network tuning commands
ONTAP 9.13.1 commands

NetApp
February 12, 2024
# Table of Contents

network tuning commands ................................................. 1
  network tuning icmp modify ........................................... 1
  network tuning icmp show ............................................... 1
  network tuning icmp6 modify .......................................... 2
  network tuning icmp6 show ............................................ 3
  network tuning tcp modify ............................................. 4
  network tuning tcp show ................................................ 4
network tuning commands

network tuning icmp modify

Modify ICMP tuning options

Availability: This command is available to cluster administrators at the admin privilege level.

Description
This command displays options which can be used to fine tune icmp protocol behavior.

Parameters

- **-node** \{<nodename>|local\} - Node
  Sets this parameter to indicate on which node the ICMP tuning options are modified.

  [-is-drop-redirect-enabled \{true|false\}] - Drop redirect ICMP
  Sets this parameter to drop redirect ICMP message.

  [-tx-icmp-limit <integer>] - Maximum number of ICMP packets sent per second
  Sets the maximum number of ICMP messages including TCP RSTs can be sent per second.

  [-redirect-timeout <integer>] - Maximum seconds for route redirect timeout
  Sets this parameter to indicate the number of seconds after which the route is deleted. Value of zero means infinity. The default value is 300 seconds.

Examples

```
cluster1::> network tuning icmp modify -node node1 -is-drop-redirect-enabled false
```

network tuning icmp show

Show ICMP tuning options

Availability: This command is available to cluster administrators at the admin privilege level.

Description
This command displays the current state of the ICMP tuning options for the given node.

Parameters

{ [-fields <fieldname>,...] } 
If you specify the -fields <fieldname>, ... parameter, the command output also includes the specified field or fields. You can use '-'fields ?' to display the fields to specify.
Displays all ICMP tuning options.

[-node {<nodename>|local}] - Node
  Specifies the node for which the ICMP tuning options are displayed.

[-is-drop-redirect-enabled {true|false}] - Drop redirect ICMP
  Displays all entries that match the "is-drop-redirect-enabled" value.

[-tx-icmp-limit <integer>] - Maximum number of ICMP packets sent per second
  Displays all entries that match the "tx-icmp-limit" value.

[-redirect-timeout <integer>] - Maximum seconds for route redirect timeout
  Displays all the entries that match the "redirect-timeout" value.

Examples

```
cluster1::> network tuning icmp show
Drop Redirect Maximum ICMP Redirect Timeout
Node  ICMP      Sends per Second  in Seconds
--------- ------------- ----------------  ----------------
nodel  true          100               300
```

network tuning icmp6 modify

Modify ICMPv6 tuning options

Availability: This command is available to cluster administrators at the admin privilege level.

Description

This command displays options which can be used to fine tune icmpv6 protocol behavior.

Parameters

-[-node {<nodename>|local}] - Node
  Sets this parameter to indicate on which node the ICMPv6 tuning options are modified.

[-is-v6-redirect-accepted {true|false}] - Accept redirects via ICMPv6
  Sets this parameter to indicate whether or not redirect ICMPv6 messages are accepted.

[-redirect-v6-timeout <integer>] - Maximum seconds for route redirect timeout
  Sets this parameter to indicate the number of seconds after which the route is deleted. Value of zero means infinity. The default value is 300 seconds.
[-tx-icmp6-err-limit <integer>] - Maximum number of ICMPv6 error messages sent per second

Sets the maximum number of ICMPv6 error messages that can be sent per second.

Examples

cluster1::> network tuning icmp6 modify -node node1 -is-v6-redirect-accepted false

network tuning icmp6 show

Show ICMPv6 tuning options

Availability: This command is available to cluster administrators at the admin privilege level.

Description

This command displays the current state of the ICMPv6 tuning options for the given node.

Parameters

{ [-fields <fieldname>,...] } If you specify the -fields <fieldname>, ... parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance ] } Displays all ICMPv6 tuning options.

[-node {<nodename>|local}] - Node Specifies the node for which the ICMPv6 tuning options are displayed.

[-is-v6-redirect-accepted {true|false}] - Accept redirects via ICMPv6 Displays all entries that match the "is-v6-redirect-accepted" value.

[-redirect-v6-timeout <integer>] - Maximum seconds for route redirect timeout Displays all the entries that match the "redirect-v6-timeout" value.

[-tx-icmp6-err-limit <integer>] - Maximum number of ICMPv6 error messages sent per second Displays all entries that match the "tx-icmp6-err-limit" value.

Examples
network tuning icmp6 show

Accept Redirect Maximum ICMPv6 Error Redirect Timeout

<table>
<thead>
<tr>
<th>Node</th>
<th>ICMPv6</th>
<th>Sends per Second</th>
<th>in Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1</td>
<td>true</td>
<td>100</td>
<td>300</td>
</tr>
</tbody>
</table>

network tuning tcp modify

Modify TCP tuning options

**Availability:** This command is available to *cluster* administrators at the *admin* privilege level.

**Description**

This commands sets TCP tuning options on the node.

**Parameters**

- `-node {<nodename>|local}` - Node
  
  Indicates on which node the TCP tuning options will be modified.

  *-is-path-mtu-discovery-enabled {true|false}* - Path MTU discovery enabled
  
  Enables path MTU discovery feature.

  *-is-rfc3465-enabled {true|false}* - RFC3465 enabled
  
  Enables the rfc3465 feature.

  *-max-cwnd-increment <integer>* - Maximum congestion window segments incrementation
  
  Sets the maximum congestion window increment segements during slow start.

  *-is-rfc3390-enabled {true|false}* - RFC3390 enabled
  
  Enables the rfc3390 feature.

  *-is-sack-enabled {true|false}* - SACK support enabled
  
  Enables the selective ACK feature.

**Examples**

```
cluster1::> network tuning tcp modify -node node1 -is-path-mtu-discovery-enabled false
```

network tuning tcp show

Show TCP tuning options
Availability: This command is available to cluster administrators at the admin privilege level.

Description

This command displays the current state of the TCP tuning options for the given node.

Parameters

{ [-fields <fieldname>,...]
  If you specify the -fields <fieldname>, ... parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.
}

|-instance ]
  Displays all TCP tuning options.

[-node {<nodename>|local}] - Node
  Specifies the node for which the TCP tuning options will be displayed.

[-is-path-mtu-discovery-enabled {true|false}] - Path MTU discovery enabled
  Displays all entries that match the "is-path-mtu-discovery-enabled" value.

[-is-rfc3465-enabled {true|false}] - RFC3465 enabled
  Displays all entries that match the "is-rfc3465-enabled" value.

[-max-cwnd-increment <integer>] - Maximum congestion window segments incrementation
  Displays all entries that match the "max-cwnd-increment" value.

[-is-rfc3390-enabled {true|false}] - RFC3390 enabled
  Displays all entries that match the "is-rfc3390-enabled" value.

[-is-sack-enabled {true|false}] - SACK support enabled
  Displays all entries that match the "is-sack-enabled" value.

Examples

| cluster1::> network tuning tcp show
<table>
<thead>
<tr>
<th>Path MTU</th>
<th>Maximum</th>
<th>Selective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Discovery</td>
<td>RFC3465</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>node1</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

Path MTU           Maximum                   Selective
--------- ---------  ------- ----------------- ------- --------
node1      true       true    2                 true    true
Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.