# || Parallels<sup>®</sup>

## Parallels RAS Front-End Load Balancing using AWS Elastic Load Balancing (NLB and ALB)

• Parallels Remote Application Server

The below guide is a step-by-step configuration guide for deploying AWS Elastic load balancing (ELB) to front-end and load-balance Parallels RAS Environment.

# **Prerequisites and Assumptions**

It is assumed that reader has a basic understanding of both AWS ELB solutions (Application Load Balancer (ALB)/Network Load Balancer (NLB)) and Parallels RAS. This guide will focus on the configuration of AWS ELB and Parallels Secure Client Gateways load balancing. It is assumed that Parallels RAS environment have already been deployed and configured on EC2 instances with 443 Inbound rule on the Parallels Secure Client Gateways security groups.

*Note:* Steps 1-5 focusing on AWS NLB configuration that will allow connectivity from native Parallels Clients. Should you need to configure load balancing for HTML5 clients only or in addition to the native Parallels Clients, please also review the configuration at Step 6.

More information AWS Elastic Load Balancing available here: <u>https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-load-balancing.html</u>

### **Document process flow**

The process that will be discussed in more detail is as illustrated below:

- 1. Configure your Target Group.
- 2. Configure Target Group attributes.
- 3. Choose the Load Balancer type.
- 4. Configure Load Balancer and Listener.
- 5. Test and Evaluate Load Balancing.
- 6. Using Network Load Balancer Access feature

# Step 1: Configure your Target Group

Create a target group, which is used in request routing. The rule for your listener routes requests to the registered targets in this target group. The load balancer checks the health of targets in this target group using the health check settings defined for the target group.

### To configure your target group

- 1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
- 2. In the navigation pane, under Load Balancing, choose Target Groups.
- 3. Choose Create target group.
- 4. Keep Target type as instance.

Step 1 Specify group details	Specify group details
	Your load balancer routes requests to the targets in a target group and performs health checks on the targets
Step 2 Register targets	<b>Basic configuration</b> Settings in this section cannot be changed after the target group is created.
	Choose a target type
	<ul> <li>Instances</li> <li>Supports load balancing to instances within a specific VPC.</li> </ul>
	<ul> <li>IP addresses</li> <li>Supports load balancing to VPC and on-premises resources.</li> <li>Facilitates routing to multiple IP addresses and network interfaces on the same instance.</li> <li>Offers flexibility with microservice based architectures, simplifying inter-application communication.</li> </ul>
	<ul> <li>Lambda function</li> <li>Facilitates routing to a single Lambda function.</li> <li>Accessible to Application Load Balancers only.</li> </ul>
	<ul> <li>Application Load Balancer</li> <li>Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.</li> <li>Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.</li> </ul>

- 5. For **Target group name**, enter a name for the new target group.
- 6. Set Protocol as **TCP**, and Port as **443**.
- 7. Select the **VPC** containing your instances.
- 8. For Health checks, keep the default settings.
- 9. Choose Next.

SD IG ICSC	
maximum of 32 a	phanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.
rotocol	Port
тср 🔻	443
PC	the instances that you want to include in the target group
SB-VPC	the instances that you want to include in the target group.
vpc-0	▼
IPV4:	
e associated loac	balancer periodically sends requests, per the settings below, to the registered targets to test their status.
ealth check pro	balancer periodically sends requests, per the settings below, to the registered targets to test their status.
he associated load lealth check pro TCP Advanced he	balancer periodically sends requests, per the settings below, to the registered targets to test their status.
Health check pro	balancer periodically sends requests, per the settings below, to the registered targets to test their status. tocol alth check settings
ealth check pro TCP Advanced he Tags - opti Consider adding	balancer periodically sends requests, per the settings below, to the registered targets to test their status. tocol alth check settings onal tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

10. On the **Register targets** page, complete the following steps. This is an optional step to create a target group. However, you must register your targets if you want to test your load balancer and ensure that it is routing traffic to your targets.

- 1. For **Available instances**, select one or more instances.
- 2. Keep the default port **443**, and choose **Include as pending below**.

Step 1 Specify group details	Register targets This is an optional step to create a target g	group. However, to ensure that your load	balancer routes traffic to t	his target group you must regis
Register targets	Available instances (2) Q Filter resources by property or value	ie		
	Instance ID		⊽ State	▽ Security groups
	- i-(	SB-AWS-RAS1	⊘ running	SBSecGroup, launo
	- i-	SB-AWS-RAS2	⊘ running	SBSecGroup
				0 selected
			Ports for Ports for	r the selected instances routing traffic to the selected instance
			443	
			1-65535 (	separate multiple ports with comma
			l	nclude as pending below
			2 selections are now pend	ing below. Include more or register ta

11. Click on **Create target group**.

Targets (	2)						
All	▼ Q Filter re	sources by property or va	ilue				
Remove	Health status	Instance ID	$\nabla$	Name $\bigtriangledown$	Port 🛡	State 🗢	Security groups
×	Pending	ŀ		SB-AWS-RAS2	443	⊘ running	SBSecGroup
						•	

# Step 2: Configure Target Group attributes

Once target group created successfully, open AWS navigation pane and go to Target groups. Choose the Target group created in Step 1 above > Actions > Edit attributes.

EC2 >	Target groups					
Targ	<b>Jet groups (1/6)</b> Info					
-	Name $\bigtriangledown$	ARN 🗢	Port 🗢	Protocol 🗢	Target type	
	NewTG1	🗇 arn:aws:elasticloadbalancin	443	HTTPS	Instance	
	NewTG3	🗗 arn:aws:elasticloadbalancin	443	тср	Instance	
	SB-TG-1	🗗 arn:aws:elasticloadbalancin	443	HTTPS	Instance	
	SB-TG-2	🗗 arn:aws:elasticloadbalancin	443	тср	Instance	
	SB-TG-Test	🗗 arn:aws:elasticloadbalancin	443	ТСР	Instance	
	SB-TG3-HTTPS	🗇 arn:aws:elasticloadbalancin	8443	HTTPS	Instance	

Edit the **Deregistration delay** from default 300 to 0 and click **Save Changes**.

### **Edit attributes**

	25	Restore defaults
Deregistrati	ion delay vait for in-flight requests to complete while deregistering a target. During this time, the state of	the target is draining.
0	seconds	
-3600		
Connect	<b>tion termination on deregistration —</b> <i>recommended</i> d, your Network Load Balancer will terminate active connections when deregistration delay is re	ached.
Stickine The type client's se	<b>ISS</b> of stickiness associated with this target group. If enabled, the load balancer binds a ession to a specific instance within the target group.	
Proxy p Before yo applicatio	<b>rotocol v2</b> ou enable proxy protocol v2, make sure that your application targets can process proxy protocol on might break.	headers otherwise your
Preserve	e client IP addresses client IP addresses and ports in the packets forwarded to targets.	

Please see here for more information regarding deregistration delay.

### Step 3: Choosing the Load Balancer Type

A load balancer serves as the single point of contact for clients. The load balancer distributes incoming traffic across multiple targets, such as Amazon EC2 instances acting as Parallels RAS Secure Client Gateways.

Elastic Load Balancing supports the following types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers and Classic Load Balancers (will be retired on August 15th, 2022).

For native Parallels Clients connectivity the Network Load Balancer can be used.



For more information on AWS Network Load Balancer please check this article

# **Step 4: Configure Load Balancer and Listener**

	Basic Configuration	
1	Name	Provide a significant name for your load balancer
	Scheme	Internet-facing
2	Network Mappings	
2	Select the appropriate VPC and choose the availabil	ity zones where your instances reside in
	Listeners and routing	
3	Protocol	ТСР
3	Port	443 (or an alternate port in case AWS ALB used for HTML5 clients. See <b>Step 6</b> below)
	Default action	Select the target group created and registered in Step 1

1. For Load balancer name, enter a name for your load balancer. For example, MY-AWS-NLB

- 2. For Scheme and IP address type, keep the default values.
- 3. For **Network mappings**, select the **VPC** that you used for your EC2 instances. For each Availability Zone that you used to launch your EC2 instances, select the Availability Zone and then select one public subnet for that Availability Zone.

By default, AWS assigns an IPv4 address to each load balancer node from the subnet for its Availability Zone. Alternatively, when you create an internet-facing load balancer, you can select an Elastic IP address for each Availability Zone. This provides your load balancer with static IP addresses.

- 4. For Listeners and routing, keep the default, which is a listener that accepts TCP traffic on port 443.
- 5. For Default action, select the target group that you created and registered in step 1.
- 6. (Optional) Add a tag to categorize your load balancer. Tag keys must be unique for each load balancer.
- 7. Review your configuration, and choose Create load balancer. A few default attributes are applied to your load balancer during creation. You can view and edit them after creating the load balancer. For more information, see Load balancer attributes.

#### **Basic configuration**

#### Load balancer name

Name must be unique within your AWS account and cannot be changed after the load balancer is created.

#### SB-AWS-NLB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

#### Scheme

Scheme cannot be changed after the load balancer is created.

#### Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more 🗹

#### Internal

An internal load balancer routes requests from clients to targets using private IP addresses.

#### IP address type Info

Select the type of IP addresses that your subnets use.

#### IPv4

Recommended for internal load balancers.

#### Dualstack

Includes IPv4 and IPv6 addresses.

### Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

#### VPC

Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is confirm the VPC for your targets, view your target groups 2.

C	D	٧/	D	r
	n-	• •	~	ι.

vpc-071d6e1781f75d822 IPv4: 10.0.0.0/16

	С	

T

#### Mappings

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported balancer or the VPC are not available for selection. Subnets cannot be removed after the load balancer is created, but additional subnets can be added.

✔ us-east-1a	
✓ us-east-1e	
Subnet	
subnet-0ebd06f34a93f3331	MySubnet 🔻
IPv4 settings	
IPv4 address	
Assigned by AWS	

#### Listeners and routing Info

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification.

Protocol	Port	Default action Info	
TCP 🔻	: 443	Forward to SB-TG-Test Target type: Instance, IPv4	тср 🖉 📿
	1-03333	Create target group 🔀	,

• IPv4	<ul> <li>us-east-1e</li> <li>subnet-0ebd06f34a93f3331 MySubnet</li> </ul>	Surrest 💽	
Attributes			

# Step 5: Test and Evaluate Load Balancing

You can test Load balancer configuration by taking note and copying the DNS name given to the Load balancer as shown from Load balancers – Description – Basic configuration

Load balancer: SB-AWS-NLB		
Description Listeners Moni	toring Integrated services	Tags
Basic Configuration		
Name	SB-AWS-NLB	
ARN	arn:aws:elasticloadbalancing:	
DNS name	SB-AWS-NLB- (A Record)	aws.com 省
State	Active	
Туре	network	
Scheme	internet-facing	

Log on from Parallels Client and confirm application launching:

• • • Parallels Client	- AWS NLB <   > ^ [] =	∃ 📰 Ĉ Q~ All Connections
✓ CONNECTIONS	Name	Description
	Calculator	Performs basic arithmetic tasks with a
	🥥 Notepad	Creates and edits text files using basic
	🛷 Paint	Create and edit drawings.
	Mordpad 🔤	Creates and edits text documents with
	📀 Microsoft Edge	Browse the web
AWS NLB		

# Step 6: Using "Network Load Balancer Access" feature

The aforementioned configuration enables support for native Parallels Clients, but connections over HTML5 client using a web browser will fail as TCP does not support stickiness. The Network Load Balancers access feature is intended for deployment scenarios where third-party front-end load balancers such as Amazon Web Services (AWS) Elastic Load Balancers (ELBs) are used. It allows you to configure an alternate hostname and port number to be used by the Network Load Balancer (NLB). This is needed to separate hostnames and ports on which TCP and HTTPS communications are carried out because AWS load balancers don't support both specific protocols over the same port.

When one need to utilize both, native Parallels and HTML5 connections, in addition to AWS NLB, AWS ALB needs to be deployed.

In this case, below please find the recommended configuration:

### **Parallels RAS Console**

1. In RAS Console > Gateways > right-click on the required Gateway Agent > Properties > HTML5 tab (one can also apply this configuration to all RAS gateways within the site by modifying the Site defaults):

2. In the Network load balancer section do the following:

- Check **Use alternate port** and specify an alternate port number (in our example, port 8443). The port must not be used by any other component in the RAS Farm or Site. When the alternate port is enabled, all native Parallels Clients will use this port to connect to the RAS Farm or Site.
- Check **Use alternate hostname** and specify the hostname of your AWS NLB (When the alternate hostname is enabled, all platform-specific Parallels Clients will use this hostname to connect to the RAS Farm or Site)

AWSSB1.RAS.LAB Properties ?	$\times$				
Site Default Properties ?	×				
Mode Network SSL/TLS HTML5 Wyse Security Web					
Configure the following settings:					
Enable HTML5 Client					
Client					
Launch sessions using: Launch apps with Parallels Client & Fallback to HTML5	$\sim$				
Allow user to select a launch method Allow opening applications in a new tab					
<ul> <li>Use Pre Windows 2000 login format</li> <li>Allow embedding of Parallels HTML5 Client into other web pages</li> <li>Allow file transfer command</li> <li>Allow clipboard command</li> <li>Allow cross-origin resource sharing</li> </ul>					
Configure					
Network Load Balancer access					
Use alternate hostname: SB-AWS-NLB- amazon	aws.(				
Use alternate port: 8443 Default					
OK Cancel H	elp				

Check this article for more information

*Note:* using an alternate host or port is not suitable in a multi-tenant environment as Tenant Broker RAS Secure Client Gateways are shared between Tenants, which would require different configurations. 3. Switch to the **Web tab** and set the web cookie as **AWSALB** 

awssb2.ras.lab Properties	?	$\times$
Site Default Properties	?	×
Mode Network SSL/TLS HTML5 Wyse Security Web		
Configure the following settings:		
Default URL		
Use the default HTML5 Client URL (if it is enabled in the HTML5 tab) or specify custom URL if you use a different web server for web requests.	a	
Default URL: https://%hostname%/RASHTML5Gateway	Defaul	t
Web cookie		
If your network load balancer requires a specific web cookie you can change t standard web cookie name used by RAS.	he	
If your network load balancer requires a specific web cookie you can change t standard web cookie name used by RAS. Web cookie: AWSALB	the Defaul	t
If your network load balancer requires a specific web cookie you can change to standard web cookie name used by RAS. Web cookie: AWSALB	Defaul	t
If your network load balancer requires a specific web cookie you can change t standard web cookie name used by RAS. Web cookie: AWSALB	Defaul	t
If your network load balancer requires a specific web cookie you can change t standard web cookie name used by RAS. Web cookie: AWSALB	Defaul	t
If your network load balancer requires a specific web cookie you can change t standard web cookie name used by RAS. Web cookie: AWSALB	Defaul	t
If your network load balancer requires a specific web cookie you can change t standard web cookie name used by RAS. Web cookie: AWSALB	Defaul	t
If your network load balancer requires a specific web cookie you can change t standard web cookie name used by RAS. Web cookie: AWSALB	Defaul	t

*Note:* When a load balancer first receives a request from a client, it routes the request to a target and generates a cookie named AWSALB, which encodes information about the selected target. The load balancer then encrypts the cookie and includes it in the response to the client. When sticky sessions are enabled, the load balancer uses the cookie received from the client to route the traffic to the same target, assuming the target is registered successfully and is considered healthy. By default, Parallels RAS uses its own ASP.NET cookie named \_SessionId, however in this case you must customize the cookie specifying the mentioned AWS cookie for sticky sessions. This can be configured using the Web cookie field on the Web Requests tab. Please note that this functionality is available in Parallels RAS 17.1 or newer.

### **AWS Application Load Balancer**

Configure AWS Application Load Balancer (ALB) as described here: <u>https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancer-getting-started.html</u>

For AWS ALB Listener we suggest the following configuration:

Protocol: HTTPS Port: 443

Add the required target group(s), specify the security settings and click Save Changes

EC2 > Load balancers > SB-AWS-ALB : Edit listener

# Edit listener

arn:aws:elasticloadbalancing:us-east-

### Listener details

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification. You can specify multiple rules and multiple certificates per listener after the load balancer is created.

Protocol	Port	
HTTPS 🔻	:	443
	, 	1-65535

#### Default actions Info

Specify the default actions for traffic on this listener. Default actions apply to traffic that does not meet the conditions of rules on your listener. Rules can be configured after the listener is created.

Target group	C	Weight (0-99	99)
SB-TG-1 Target type: Instance, IPv4	HTTPS 🔻	1	×
	Traffic distribution:	100%	
Select a target group	•	0	×
Create target group 🗹			

Secure listener settings Info
<b>Security policy</b> Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration, known as a security policy, to negotiate SSL connections with clients.
ELBSecurityPolicy-2016-08
Compare security policies 🔀
<b>Default SSL certificate</b> The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can add more certificates after you create the load balancer.
From ACM  AWSSB1.RAS.LAB
Request new ACM certificate 🖸

Cancel

Target Group settings for AWS Application Load Balancer:

- Target type: Instance
- Protocol **HTTPS**
- Port **443**

Ensure you have enabled session stickiness for the target group associated with your AWS ALB:

Deregistration delay The time to wait for in-flight requests to complete while deregistering a target. During this time, the state of the ta  o seconds D-3600 Slow start duration During this period, a newly registered target receives an increasing share of requests, until it reaches its fair share.  o seconds Requires 30 to 900 seconds to enable, or 0 seconds to disable. This attribute cannot be combined with the Least ou algorithm.  Load balancing algorithm Determines how the load balancer selects targets from this target group when routing requests.  Round robin Least outstanding requests Cannot be combined with the Slow start duration attribute.  Stickiness The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.	get is draining. standing requests
<ul> <li>Ine time to wait for in-fught requests to complete while deregistering a target. During this time, the state of the ta</li> <li>o seconds</li> <li>During this period, a newly registered target receives an increasing share of requests, until it reaches its fair share.</li> <li>o seconds</li> <li>Requires 30 to 900 seconds to enable, or 0 seconds to disable. This attribute cannot be combined with the Least ou algorithm.</li> <li>Load balancing algorithm</li> <li>Determines how the load balancer selects targets from this target group when routing requests.</li> <li>Round robin</li> <li>Least outstanding requests</li> <li>Cannot be combined with the Slow start duration attribute.</li> <li>Stickiness</li> <li>The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.</li> </ul>	get is draining. standing requests
<ul> <li>Seconds</li> <li>Seconds</li> <li>Seconds</li> <li>Requires 30 to 900 seconds to enable, or 0 seconds to disable. This attribute cannot be combined with the Least ou algorithm.</li> <li>Least outstanding requests</li> <li>Cannot be combined with the Slow start duration attribute.</li> <li>Stickiness</li> <li>The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.</li> </ul>	standing requests
<ul> <li>Slow start duration</li> <li>During this period, a newly registered target receives an increasing share of requests, until it reaches its fair share.</li> <li>0 seconds</li> <li>Requires 30 to 900 seconds to enable, or 0 seconds to disable. This attribute cannot be combined with the Least ou algorithm.</li> <li>Load balancing algorithm</li> <li>Determines how the load balancer selects targets from this target group when routing requests.</li> <li>Round robin</li> <li>Least outstanding requests Cannot be combined with the Slow start duration attribute.</li> <li>Stickiness</li> <li>The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.</li> </ul>	standing requests
<ul> <li>o seconds</li> <li>Requires 30 to 900 seconds to enable, or 0 seconds to disable. This attribute cannot be combined with the Least ou ligorithm.</li> <li>coad balancing algorithm</li> <li>Determines how the load balancer selects targets from this target group when routing requests.</li> <li>P Round robin</li> <li>Cleast outstanding requests</li> <li>Cannot be combined with the Slow start duration attribute.</li> <li>2 Stickiness</li> <li>The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.</li> </ul>	standing requests
<ul> <li>Requires 30 to 900 seconds to enable, or 0 seconds to disable. This attribute cannot be combined with the Least ou algorithm.</li> <li>Load balancing algorithm</li> <li>Determines how the load balancer selects targets from this target group when routing requests.</li> <li>Round robin</li> <li>Least outstanding requests Cannot be combined with the Slow start duration attribute.</li> <li>Stickiness The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.</li> </ul>	standing requests
Stickiness The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.	
The type of stickiness associated with this target group. If enabled, the load balancer binds a client's session to within the target group.	
	specific instance
Stickiness type	
Load balancer generated cookie	
<ul> <li>Application-based cookie</li> </ul>	
Stickiness duration	
1 davs 💌	

### **AWS Network Load Balancer**

AWS NLB Listener port needs to be changed to an alternate one that we configured in Parallels RAS Console above (in our example, **8443**)

# Edit listener

arn:aws:elasticloadbalancing:us-east-1:204462620958:listener/net/SB-AWS-NLB/f643fecf5306363a/cf7df623a

### Listener details Info A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener routed per your specification. Protocol Port Default action Info Forward to TCP 8443 SB-TG-2 TCP Target type: Instance, IPv4 1-65535 Create target group 🗹 Cancel Save

### **Testing Load Balancing using Parallels HTML5 Client**

Copy the DNS hostname of AWS ALB in AWS Console (e.g. SB-AWS-ALB-########.us-east-1.elb.amazonaws.com) and try accessing this using the web browser.

To test the work of AWS ALB (connection is being done over HTTPS):

Right-click on an app > Open in Parallels HTML5 Client

AWSSB1





To check the load balancing over TCP, in the same Parallels HTML5 portal, right-click on an app > **Open in Parallels Client** 



You will notice that the native Parallels Client is establishing connection using the alternate hostname:



### AWSSB1

8	Cal	cul Edit H	lelp		×
Calculator					0
	MC	MR	MS	M+	M-
	-	CE	с	±	√
	7	8	9	/	%
	4	5	6	*	1/x
	1	2	3	-	
	(	)	•	+	

### **Testing Load Balancing using Parallels Client**

Since recent modification, at Parallels Client we need to specify the alternate port that was set in Parallels RAS Console and AWS NLB Listener.

Conn	ection Properties - AWS NLE	3	
Connection Display Printing Loc	cal Resources Experience Netw	ork Authentication	င်္သိ <sub>င်္သိ</sub> Advanced
Connection Settings			
Primary Connection:	SB-AWS-NLB-1		
Connection Mode:	Gateway SSL Mode	<b></b>	
Port:	8443		
	Secondary Connections		
Friendly Name:	AWS NLB		
Login			
Auto Login			
Authentication Type:	Credentials	<b></b>	
Username:			
Password:			
	✓ Save Password		
Domain:			
		Cancel	ОК

### Connect and launch a published app

• • • Parallels Clien	t - AWS NLB $<$ $>$ $\land$	► III III Connections
	Name	Description
AWS NLB	<ul> <li>Calculator</li> <li>Notepad</li> <li>Paint</li> <li>Wordpad</li> <li>Microsoft Edge</li> </ul>	Performs basic arithmetic tasks with a Calcul —
		MC MR MS M+ M- ← CE C ± √ 7 8 9 / %
		$\begin{array}{c} 4 & 5 & 6 & * & 1/x \\ 1 & 2 & 3 & - & = \\ 0 & \cdot & + & = \end{array}$

# Links for reference

For more information regarding Parallels RAS please see here: <u>https://www.parallels.com/products/ras/remote-application-server/</u>

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.