



# Requirements

## Element Software

NetApp  
October 01, 2024

# Table of Contents

- Requirements ..... 1
  - Find more information ..... 1
  - Networking ..... 1
  - Switch configuration for clusters running Element software ..... 1
  - Network port requirements ..... 3

# Requirements

Before you get started, you should review the prerequisites to deploy NetApp Element software, including networking and port requirements.

- [Networking requirements](#)
- [Switch configuration](#)
- [Network port requirements](#)

## Find more information

- [SolidFire and Element Software Documentation](#)

## Networking

The network setup for a SolidFire system consists of switch and port requirements. The implementation of these depends on your system.

### For more information

- [Switch configuration for clusters running Element software](#)
- [Network port requirements](#)
- [SolidFire and Element Software Documentation](#)
- [NetApp Element Plug-in for vCenter Server](#)

## Switch configuration for clusters running Element software

The NetApp Element software system has certain switch requirements and best practices for optimal storage performance.

Storage nodes require 10 or 25GbE Ethernet switches, depending on specific node hardware, for iSCSI storage services and node intra-cluster services communication. 1GbE switches can be used for these types of traffic:

- Management of the cluster and the nodes
- Intra-cluster management traffic between the nodes
- Traffic between the cluster nodes and the management node virtual machine

**Best Practice:** You should implement the following best practices when configuring Ethernet switches for cluster traffic:

- For non-storage traffic in the cluster, deploy a pair of 1GbE switches to provide high availability and load sharing.
- On the storage network switches, deploy switches in pairs and configure and utilize jumbo frames (an MTU size of 9216 bytes). This ensures a successful installation and eliminates storage network errors due to fragmented packets.

Element deployment requires at least two network segments, one for each of the following types of traffic:

- Management
- Storage/Data

Depending on the NetApp H-Series storage node models and the planned cabling configuration, you can physically separate these networks using separate switches or logically separate them using VLANs. For most deployments, however, you need to logically separate these networks using VLANs.

Storage nodes need to be able to communicate before, during, and after deployment.

If you are implementing separate management networks for storage nodes, ensure that these management networks have network routes between them. These networks must have gateways assigned, and there must be a route between the gateways. Ensure that each new node has a gateway assigned to facilitate communication between nodes and management networks.

NetApp Element requires the following:

- All switch ports connected to NetApp H-Series storage nodes must be configured as spanning tree edge ports.
  - On Cisco switches, depending on the switch model, software version and port type, you can do this with one of the following commands:
    - `spanning-tree port type edge`
    - `spanning-tree port type edge trunk`
    - `spanning-tree portfast`
    - `spanning-tree portfast trunk`
  - On Mellanox switches, you can do this with the `spanning-tree port type edge` command.
- The switches handling storage traffic must support speeds of at least 10GbE per port (up to 25GbE per port is supported).
- The switches handling management traffic must support speeds of at least 1GbE per port.
- You must configure jumbo frames on the switch ports handling storage traffic. Hosts must be able to send 9000 byte packets end-to-end for a successful installation.
- Round-trip network latency between all storage nodes should not exceed 2ms.

Some nodes provide additional out-of-band management capabilities via a dedicated management port. NetApp H300S, H500S, and H700S nodes also allow for IPMI access via Port A. As a best practice, you should ease remote management by configuring out-of-band management for all nodes in your environment.

## For more information

- [NetApp HCI network and switch requirements](#)
- [SolidFire and Element Software Documentation](#)
- [NetApp Element Plug-in for vCenter Server](#)

## Network port requirements

You might need to allow the following TCP and UDP ports through your data center's edge firewall so that you can manage the system remotely and allow clients outside of your data center to connect to resources. Some of these ports might not be required, depending on how you use the system.

All ports are TCP unless stated otherwise, and all TCP ports must support three-way handshake communication between the NetApp Support Server, management node, and nodes running Element software. For example, the host on a management node source communicates with the host on a storage cluster MVIP destination through TCP port 443, and the destination host communicates back to the source host through any port.



Enable ICMP between the management node, nodes running Element software, and cluster MVIP.

The following abbreviations are used in the table:

- MIP: Management IP address, a per-node address
- SIP: Storage IP address, a per-node address
- MVIP: Management virtual IP address
- SVIP: Storage virtual IP address

| Source          | Destination                          | Port       | Description   |
|-----------------|--------------------------------------|------------|---|
| iSCSI clients   | Storage cluster MVIP                 | 443        | (Optional) UI and API access                                    |
| iSCSI clients   | Storage cluster SVIP                 | 3260       | Client iSCSI communications                                     |
| iSCSI clients   | Storage node SIP                     | 3260       | Client iSCSI communications                                     |
| Management node | <code>sfsupport.solidfire.com</code> | 22         | Reverse SSH tunnel for support access                           |
| Management node | Storage node MIP                     | 22         | SSH access for support  |
| Management node | DNS servers                          | 53 TCP/UDP | DNS lookup  |
| Management node | Storage node MIP                     | 442        | UI and API access to storage node and Element software upgrades |

| Source                | Destination              | Port        | Description  |
|-----------------------|--------------------------|-------------|--|
| Management node       | Storage cluster MVIP     | 442         | UI and API access to storage node and Element software upgrades                      |
| Management node       | monitoring.solidfire.com | 443         | Storage cluster reporting to Active IQ   |
| Management node       | Storage cluster MVIP     | 443         | UI and API access to storage node and Element software upgrades                      |
| Management node       | repo.netapp.com          | 443         | Provides access to components necessary to install/update on-premises deployment.    |
| Management node       | Storage node BMC/IPMI    | 623 UDP     | RMCP port. This is required to manage IPMI-enabled systems.                          |
| Management node       | Witness Node             | 9442        | Per-node configuration API service   |
| Management node       | vCenter Server           | 9443        | vCenter Plug-in registration. The port can be closed after registration is complete. |
| SNMP server           | Storage cluster MVIP     | 161 UDP     | SNMP polling   |
| SNMP server           | Storage node MIP         | 161 UDP     | SNMP polling   |
| Storage node BMC/IPMI | Management node          | 623 UDP     | RMCP port. This is required to manage IPMI-enabled systems.                          |
| Storage node MIP      | DNS servers              | 53 TCP/UDP  | DNS lookup   |
| Storage node MIP      | Management node          | 80          | Element software upgrades  |
| Storage node MIP      | S3/Swift endpoint        | 80          | (Optional) HTTP communication to S3/Swift endpoint for backup and recovery           |
| Storage node MIP      | NTP server               | 123 UDP     | NTP  |
| Storage node MIP      | Management node          | 162 UDP     | (Optional) SNMP traps  |
| Storage node MIP      | SNMP server              | 162 UDP     | (Optional) SNMP traps  |
| Storage node MIP      | LDAP server              | 389 TCP/UDP | (Optional) LDAP lookup   |
| Storage node MIP      | Management node          | 443         | Element storage firmware upgrades  |

| Source                  | Destination                 | Port                         | Description   |
|-------------------------|-----------------------------|------------------------------|---|
| Storage node MIP        | Remote storage cluster MVIP | 443                          | Remote replication cluster pairing communication                            |
| Storage node MIP        | Remote storage node MIP     | 443                          | Remote replication cluster pairing communication                            |
| Storage node MIP        | S3/Swift endpoint           | 443                          | (Optional) HTTPS communication to S3/Swift endpoint for backup and recovery |
| Storage node MIP        | Management node             | 514 TCP/UDP<br>10514 TCP/UDP | Syslog forwarding   |
| Storage node MIP        | Syslog server               | 514 TCP/UDP<br>10514 TCP/UDP | Syslog forwarding   |
| Storage node MIP        | LDAPS server                | 636 TCP/UDP                  | LDAPS lookup  |
| Storage node MIP        | Remote storage node MIP     | 2181                         | Intercluster communication for remote replication                           |
| Storage node SIP        | Remote storage node SIP     | 2181                         | Intercluster communication for remote replication                           |
| Storage node SIP        | Storage node SIP            | 3260                         | Internode iSCSI   |
| Storage node SIP        | Remote storage node SIP     | 4000 through 4020            | Remote replication node-to-node data transfer                               |
| System administrator PC | Management node             | 442                          | HTTPS UI access to management node  |
| System administrator PC | Storage node MIP            | 442                          | HTTPS UI and API access to storage node                                     |
| System administrator PC | Management node             | 443                          | HTTPS UI and API access to management node                                  |
| System administrator PC | Storage cluster MVIP        | 443                          | HTTPS UI and API access to storage cluster                                  |

| Source                  | Destination  | Port    | Description   |
|-------------------------|--|---------|---|
| System administrator PC | Storage node baseboard management controller (BMC)/Intelligent Platform Management Interface (IPMI) H410 and H600 series | 443     | HTTPS UI and API access to node remote control  |
| System administrator PC | Storage node MIP   | 443     | HTTPS storage cluster creation, post-deployment UI access to storage cluster              |
| System administrator PC | Storage node BMC/IPMI H410 and H600 series   | 623 UDP | Remote Management Control Protocol port. This is required to manage IPMI-enabled systems. |
| System administrator PC | Witness Node   | 8080    | Witness Node per-node web UI  |
| vCenter Server          | Storage cluster MVIP   | 443     | vCenter Plug-in API access  |
| vCenter Server          | Remote plug-in   | 8333    | Remote vCenter Plug-in service  |
| vCenter Server          | Management node  | 8443    | (Optional) vCenter Plug-in QoSSIOC service.   |
| vCenter Server          | Storage cluster MVIP   | 8444    | vCenter VASA provider access (VVols only)   |
| vCenter Server          | Management node  | 9443    | vCenter Plug-in registration. The port can be closed after registration is complete.      |

## For more information

- [SolidFire and Element Software Documentation](#)
- [NetApp Element Plug-in for vCenter Server](#)



## 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.