. Netzwerkschnittstelle-I/O-Zähler.
- Systeminformationen. Zähler für Systeminformationen.
- RAS-Gateway-Informationen. RAS-Gateway-Zähler.

Leistungskennzahlen werden im Dashboard als Diagramm angezeigt. Verschiedene Zähler werden mithilfe verschiedener Farben angezeigt.

Um einen bestimmten Bereich eines Diagramms vergrößern, wählen Sie einen rechteckigen Block mit der Maus aus. Sie können auch die Zoom-Steuerung über dem Dashboard für die Vergrößerung des Zeitbereichs, zur Zeitverschiebung nach vorn oder zur Zeitverschiebung nach hinten verwenden. Um einen bestimmten Zeitbereich auszuwählen, klicken Sie auf das Uhrsymbol oben und geben Sie dann einen Zeitbereich an.

Standardmäßig wird das Dashboard im Kioskmodus geöffnet. Um das Dashboard zu verlassen, drücken Sie „Esc“. Um den Ansichtsmodus zu wechseln, klicken Sie auf das „Monitor“-Symbol oben rechts. Wenn Sie den Kioskmodus beenden, wird die Seite RAS-Infrastruktur-Systemzustand angezeigt:



Das Menü oben hat folgende Optionen:

- Hosts. Ermöglicht Ihnen die Auswahl von einem oder mehreren Servern, für die die Leistungskennzahlen angezeigt werden sollen. Zum Anzeigen der Daten für alle Server des Standorts wählen Sie Alle. Wenn Sie keine Server in der Liste sehen, müssen Sie warten, bis der Parallels RAS Performance Monitor die ersten statistischen Daten gesammelt hat. Dies erfolgt nur bei der Erstinstallation.
- Instanz. Mit diesem Element können Sie eine spezifische Zählerinstanz aussuchen (wenn mehr als eine vorhanden ist). Bei Netzwerkzählern ist dies normalerweise der Name einer Netzwerkschnittstelle. Bei Festplattenzählern ist dies ein Festplattenname. Andere Typen von Zählern haben normalerweise nicht mehrere Instanzen.
- Serverfarm und Site. Wählen Sie eine Site aus, für die die Daten angezeigt werden sollen. Zum Anzeigen der Daten für alle Sites in der Farm wählen Sie Alle. Wenn Sie eine andere RAS-Farm haben und der RAS Performance Monitor konfiguriert und aktiviert ist, können Sie auch eine Site aus dieser Farm auswählen.
- Agenttyp. Wählen Sie einen RAS-Agenttyp aus.
- Gruppe. Wählen Sie eine RDS-Gruppe aus.

Weitere Informationen über Leistungskennzahlen und ihre Bedeutung finden Sie den folgenden Artikeln bei Microsoft:

- https://technet.microsoft.com/de-de/library/cc976785.aspx
- https://technet.microsoft.com/de-de/library/2008.08.pulse.aspx

Weitere Informationen finden Sie unter RAS-Leistungsindikatoren (S. 145).

Konfigurieren der Sicherheit für RAS Performance Monitor

Standardmäßig kann jeder Benutzer auf die Seite „Performance Monitor“ zugreifen und Leistungskennzahlen anzeigen. Um die Sicherheit zu erhöhen, können Sie den RAS Performance Monitor so einrichten, dass Zugangsdaten notwendig sind, sodass nur autorisierte Benutzer ihn sehen können.

Entfernen Sie zunächst die anonyme Authentifizierung aus der Grafana-Konfigurationsdatei wie folgt:

1. Öffnen Sie die Datei C:\Program Files\Parallels\RAS Performance Monitor\conf\defaults.ini.
2. Suchen Sie in der Datei nach Folgendem:

```
################################### Anonymous Auth
######################

[auth.anonymous]

# enable anonymous access

enabled = true
```

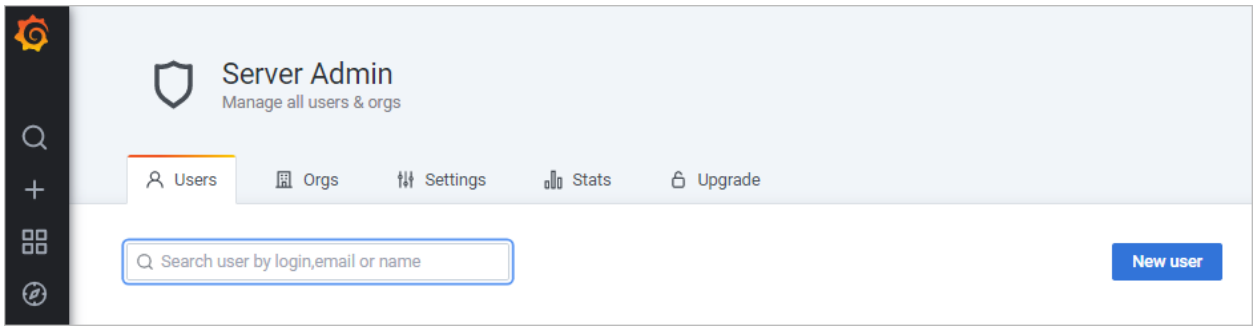
3. Ändern Sie `"enabled = true"` auf `"enabled = false"`.

   Hinweis: Der Benutzer wird nach der Deaktivierung des anonymen Zugriffs automatisch aufgefordert, das Admin-Passwort zu ändern. Danach kann das Passwort gemäß der offiziellen Grafana-Dokumentation geändert werden: https://grafana.com/docs/grafana/latest/manage-users/user-admin/change-your-password/.

4. Neustart des Grafana-Service.
5. Wählen Sie die Kategorie Überwachung und melden Sie sich mit den folgenden Zugangsdaten bei Grafana an:
   - Benutzer: admin
   - Passwort: admin (wenn Sie das Passwort zuvor geändert haben, verwenden Sie das aktuelle Passwort).

6 Wenn Sie angemeldet sind, drücken Sie „Esc“ und klicken Sie auf das Schildsymbol > Benutzer.

7 Klicken Sie auf Neuer Benutzer und erstellen Sie einen neuen Benutzer.



8 Sie müssen den Benutzer nun zur Liste Ihrer Organisation hinzufügen. Klicken Sie dazu in der Liste Benutzer auf Bearbeiten, um den Benutzer zu bearbeiten, legen Sie die Organisation fest und machen Sie den Benutzer zum Betrachter.

9 Klicken Sie auf Hinzufügen, um den Benutzer zur Liste Ihrer Organisation hinzuzufügen. Der Benutzer kann nun die Statistiken des RAS-Performance-Monitors einsehen.

KAPITEL 11

RAS-Agents aktualisieren

Wenn Sie Parallels RAS-Komponenten zu einer Farm hinzufügen, installieren Sie einen entsprechenden RAS-Agent darauf. Dazu gehören RAS Connection Broker, RD Session Host Agent, VDI Agent, Guest Agent, Remote PC Agent. Zusätzlich zu den Funktionen, mit denen Sie den Agent-Status überprüfen und bei Bedarf aktualisieren können, können Sie ein Bulk-Agent-Update oder -Upgrade durchführen.

Es gibt zwei Möglichkeiten, wie Sie herausfinden können, ob Agents aktualisiert werden müssen. Sie können sich von Parallels RAS benachrichtigen lassen oder den Status überprüfen und den Aktualisierungsvorgang manuell einleiten.

Wenn Sie das RAS-Verwaltungsportal öffnen, wird evtl. eine Nachricht angezeigt, die Sie darauf hinweist, dass RAS-Agents aktualisiert werden müssen. Sie können den Aktualisierungsvorgang starten, indem Sie in diesem Dialogfeld auf den Link Update im Nachrichtenfeld klicken.

Um den Vorgang manuell zu starten, wählen Sie die Kategorie Site aus und klicken dann auf Alle Agents aktualisieren. Befolgen Sie die Anweisungen auf dem Bildschirm und wählen Sie die Server aus, auf denen ein Agent ein Update oder Upgrade benötigt. Hinweis: Wenn alle Agents auf allen Servern, die in einem bestimmten Bereich angezeigt werden, auf dem neuesten Stand sind, wird der Link Alle Agents aktualisieren nicht angezeigt.

KAPITEL 12

Hilfe und Support

Die Kategorie Hilfe und Support enthält Links zu Ressourcen, die Sie dabei unterstützen, Antworten auf Fragen zu finden, Probleme zu lösen, Software und Dokumentation herunterzuladen und Parallels Support zu kontaktieren.

Beachten Sie, dass einige Links Sie auf die Seite Parallels My Account führen, wo Sie sich anmelden müssen. Wenn Sie ein Parallels RAS-Abonnement besitzen, haben Sie bereits ein Konto. Wenn Sie noch kein Parallels-Konto haben, müssen Sie zunächst eines einrichten.

Um sich mit dem Parallels Support in Verbindung zu setzen, verwenden Sie die Links im Abschnitt Support:

- Systembericht in Parallels hochladen: Sammelt die erforderlichen Daten und sendet einen Systembericht an Parallels. Bitte beachten Sie, dass es sich dabei nicht um eine offizielle Supportanfrage handelt.
- Systembericht herunterladen: Erfasst die Daten und speichert sie am angegebenen Ort. Das kann hilfreich sein, wenn ein Mitarbeiter vom Parallels Support Sie darum bittet, einen Bericht einzusenden.
- Support-Anfrage erstellen: Sendet eine offizielle Support-Anfrage an Parallels, die auch einen Systembericht mit weiteren Umgebungsinformationen für Parallels Support enthalten kann. Klicken Sie auf diesen Link und folgen Sie den Anweisungen auf dem Bildschirm.

KAPITEL 13

Anhang

In diesem Kapitel

Microsoft-Lizenzanforderungen in Parallels RAS 127
Port-Referenz..... 133
RAS-Leistungsindikatoren 145

Microsoft-Lizenzanforderungen in Parallels RAS

Dieser Abschnitt dient als Anleitung, um Klarheit über die Microsoft-Lizenzanforderungen in einer Parallels RAS-Umgebung zu schaffen, dient aber nicht als ausschließliche Liste. Wenn Sie weitere Informationen benötigen, wenden Sie sich bitte an Ihren Microsoft-Lizenzpartner.

Die Microsoft-Lizenzanforderungen umfassen:

Allgemein

- Jedes Windows Server- und Desktop-Betriebssystem (OS), das verwendet werden soll.
- Das Windows Server-Betriebssystem, auf das zugegriffen werden soll, muss durch Microsoft Windows Server-Clientzugriffslizenzen (CALs) abgedeckt sein.

RD-Sitzungshosts

Wenn auf Windows Server aus der Ferne zugegriffen wird (für nicht-administrative Arbeiten), dann benötigen Sie eine Lizenz für den Zugriff auf den Remotedesktopdienst (RDS):

- RDS-CALs sind für Benutzer oder Geräte erforderlich, die die Remotedesktopdienst-Funktionalität auf Windows Server nutzen möchten. Die folgenden Typen von RDS CAL sind verfügbar:
  - **a** RDS-CAL pro Gerät: Erlaubt einem Gerät (das von einem beliebigen Benutzer verwendet wird) die Nutzung der Remotedesktopdienste-Funktionalität auf jedem Ihrer Server.
  - **b** RDS-CAL pro Benutzer: Erlaubt einem Benutzer (mit einem beliebigen Gerät) die Nutzung der Remotedesktopdienste-Funktionalität auf jedem Ihrer Server.
  - **c** RDS External Connector: Erlaubt mehreren externen Benutzern den Zugriff auf einen einzelnen Remotedesktopserver. Wenn Sie mehrere Server haben, benötigen Sie

mehrere externe Connectors zusätzlich zu den erforderlichen Windows Server External Connectors.

Sie können sich dafür entscheiden, RDS-CALs pro Gerät und RDS-CALs pro Benutzer gleichzeitig mit der Server-Software zu kombinieren. Reguläre Benutzer- oder Geräte-CALs werden zusätzlich zu den RDS-CALs pro Benutzer oder Gerät benötigt.

- RDS SAL ist ein Dienst, der eine Microsoft Abonnenten-Zugangslizenz (SAL) für Remotedesktopdienste (RDS) („RDS SAL“ genannt) auf virtuellen Maschinen bereitstellt, die in Compute Resource erstellt wurden. Dadurch ist es möglich, dass drei oder mehr Benutzer eine Verbindung zu einem Remotedesktop (RD-Sitzungshost) für eine bestimmte virtuelle Maschine in Compute Resource (für SPLA-Partner) herstellen können.

Weitere Informationen:

- Lizenzieren Sie Ihre RDS-Bereitstellung mit Client-Zugriffslizenzen (CALs): https://docs.microsoft.com/de-de/windows-server/remote/remote-desktop-services/rds-client-access-license.
- Datenblatt zur RDS-Lizenzierung https://download.microsoft.com/download/6/B/A/6BA3215A-C8B5-4AD1-AA8E-6C93606A4CFB/Windows_Server_2012_R2_Remote_Desktop_Services_Licensing_Datasheet.pdf.
- Übersicht und FAQ zu RDS CAL https://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Licensing-Windows-Server-2012-R2-RDS-and-Desktop-Apps-for-RDS.pdf.
- Lizenzierung von Microsoft Desktop-Anwendungssoftware zur Verwendung mit Windows Server RDS https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/desktop_application_with_windows_server_remote_desktop_services.pdf.

Hypervisor und VDI

1 Bei Verwendung von Microsoft Hyper-V als Hypervisor sind Lizenzen für das Microsoft Windows Server-Betriebssystem erforderlich

Weitere Informationen:

- Datenblatt für Lizenz für Windows Server 2022 https://www.microsoft.com/en-us/windows-server/pricing.
- Datenblatt für Lizenz für Windows Server 2019 https://download.microsoft.com/download/7/C/E/7CED6910-C7B2-4196-8C55-208EE0B427E2/Windows_Server_2019_licensing_datasheet_EN_US.pdf.
- Datenblatt für Lizenz für Windows Server 2016 https://download.microsoft.com/download/7/2/9/7290EA05-DC56-4BED-9400-138C5701F174/WS2016LicensingDatasheet.pdf.

2 Bei Verwendung von Virtual Desktop Infrastructure (VDI) sind Lizenzen für Windows Software Assurance oder Azure Virtual Desktop Access (VDA) erforderlich. Microsoft lizenziert Windows nach Zugriffsgerät:

- Die Zugriffsrechte für virtuelle Desktops sind ein Vorteil der Windows Client Software Assurance (SA). Kunden, die unter SA abgedeckte PCs nutzen wollen, haben ohne zusätzliche Kosten Zugriff auf ihre VDI-Desktops.
- Kunden, die Geräte verwenden möchten, die nicht für Windows Client SA qualifiziert sind, wie z. B. Thin Clients, müssen diese Geräte mit Azure Virtual Desktop Access (VDA) lizenzieren, um auf einen Windows VDI-Desktop zugreifen zu können. Windows VDA ist auch auf Geräte von Dritten anwendbar, z. B. auf PCs von Auftragnehmern oder Mitarbeitern.

Weitere Informationen:

- Lizenzierungsportal für Windows 11 https://www.microsoft.com/de-de/Licensing/product-licensing/windows.
- Lizenzierungsportal für Windows 10 https://www.microsoft.com/de-de/licensing/product-licensing/windows10?activetab=windows10-pivot:primaryr3.
- Anleitung zur Lizenzierung des Windows Desktop-Betriebssystems für die Verwendung mit virtuellen Maschinen https://download.microsoft.com/download/9/8/d/98d6a56c-4d79-40f4-8462-da3ecba2dc2c/licensing_windows_desktop_os_for_virtual_machines.pdf.
- Lizenzierung von Windows-Desktops für VDI-Umgebungen https://docs.microsoft.com/en-us/answers/storage/temp/12620-microsoft-vdi-and-vda-faq-v3-0.pdf.

Microsoft Azure

Microsoft Online Business Services, wie Microsoft 365 oder Microsoft Azure, benötigen Microsoft Entra ID für die Anmeldung und zur Unterstützung des Identitätsschutzes. Wenn Sie einen beliebigen Microsoft Online Business-Dienst abonnieren, erhalten Sie automatisch Microsoft Entra ID mit Zugriff auf alle kostenlosen Funktionen. Um Ihre Microsoft Entra ID-Implementierung zu erweitern, können Sie auch kostenpflichtige Funktionen hinzufügen, indem Sie auf Microsoft Entra ID Premium P1- oder Premium P2-Lizenzen upgraden.

Weitere Informationen:

- Microsoft Entra ID-Implementierungenhttps://docs.microsoft.com/de-de/azure/active-directory/fundamentals/active-directory-whatis

- Azure-Hybridborteile https://azure.microsoft.com/de-de/pricing/hybrid-benefit/

Azure Virtual Desktop

- Der Zugriff auf Windows 10 Enterprise-Multisession, Windows 11 Enterprise-Multisession, Windows 10 Enterprise- und Windows 11 Enterprise-Desktops und -Anwendungen ist ohne zusätzliche Kosten möglich (ausgenommen Rechen-, Speicher- und Netzwerkkosten), wenn Sie eine der folgenden Lizenzen pro Benutzer besitzen:
  - **a** Microsoft 365 E3/E5
  - **b** Microsoft 365 A3/A5/Student Use Benefits
  - **c** Microsoft 365 F3
  - **d** Microsoft 365 Business Premium
  - **e** Windows 10 Enterprise E3/E5
  - **f** Windows 10 Education A3/A5
  - **g** Windows 10 VDA pro Benutzer
- Der Zugriff auf Desktops, die von den Windows Server-Remotedesktopdiensten unter Windows Server 2012 R2 und neuer betrieben werden, wird ohne zusätzliche Kosten (ausgenommen Rechen-, Speicher- und Netzwerkkosten) bereitgestellt, wenn Sie eine RDS-CAL-Lizenz pro Benutzer oder pro Gerät mit aktiver Software Assurance (SA) besitzen.

Weitere Informationen:

- Preisübersicht für Azure Virtual Desktop: https://azure.microsoft.com/de-de/pricing/details/virtual-desktop/

FSLogix

Sie sind berechtigt, auf die FSLogix Profile Container, Office 365 Container, Application Masking und Java Redirection zuzugreifen, wenn Sie eine der folgenden Lizenzen besitzen:

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/ Student Use Benefits
- Microsoft 365 F1/F3
- Microsoft 365 Business
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA pro Benutzer
- Client-Zugriffslizenz (CAL) für Remotedesktopdienste (RDS)

- Abonnenten-Zugangslizenz (SAL) für Remotedesktopdienste (RDS)

FSLogix-Lösungen können in jedem öffentlichen oder privaten Rechenzentrum eingesetzt werden, solange der Benutzer über eine entsprechende Lizenz verfügt.

Weitere Informationen:

- Übersicht über FSLogix https://docs.microsoft.com/de-de/fslogix/overview.

Microsoft SQL-Server

SQL Server ist erforderlich, wenn Sie Parallels RAS Reporting verwenden. Die SQL Server-Installation kann auf Folgendem basieren:

- SQL Express, das zwar kostenlos ist, bei dem aber die Größe der Datenbank auf 10 GB begrenzt ist.
- SQL Server kommerzielle Edition Standard oder Enterprise, mit Core-basierten Lizenzen oder Server + CAL-basierten Lizenzen.

Weitere Informationen:

- Lizenzierungshandbuch für SQL Server 2019 https://download.microsoft.com/download/6/6/0/66078040-86d8-4f6e-b0c5-e9919bbcb537/SQL%20Server%202019%20Licensing%20guide.pdf

App-V

App-V wird nicht eigenständig lizenziert, sondern ist in anderen Lizenzverträgen wie Microsoft Volume Licensing, Windows Software Assurance Microsoft, Remote Desktop Services (RDS) CAL, als Teil eines umfassenderen Microsoft-Lizenzvertrags enthalten. Zum Beispiel kann mit einer RDS-CAL (entweder pro Benutzer oder pro Gerät) der App-V-Client auf dem RD-Sitzungshost verwendet werden, um App-V-Anwendungen bereitzustellen.

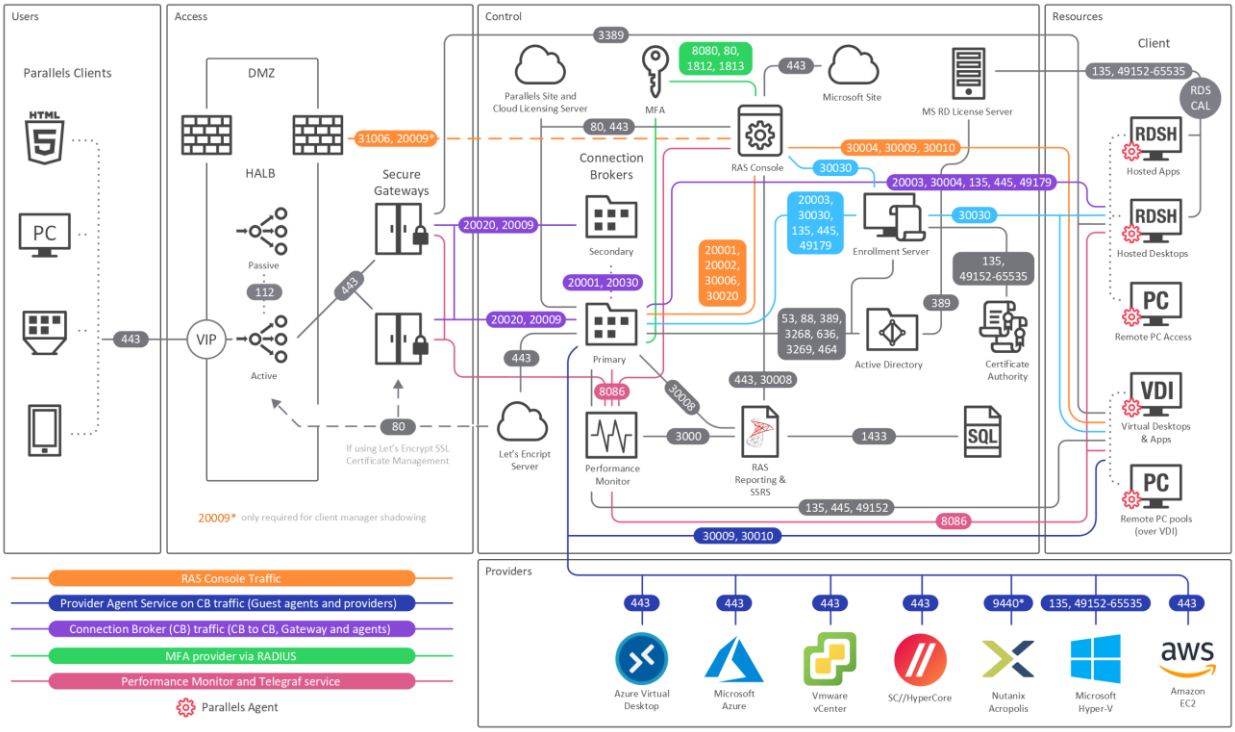
Für die korrekte Lizenzierung von App-V sollten Sie sich an einen Microsoft Partner (Lösungsanbieter) wenden, der sich mit Microsoft Volume Licensing auskennt (Liste der Microsoft Partner: https://www.microsoft.com/de-de/solution-providers/home?type=companies&competency=100010).

Andere Referenzen

Eine detaillierte Liste der Nutzungsbedingungen für die Microsoft-Volumenlizenzierung finden Sie unterhttps://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=PT&lang=German.

Port-Referenz

Die folgende Übersicht zeigt die in Parallels RAS verwendeten Kommunikationsports.



Die obige Übersicht enthält SAML SSO-Komponenten wie den RAS-RAS-Registrierungsserver, jedoch nicht den Mandantenmakler.

Tipp: Wenn Sie die PDF-Version dieses Leitfadens lesen, klicken Sie auf den folgenden Link, um das Diagramm in voller Größe in einem Webbrowser anzuzeigen: https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/index.htm#47092.

Parallels Client

Quelle	Ziel	Protokolle	Ports	Beschreibung
Parallels Client	HALB	TCP, UDP TCP, UDP	80, 443 20009	Verwaltung und Verbindungen von Benutzersitzungen. Device Manager Shadowing über Firewall (indirekte Netzwerkverbindung).

	RAS Secure Gateway im Weiterleitungsmodus	TCP, UDP TCP, UDP UDP	80, 443 3389 20000	Verwaltung und Verbindungen von Benutzersitzungen. Optional – Wird für die Benutzersitzung verwendet, wenn der RDP-Lastausgleich aktiviert ist (Standard-RDP). Secure Gateway Lookup Broadcast.
	RAS Secure Gateway im Normalmodus	TCP, UDP TCP, UDP TCP, UDP UDP	80, 443, 3389 20009 20000	Verwaltung und Verbindungen von Benutzersitzungen. Optional – Wird für die Benutzersitzung verwendet, wenn der RDP-Lastausgleich aktiviert ist (Standard-RDP). Device Manager Shadowing über Firewall (indirekte Netzwerkverbindung) Secure Gateway Lookup Broadcast
	Sitzungshost (VDI, RDS, RemotePC)	TCP, UDP	3389	Wird nur für Direktverbindungen von Benutzersitzungen verwendet. RDP-Verbindung ist immer verschlüsselt.
	Azure Virtual Desktop-Dienste	TCP UDP	443 3390	Azure Virtual Desktop Gateway-Verbindung Wird nur für Benutzersitzungsverbindungen im ShortPath-Modus verwendet.
	Microsoft-Website	TCP	443	Microsoft-Remotedesktopclient herunterladen
	Parallels-Website	TCP	80, 443	Nach Updates suchen und Parallels Client herunterladen

Internetbrowser

Quelle	Ziel	Protokolle	Ports	Beschreibung
Internetbrowser (HTML5) und Let's Encrypt-Dienst	RAS Web-Administrationsdienst [RAS-Verwaltungsportal]	TCP	20443	Zugriff von Administratoren auf HTML5-basiertes Verwaltungsportal der RAS-Umgebung
	HALB	TCP	80, 443	Zugriff für Endbenutzer auf Parallels RAS Web Client (auf Secure Gateway im Normalmodus) über HALB **Hinweis:** Die Ports 80 und 443 müssen für eingehende Anfragen geöffnet sein, wenn Sie Let's Encrypt verwenden.

	RAS Secure Gateway	TCP	80, 443	Zugriff für Endbenutzer auf Parallels RAS Web Client (auf Secure Gateway im Normalmodus) **Hinweis:** Die Ports 80 und 443 müssen für eingehende Anfragen geöffnet sein, wenn Sie Let's Encrypt verwenden.

HALB

Quelle	Ziel	Protokolle	Ports	Beschreibung
HALB	HALB	VRRP	112	HALB-zu-HALB-Kommunikation für die automatische Zuweisung von VIP an aktiven HALB.
	RAS Secure Gateway im Weiterleitungsmodus	TCP, UDP	80, 443	Verwaltung und Verbindungen von Benutzersitzungen.
	RAS Secure Gateway im Normalmodus	TCP, UDP TCP, UDP	80, 443 20009	Verwaltung und Verbindungen von Benutzersitzungen. Device Manager Shadowing über Firewall (indirekte Netzwerkverbindung).

RAS Secure Gateway

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS Secure Gateway im Weiterleitungsmodus	RAS Secure Gateway im Normalmodus	TCP, UDP TCP, UDP	80, 443 3389	Verwaltung und Verbindungen von Benutzersitzungen. Optional – wird für Benutzersitzung verwendet, wenn RDP-Lastverteilung aktiviert ist.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf-Dienst) sendet gesammelte Leistungsdaten an InfluxDB.
RAS Secure Gateway im Normalmodus	Remote-Desktop Services	TCP, UDP	3389	RDP-Verbindungen
	RAS Connection Broker	TCP TCP, UDP	20002 20009	RAS Connection Broker Service-Port (Kommunikation mit RAS Secure Gateways und der RAS-Konsole – nur im Normalmodus).

				Device Manager Shadowing über Firewall (indirekte Netzwerkverbindung), wenn RAS-Konsole auf RAS Connection Broker läuft
	RAS Performance Monitor	TCP	8086	Agent (Telegraf-Dienst) sendet gesammelte Leistungsdaten an InfluxDB.
	Localhost	TCP	20020	Kommunikation mit Nutzerportal-Webserver (NodeJS).

RAS Connection Broker

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS Connection Broker	AD DS-Controller	TCP TCP TCP, UDP UDP	389, 3268 636, 3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP	20001 20030	Redundanzdienst. Kommunikation zwischen Connection Brokern, die auf derselben Site laufen.
	Parallels-Lizenzierungsserver	TCP	443	RAS Connection Broker (primärer Connection Broker in der Lizenzierungssite) kommuniziert mit dem Parallels-Lizenzierungsserver (https://ras.parallels.com). Hinweis: Nicht erforderlich für RAS Connection Broker des Mandantenmaklers (siehe Abschnitt Mandantenmakler).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf-Dienst) sendet gesammelte Leistungsdaten an InfluxDB.
	RAS RD Session Host Agent	TCP, UDP	30004	Server für Connection Broker-Anfragen.
	RAS Provider Agent	TCP, UDP	30006	Provider Agent-Kommunikationsport.
	RAS Remote PC Agent	TCP, UDP	30004	Kommunikationsport für Remote PC Agent (Agent-Status, Zähler- und Sitzungsdaten)
	2FA Server	TCP, UDP	8080, 80 1812, 1813	Deepnet / Safenet Radius

RAS-Registrierungsserver	TCP	30030	RAS Connection Broker sendet Verbindungsanforderung an RAS-Registrierungsserver.
RAS-Berichterstellung	TCP	30008	Master-RAS Connection Broker kommuniziert mit RAS Reporting (auf demselben Host installiert wie SSRS).
RAS Remote Installer Service	TCP	30020	Remote Agent-Pushing
RAS RD Session Host Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS-Registrierungsserver	TCP	135, 445, 49179	Remote-Push-Installation/Übernahme von Software
SMTP	TCP	587	Notifdispatcher ist der Dienst, der die E-Mails über den in den Postfach-Einstellungen angegebenen Port versendet (+SSL/TLS)
Let's Encrypt-Dienst	TCP	80, 443	Kommunikation zwischen dem Let's Encrypt-Client (verfügbar im primären Connection Broker) und einem Let's Encrypt-Server.

RAS-Konsole

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS-Konsole	RAS-Berichterstellung	TCP	30008	Die RAS-Konsole ist mit dem primären RAS Connection Broker verbunden, der mit RAS Reporting (auf demselben Host installiert wie SSRS) kommuniziert. SSRS kommuniziert mit SQL über TCP 1433 (oder dynamisch, wenn 1433 in den Einstellungen nicht hergestellt wurde).
	SSRS	TCP	443	Abrufen von Berichten.
	HALB	TCP, UDP	31006	Wird für die Konfiguration verwendet.
	Parallels Client	TCP	50005	Shadowing von der RAS-Konsole bei einer Direktverbindung zum Netzwerk.
	RAS RD Session Host Agent	UDP, TCP	30004	Wird für die Aufgabe „Agent kontrollieren“ verwendet. Zur Verwaltung der Komponenten verwendet.
	RAS Guest Agent	TCP UDP	30009 30010	Wird für die Aufgabe „Agent kontrollieren“ verwendet. Zur Verwaltung der Komponenten verwendet.
	RAS Remote PC Agent	UDP, TCP	30004	Wird für die Aufgabe „Agent kontrollieren“ verwendet. Zur Verwaltung der Komponenten verwendet.
	RAS Provider Agent	UDP, TCP	30006	Wird für die Aufgabe „Agent kontrollieren“ verwendet. Zur Verwaltung der Komponente verwendet.
	MFA-Server(s)	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius
	Microsoft-Website	TCP	80, 443	Nach Updates suchen und Parallels Client herunterladen
	Parallels-Website	TCP	80	Nach Updates suchen und Parallels Client herunterladen
	RAS Performance Monitor	TCP	3000	RAS-Browser-Plugin-Verbindung zu Grafana.
	RAS Connection Broker	TCP	20002, 20001	Kommunikation mit Connection Broker und Redundanz.

	RAS-Registrierungsserver	TCP, UDP	30030	Wird für die Aufgabe „Agent kontrollieren“ verwendet. Wird zur Verwaltung der Komponenten und Fehlerbehebung verwendet.
	Wyse Broker	UDP	1234 (nur ausgehend) 68 (nur eingehend)	Wyse Broker Discovery Request Broadcast Packet (V_WYSEBCAST). Wyse Broker Discovery Reply Packet (V_WYSETEST).
	SMTP	TCP	587	RAS-Konsole kann Test-E-Mails über den in den Postfach-Einstellungen angegebenen Port versendet (+SSL/TLS)

SSRS

Quelle	Ziel	Protokolle	Ports	Beschreibung
SSRS	Microsoft SQL-Server	TCP	1433	RAS-Konsole ist mit RAS Reporting verbunden

RAS-Berichterstellung

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS Reporting Service	MS SQL	TCP	1433	Speicher von RAS-Aktivitätsinformationen
	SSRS	TCP	8085, 443	Auflistung von Berichten (inkl. benutzerdefinierter Berichte)

RAS Web-Administrationsdienst (REST/Verwaltungsportal)

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS Web-Administrationsdienst	RAS RD Session Host Agent	TCP	30004	Protokollabruf
	RAS Guest Agent	TCP	30010	Protokollabruf
	RAS Provider Agent	TCP	30006	Protokollabruf

	RAS Connection Broker	TCP	20002, 20001 30020	Kommunikation mit GA und Redundanz Wird bei der Veröffentlichung verwendet, um nach installierten Anwendungen zu suchen oder einzelne Dateien/Ordner zu durchsuchen. 30020 – Remote Agent Pushing (vor RAS 18).
	RAS RD Session Host Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS-Registrierungsserver	TCP	135, 445	Remote-Push-Installation/Übernahme von Software (vor RAS 18).
	RAS Reporting Service	TCP	3000	Integration von RAS Reporting in das iFrame-Management-Portal

RAS PowerShell

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS PowerShell	RAS RD Session Host Agent	TCP	30004	Protokollabruf
	RAS Guest Agent	TCP	30010	Protokollabruf
	RAS Remote PC Agent	TCP	30004	Protokollabruf
	RAS Provider Agent	TCP	30006	Protokollabruf
	RAS Connection Broker	TCP	20002, 20001	Kommunikation mit GA und Redundanz Wird bei der Veröffentlichung verwendet, um nach installierten Anwendungen zu suchen oder einzelne Dateien/Ordner zu durchsuchen.

RAS Provider Agent

Quelle	Ziel	Protokolle	Ports	Beschreibung

RAS Provider Agent	RAS Connection Broker	TCP	20003	Connection Broker-Kommunikationsport.
	RAS Guest Agent	TCP UDP	30010 30009	TCP wird zum Senden der Befehle verwendet. Beim ersten Handshake wird UDP verwendet.
	RAS Performance Monitor	TCP	8086	Der Agent (Telegraf-Dienst) sendet die gesammelten Leistungsdaten an InfluxDB – gilt nur für Hyper-V.
	Hyper-V	TCP	135, 49152-65535	Wird verwendet, um zu prüfen, ob der Host eingeschaltet ist, und um Befehle zum Exportieren, Importieren, Löschen, Herunterfahren, Neustarten oder Anhalten zu senden.
	Nutanix AHV (AOS)	TCP	9440	Wird verwendet, um zu prüfen, ob der Host eingeschaltet ist. Sendet außerdem Befehle zum Klonen, Löschen, Herunterfahren und Neustarten (RestAPI-Aufrufe, PoSH, Remote ncli).
	VMWare	TCP	443	Wird verwendet, um zu prüfen, ob der Host eingeschaltet ist. Sendet außerdem Befehle zum Klonen, Löschen, Herunterfahren, Neustarten und Anhalten.
	Microsoft Azure	TCP	443	Wird verwendet, um zu prüfen, ob der Gast eingeschaltet ist. Sendet außerdem Befehle zum Klonen, Herunterfahren und Neustarten (über REST).
	Azure Virtual Desktop	TCP	443	Wird verwendet, um zu prüfen, ob der Host eingeschaltet ist. Sendet außerdem Befehle zum Klonen, Herunterfahren und Neustarten (über REST).
	AWS	TCP	443	Wird verwendet, um zu prüfen, ob der Host eingeschaltet ist. Sendet außerdem Befehle zum Klonen, Herunterfahren und Neustarten (über REST).
	Scale	TCP	443	Wird verwendet, um zu prüfen, ob der Host eingeschaltet ist. Sendet außerdem Befehle zum Klonen, Herunterfahren und Neustarten (über REST).
	Remote-PC über VDI	TCP	135, 49152-65535	Wird verwendet, um zu prüfen, ob der Host eingeschaltet ist. Sendet außerdem Befehle zum Herunterfahren, Neustarten oder Anhalten.

RAS-Registrierungsserver

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS-Registrierungsserver	AD DS-Controller	TCP TCP TCP, UDP UDP	389, 3268 636, 3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP UDP	20003 20003	Synchronisation von Einstellungen und Leistungsindikatoren. Verbindungsanforderung ablehnen
	Zertifizierungsstelle (CA)	TCP TCP	135 Dynamikbereich 49152 – 65535	DCOM/RPC-Ports

RAS RD Session Host Agent

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS RD Session Host Agent	RAS Connection Broker	TCP, UDP	20003	Wird zur Kommunikation mit RAS Connection Brokers. verwendet.
	Localhost	TCP	30005	Für interne Befehle (memshell, printer, redirector).
	FSlogix	TCP	443	FSlogix-Installationsprogramm herunterladen
	RAS Performance Monitor	TCP	8086	Agent (Telegraf-Dienst) sendet gesammelte Leistungsdaten an InfluxDB.
	RAS-Registrierungsserver	TCP	30030	RAS RD Session Host Agent (PrlsSCDriver) stellt eine Verbindung her, um die Anmeldeinformationen zu beziehen.

RAS Guest Agent

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS Guest Agent (wird von Azure Virtual Desktop verwendet)	Provider Agent	TCP, UDP	30006	Kommunikation mit Provider Agent Subnetz-Broadcast wird gesendet, um Provider Agent zu finden.

				Regelmäßige UDP-Takte
	Localhost	TCP	30005	Für interne Befehle – memshell, printer, redirector.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf-Dienst) sendet gesammelte Leistungsdaten an InfluxDB.
	RAS-Registrierungsserver	TCP	30030	RAS Guest Agent (PrlsSCDriver) stellt eine Verbindung her, um die Anmeldeinformationen zu beziehen.
	FSlogix	TCP	443	FSlogix-Installationsprogramm herunterladen

RAS Remote PC Agent

Quelle	Ziel	Protokolle	Ports	Beschreibung
RAS Remote PC Agent	RAS Connection Broker	TCP, UDP	20003	Wird zur Kommunikation mit RAS Connection Brokers. verwendet.
	Localhost	TCP	30005	Für interne Befehle – memshell, printer, redirector.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf-Dienst) sendet gesammelte Leistungsdaten an InfluxDB.
	RAS-Registrierungsserver	TCP, UDP	30030	RAS Remote PC (PrlsSCDriver) stellt eine Verbindung her, um die Anmeldeinformationen zu beziehen.
	FSlogix	TCP	443	FSlogix-Installationsprogramm herunterladen

Mandantenmakler

Quelle	Ziel	Protokolle	Ports	Beschreibung
Mandant – RAS Connection Broker	Broker des Mandanten – RAS Connection Broker	TCP	20003	Der RAS Connection Broker des Mandanten kommuniziert mit dem Mandantenmakler, um eine Verbindung zum Mandantenmakler herzustellen, Konfiguration und Status zu synchronisieren

Ports für Active Directory und Domain Services

Informationen zu Portanforderungen für Active Directory und Active Directory Domain Services finden Sie in diesem Artikel: https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx.

Azure Virtual Desktop

Die virtuellen Azure-Maschinen, die Sie für Azure Virtual Desktop erstellen, müssen Zugriff auf die folgenden URL in der kommerziellen Azure-Cloud haben:

Lösung für	Ausgehender TCP-Port	Zweck	Dienst-Tag
*.wvd.microsoft.com	443	Dienstverkehr	AzureVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	Agent-Verkehr	AzureCloud
production.diagnostics.monitoring.core.windows.net	443	Agent-Verkehr	AzureCloud
*xt.blob.core.windows.net	443	Agent-Verkehr	AzureCloud
*eh.servicebus.windows.net	443	Agent-Verkehr	AzureCloud
*xt.table.core.windows.net	443	Agent-Verkehr	AzureCloud
*xt.queue.core.windows.net	443	Agent-Verkehr	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows-Aktivierung	Internet
mrsglobalsteus2prod.blob.core.windows.net	443	Aktualisierungen von Agent und SXS-Stack	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Support für Azure-Portal	AzureCloud
169.254.169.254	80	Endpunkt Azure-Instanz-Metadaten-Dienst	k. A.
168.63.129,16	80	Zustandsüberwachung des Hosts	k. A.
https://download.parallels.com/ras/Configuration_01-20-2022.zip	443	Den Host einem Hostpool zuweisen.	AzureVirtualDesktop

In der folgenden Tabelle sind optionale URLs aufgeführt, auf die Ihre virtuellen Azure-Maschinen Zugriff haben können:

Lösung für	Ausgehender	Zweck	Azure Gov

	TCP-Port		
*.microsoftonline.com	443	Authentifizierung für Microsoft Online-Dienste	login.microsoftonline.us
*.events.data.microsoft.com	443	Telemetriedienst	Keinen
www.msftconnecttest.com	443	Ermittelt, ob das Betriebssystem mit dem Internet verbunden ist	Keinen
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	Keinen
login.windows.net	443	Anmelden bei Microsoft Online-Diensten, Microsoft 365	login.microsoftonline.us
*.sfx.ms	443	Aktualisierungen für OneDrive-Client-Software	oneclient.sfx.ms
*.digicert.com	443	Überprüfung des Zertifikatswiderrufs	Keinen
*.azure-dns.com	443	Azure-DNS-Auflösung	Keinen
*.azure-dns.net	443	Azure-DNS-Auflösung	Keinen

Für aktuelle Informationen besuchen Sie bitte auch die Microsoft-Website unter https://docs.microsoft.com/de-de/azure/virtual-desktop/safe-url-list#required-url-check-tool.

RAS-Leistungsindikatoren

Die folgende Tabelle listet die in Parallels RAS verfügbaren Leistungsindikatoren pro Komponente auf:

Parallels RAS Gateway (2XProxyGateway.exe)

ID	Name	Beschreibung
ras_gw_tot_conn	Gesamtzahl der Verbindungen	Gesamtzahl der Verbindungen mit dem Gateway
ras_gw_tot_threads	Gesamtzahl der Threads	Die Gesamtzahl der Threads, die auf dem Gateway laufen
ras_gw_rpd_sess	Getunnelte RDP-Sitzungen	Die Anzahl der getunnelten RDP-Sitzungen
ras_gw_rpd_sess_s	Getunnelte RDP-SSL-Sitzungen	Die Anzahl der getunnelten RDP-Sitzungen über SSL
ras_gw_html	HTTP-Verbindungen	Die Anzahl der getunnelten HTTP-Sockets
ras_gw_html_s	HTTPS-Verbindungen	Die Anzahl der getunnelten HTTPS-Sockets
ras_gw_html5	HTML5-Verbindungen	Die Anzahl der getunnelten HTTP5-Sockets

ras_gw_html5_s	HTML5-SSL-Verbindungen	Die Anzahl der getunnelten HTTP5-Sockets über SSL
ras_gw_cm	Geräte-Manager-Verbindungen	Die Anzahl der Parallels Geräte-Manager-Verbindungen
ras_gw_cm_s	Geräte-Manager-SSL-Verbindungen	Die Anzahl der Parallels Geräte-Manager-Verbindungen über SSL
ras_gw_wyse	Wyse-Verbindungen	Die Anzahl der Wyse-Verbindungen
ras_gw_wyse_s	Wyse-SSL-Verbindungen	Die Anzahl der Wyse-SSL-Verbindungen
ras_gw_rdpudp	Getunnelte RDP-UDP-Sitzungen	Die Anzahl der RDP-UDP-Verbindungen
ras_gw_rdpudp_s	Getunnelte RDP-UDP-DTLS-Sitzungen	Die Anzahl der RDP-UDP-Verbindungen über DTLS
ras_gw_cache_sock	Sockets mit Cache	Die Anzahl der Sockets mit Cache zwischen Gateway und Connection Broker
ras_gw_idle_threads	Threads im Leerlauf	Die Anzahl der Threads im Leerlauf auf dem Gateway
ras_gw_client	Client-Verbindungen	Die Anzahl der Parallels Client-Verbindungen
ras_gw_client_s	Client-SSL-Verbindungen	Die Anzahl der Parallels Client-Verbindungen über SSL

Parallels RAS Connection Broker (2XController.exe)

ID	Name	Beschreibung
ras_pa_avg_client_connection_time	Durchschnittliche Zeit für die Client-Verbindung	Die durchschnittliche Client-Verbindungszeit
ras_pa_avg_client_auth_time	Durchschnittliche Zeit für die Benutzerauthentifizierung	Die durchschnittliche Zeit, die benötigt wird, um einen Benutzer zu authentifizieren
ras_pa_avg_client_policy_time	Durchschnittliche Zeit zum Abrufen der Benutzerrichtlinie	Die durchschnittliche Zeit, die benötigt wird, um die Richtlinie des Benutzers abzurufen
ras_pa_avg_client_rep_time	Durchschnittliche Zeit zum Senden der Client-Telemetrie	Die durchschnittliche Zeit, die benötigt wird, um die Client-Telemetrie zu senden Wird von CEP verwendet.
ras_pa_avg_client_applist_time	Durchschnittliche Zeit zum Abrufen der veröffentlichten Elemente des Benutzers	Die durchschnittliche Zeit, die benötigt wird, um die Liste der veröffentlichten Elemente des Benutzers abzurufen
ras_pa_avg_client_appicons_time	Durchschnittliche Zeit zum Abrufen von Symbolen	Die durchschnittliche Zeit, die benötigt wird, um die Richtlinie des Benutzers abzurufen

ras_pa_avg_client_getidle_time	Durchschnittliche Zeit zum Starten einer Anforderung	Die durchschnittliche Zeit, die zum Starten einer Anforderung benötigt wird.

Parallels RAS RDS Agent (2XAgent.exe)

ID	Name	Beschreibung
act_sess	Aktive RDS-Sitzungen	Die Anzahl der aktiven RDS-Sitzungen.
disc_sess	Getrennte RDS-Sitzungen	Die Anzahl der getrennten RDS-Sitzungen.

Index

A

Administratoren - 19

Agent-Einstellungen - 46

Aktive Sitzungen (Active Sessions) - 55

Allgemein - 46, 69

Anbieter - 91

Anhang - 127

Anmelden beim RAS-Verwaltungsportal - 12

Anzeigen von Leistungskennzahlen - 121

Arbeiten mit Let's Encrypt-Zertifikaten - 63

Azure Virtual Desktop - 144

B

Benutzeroberfläche des RAS-Verwaltungsportals - 14

Benutzerprofil - 51

Benutzersitzungen - 98

Bevorzugtes Routing konfigurieren - 115

C

Client- und Server-Konfiguration - 74

Connection Brokers - 85

D

Desktopzugriff - 51

Drucken und scannen - 52

E

Ein Zertifikat aus einer Datei importieren - 65

Ein Zertifikat für Gateways und HALB zuweisen - 66

Einführung - 7

Erste Schritte mit dem RAS-Verwaltungsportal - 12

Erstellen eines selbstsignierten Zertifikats - 61

Exportieren eines Zertifikats in eine Datei - 65

F

Farm-Einstellungen - 19

FSLogix-Profilcontainer - 32

G

Gateway hinzufügen - 68

Gateway konfigurieren - 69

Gateways - 67

Gateways verwalten - 84

Generieren einer Zertifikatsignaturanforderung (CSR) - 62

H

HALB - 135

Hilfe und Support - 126

I

Infrastruktur - 43

Installation - 10

Installation und Konfiguration - 10

Installieren von RAS Performance Monitor - 119

Internetbrowser - 134

K

Konfiguration von MFA-Regeln - 30

Konfigurieren der Sicherheit für RAS Performance Monitor - 123

Konfigurieren eines RAS Connection Brokers - 85

Konfigurieren eines RD-Sitzungshosts - 45

L

Laufende Prozesse - 56

Laufende Ressourcen - 56, 99

Let's Encrypt-Zertifikate - 63

Lizenzierung - 20

M

Mailbox - 20

Mandantenmakler - 143

Microsoft-Lizenzanforderungen in Parallels RAS - 127

Modus - 70

Multifaktor-Authentifizierung - 25

N

Netzwerk - 71

Neue Funktionen - 8

Nutzerportal - 76

P

Parallels Client - 133

Parallels RAS 19-Versionsverlauf - 7

Port-Referenz - 133

Ports für Active Directory und Domain Services - 144

Problembehandlung - 57

R

RAS Connection Broker - 136

RAS Connection Broker verwalten - 90

RAS Guest Agent - 142

RAS PowerShell - 140

RAS Provider Agent - 140

RAS RD Session Host Agent - 142

RAS Remote PC Agent - 143

RAS Secure Gateway - 135

RAS Web-Administrationsdienst (REST/Verwaltungsportal) - 139

RAS Web-Administrationsdienst konfigurieren - 12

RAS-Agents aktualisieren - 125

RAS-Berichterstellung - 139

RAS-Konsole - 138

RAS-Leistungsindikatoren - 145

RAS-Registrierungsserver - 142

RDSH-Gruppen - 58

RD-Sitzungshost hinzufügen - 43

RD-Sitzungshosts - 43

S

Sekundären Connection Broker hinzufügen - 87

Sicherheit - 83

Site-Einstellungen - 23

Site-Kategorie - 18

Site-Standardeinstellungen und Hosts für FSLogix konfigurieren - 36

Sitzungen - 93

Sitzungsinformationen - 93

SSL/TLS - 72

SSRS - 139

Standardeinstellungen der Site - 92

Standardeinstellungen der Site (Publishing) - 112

U

Überblick - 7, 53, 93, 118

Überwachung - 118

Überwachung im RAS-Verwaltungsportal aktivieren - 120

Universal Scanning - 40

Universelles Drucken - 37

V

Verbinden und Authentifizierung - 23

Veröffentlichen einer Anwendung - 102

Veröffentlichen eines Desktops - 103

Veröffentlichen eines Dokuments - 105

Veröffentlichen eines Ordners im Dateisystem - 105

Veröffentlichung - 101

Verwalten eines RD-Sitzungshosts - 53

Verwalten veröffentlichter Anwendungen - 107

Verwalten veröffentlichter Desktops - 109

Verwalten veröffentlichter Ressourcen - 106

Verwalten von Ordnern - 110

Verwaltung bestehender Profile durch Parallels RAS konfigurieren - 34

Verwenden von Filterregeln - 114

Verwenden von Google Authenticator - 28

Verwenden von RADIUS - 26

Verwendung von Standardwerten für Sites oder Hostpools - 45

Virtual Desktop-Infrastruktur - 59

Voraussetzungen - 10

W

Web - 80

Wie Parallels RAS Zertifikate von Let's Encrypt anfordert - 64

Wyse - 83

Z

Zertifikate - 60