Configure the SP/BMC network

ONTAP 9

NetApp
May 05, 2023

Table of Contents

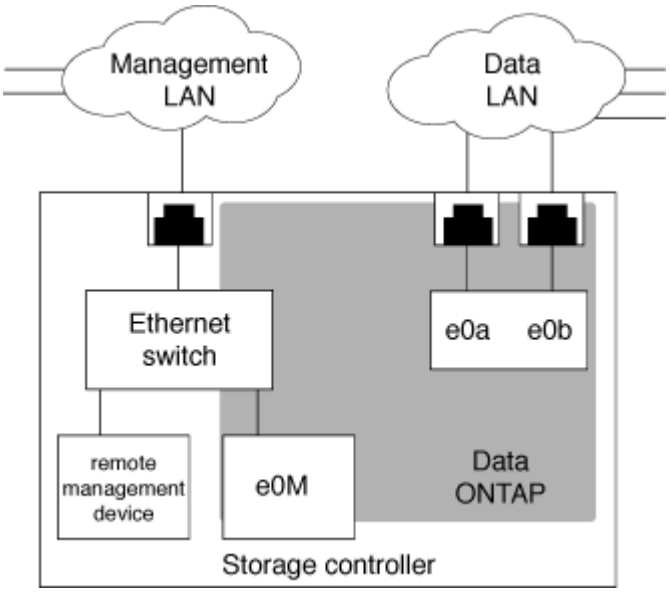
Configure the SP/BMC network 1
Isolate management network traffic 1
Considerations for the SP/BMC network configuration 1
Enable the SP/BMC automatic network configuration 3
Configure the SP/BMC network manually 3
Modify the SP API service configuration 5

Configure the SP/BMC network

Isolate management network traffic

It is a best practice to configure SP/BMC and the e0M management interface on a subnet dedicated to management traffic. Running data traffic over the management network can cause performance degradation and routing problems.

The management Ethernet port on most storage controllers (indicated by a wrench icon on the rear of the chassis) is connected to an internal Ethernet switch. The internal switch provides connectivity to SP/BMC and to the e0M management interface, which you can use to access the storage system via TCP/IP protocols like Telnet, SSH, and SNMP.



If you plan to use both the remote management device and e0M, you must configure them on the same IP subnet. Since these are low-bandwidth interfaces, the best practice is to configure SP/BMC and e0M on a subnet dedicated to management traffic.

If you cannot isolate management traffic, or if your dedicated management network is unusually large, you should try to keep the volume of network traffic as low as possible. Excessive ingress broadcast or multicast traffic may degrade SP/BMC performance.

Some storage controllers, such as the AFF A800, have two external ports, one for BMC and the other for e0M. For these controllers, there is no requirement to configure BMC and e0M on the same IP subnet.

Considerations for the SP/BMC network configuration

You can enable cluster-level, automatic network configuration for the SP (recommended). You can also leave the SP automatic network configuration disabled (the default) and manage the SP network configuration manually at the node level. A few considerations exist for each case.

This topic applies to both the SP and the BMC.

The SP automatic network configuration enables the SP to use address resources (including the IP address, subnet mask, and gateway address) from the specified subnet to set up its network automatically. With the SP automatic network configuration, you do not need to manually assign IP addresses for the SP of each node. By default, the SP automatic network configuration is disabled; this is because enabling the configuration requires that the subnet to be used for the configuration be defined in the cluster first.

If you enable the SP automatic network configuration, the following scenarios and considerations apply:

- If the SP has never been configured, the SP network is configured automatically based on the subnet specified for the SP automatic network configuration.
- If the SP was previously configured manually, or if the existing SP network configuration is based on a different subnet, the SP network of all nodes in the cluster are reconfigured based on the subnet that you specify in the SP automatic network configuration.

  The reconfiguration could result in the SP being assigned a different address, which might have an impact on your DNS configuration and its ability to resolve SP host names. As a result, you might need to update your DNS configuration.

- A node that joins the cluster uses the specified subnet to configure its SP network automatically.
- The `system service-processor network modify` command does not enable you to change the SP IP address.

  When the SP automatic network configuration is enabled, the command only allows you to enable or disable the SP network interface.

  - If the SP automatic network configuration was previously enabled, disabling the SP network interface results in the assigned address resource being released and returned to the subnet.
  - If you disable the SP network interface and then reenable it, the SP might be reconfigured with a different address.

If the SP automatic network configuration is disabled (the default), the following scenarios and considerations apply:

- If the SP has never been configured, SP IPv4 network configuration defaults to using IPv4 DHCP, and IPv6 is disabled.

  A node that joins the cluster also uses IPv4 DHCP for its SP network configuration by default.

- The `system service-processor network modify` command enables you to configure a node's SP IP address.

  A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a scenario with duplicate addresses.

If the SP automatic network configuration is disabled after having been enabled previously, the following scenarios and considerations apply:

- If the SP automatic network configuration has the IPv4 address family disabled, the SP IPv4 network defaults to using DHCP, and the `system service-processor network modify` command enables you to modify the SP IPv4 configuration for individual nodes.

- If the SP automatic network configuration has the IPv6 address family disabled, the SP IPv6 network is also disabled, and the `system service-processor network modify` command enables you to enable and modify the SP IPv6 configuration for individual nodes.

Enable the SP/BMC automatic network configuration

Enabling the SP to use automatic network configuration is preferred over manually configuring the SP network. Because the SP automatic network configuration is cluster wide, you do not need to manually manage the SP network for individual nodes.

This task applies to both the SP and the BMC.

- The subnet you want to use for the SP automatic network configuration must already be defined in the cluster and must have no resource conflicts with the SP network interface.

  The `network subnet show` command displays subnet information for the cluster.

  The parameter that forces subnet association (the `-force-update-lif-associations` parameter of the `network subnet` commands) is supported only on network LIFs and not on the SP network interface.

- If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP.

  The `network options ipv6 show` command displays the current state of IPv6 settings for ONTAP.

Steps

1. Specify the IPv4 or IPv6 address family and name for the subnet that you want the SP to use by using the `system service-processor network auto-configuration enable` command.
2. Display the SP automatic network configuration by using the `system service-processor network auto-configuration show` command.
3. If you subsequently want to disable or reenable the SP IPv4 or IPv6 network interface for all nodes that are in quorum, use the `system service-processor network modify` command with the `-address -family` [`IPv4`|`IPv6`] and `-enable` [`true`|`false`] parameters.

   When the SP automatic network configuration is enabled, you cannot modify the SP IP address for a node that is in quorum. You can only enable or disable the SP IPv4 or IPv6 network interface.

   If a node is out of quorum, you can modify the node's SP network configuration, including the SP IP address, by running `system service-processor network modify` from the node and confirming that you want to override the SP automatic network configuration for the node. However, when the node joins the quorum, the SP automatic reconfiguration takes place for the node based on the specified subnet.

Configure the SP/BMC network manually

If you do not have automatic network configuration set up for the SP, you must manually configure a node's SP network for the SP to be accessible by using an IP address.

What you'll need

If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP. The

`network options ipv6` commands manage IPv6 settings for ONTAP.

This task applies to both the SP and the BMC.

You can configure the SP to use IPv4, IPv6, or both. The SP IPv4 configuration supports static and DHCP addressing, and the SP IPv6 configuration supports static addressing only.

If the SP automatic network configuration has been set up, you do not need to manually configure the SP network for individual nodes, and the `system service-processor network modify` command allows you to only enable or disable the SP network interface.

Steps

1. Configure the SP network for a node by using the `system service-processor network modify` command.
   - The `-address-family` parameter specifies whether the IPv4 or IPv6 configuration of the SP is to be modified.
   - The `-enable` parameter enables the network interface of the specified IP address family.
   - The `-dhcp` parameter specifies whether to use the network configuration from the DHCP server or the network address that you provide.

     You can enable DHCP (by setting `-dhcp` to `v4`) only if you are using IPv4. You cannot enable DHCP for IPv6 configurations.
   - The `-ip-address` parameter specifies the public IP address for the SP.

     A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a duplicate address assignment.
   - The `-netmask` parameter specifies the netmask for the SP (if using IPv4.)
   - The `-prefix-length` parameter specifies the network prefix-length of the subnet mask for the SP (if using IPv6.)
   - The `-gateway` parameter specifies the gateway IP address for the SP.
2. Configure the SP network for the remaining nodes in the cluster by repeating the step 1.
3. Display the SP network configuration and verify the SP setup status by using the `system service-processor network show` command with the `-instance` or `-field setup-status` parameters.

   The SP setup status for a node can be one of the following:
   - `not-setup` — Not configured
   - `succeeded` — Configuration succeeded
   - `in-progress` — Configuration in progress
   - `failed` — Configuration failed

Example of configuring the SP network

The following example configures the SP of a node to use IPv4, enables the SP, and displays the SP network configuration to verify the settings:

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                             Node: node1
                     Address Type: IPv4
                Interface Enabled: true
                   Type of Device: SP
                           Status: online
                      Link Status: up
                      DHCP Status: none
                       IP Address: 192.168.123.98
                      MAC Address: ab:cd:ef:fe:ed:02
                          Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

Modify the SP API service configuration

The SP API is a secure network API that enables ONTAP to communicate with the SP over the network. You can change the port used by the SP API service, renew the certificates the service uses for internal communication, or disable the service entirely. You need to modify the configuration only in rare situations.

About this task

- The SP API service uses port `50000` by default.

  You can change the port value if, for example, you are in a network setting where port `50000` is used for communication by another networking application, or you want to differentiate between traffic from other applications and traffic generated by the SP API service.

- The SSL and SSH certificates used by the SP API service are internal to the cluster and not distributed externally.

In the unlikely event that the certificates are compromised, you can renew them.

- The SP API service is enabled by default.

  You only need to disable the SP API service in rare situations, such as in a private LAN where the SP is not configured or used and you want to disable the service.

  If the SP API service is disabled, the API does not accept any incoming connections. In addition, functionality such as network-based SP firmware updates and network-based SP “down system” log collection becomes unavailable. The system switches to using the serial interface.

Steps

1. Switch to the advanced privilege level by using the `set -privilege advanced` command.
2. Modify the SP API service configuration:

If you want to…	Use the following command…
Change the port used by the SP API service	`system service-processor api-service modify` with the `-port {49152..65535}` parameter
Renew the SSL and SSH certificates used by the SP API service for internal communication	• For ONTAP 9.5 or later use `system service-processor api-service renew-internal-certificate` • For ONTAP 9.4 and earlier use • `system service-processor api-service renew-certificates` If no parameter is specified, only the host certificates (including the client and server certificates) are renewed. If the `-renew-all true` parameter is specified, both the host certificates and the root CA certificate are renewed.
comm	
Disable or reenable the SP API service	`system service-processor api-service modify` with the `-is-enabled {true|false}` parameter

3. Display the SP API service configuration by using the `system service-processor api-service show` command.

Copyright information

Trademark information