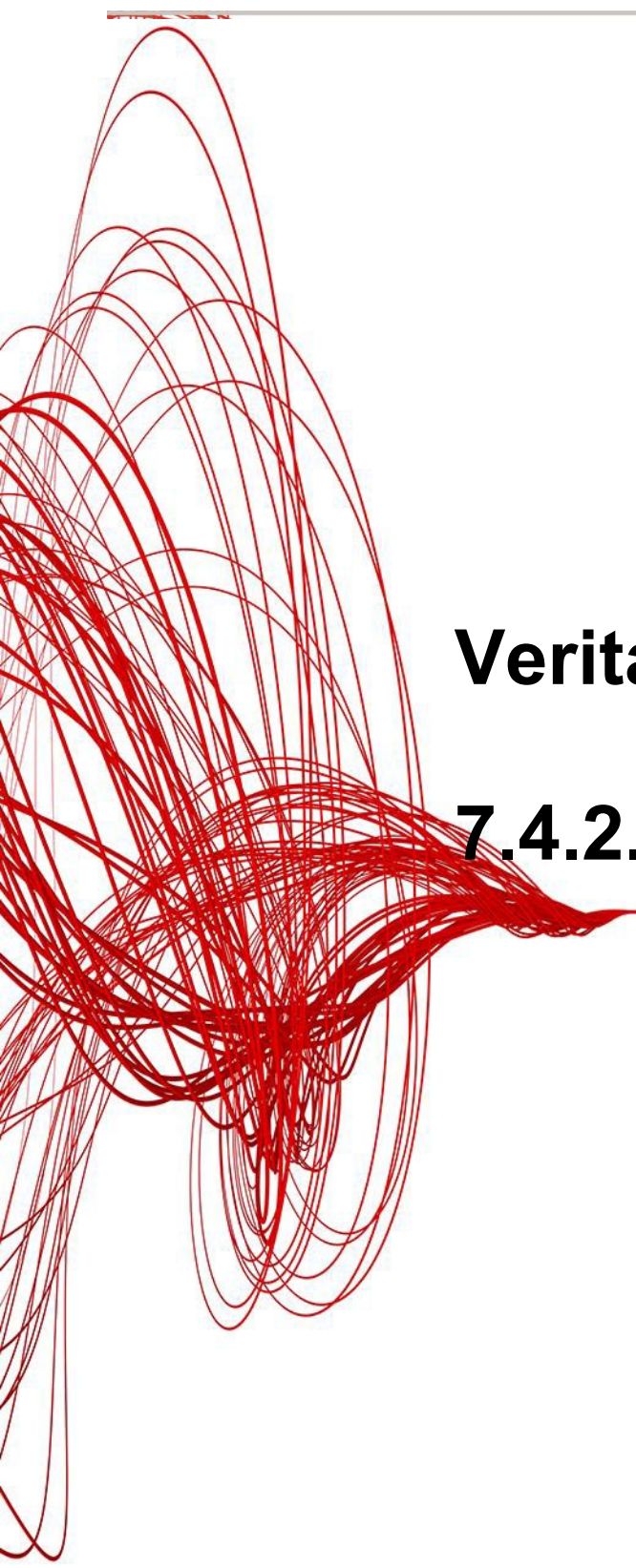

Veritas Access Appliance

7.4.2.100 Release Update

Linux

VERITAS

The truth in information.

Contents

About the release

This update contains critical updates, and enhancements for the Veritas 3340 Access Appliance (7.4.2) release. This patch can be applied only on top of the Veritas 3340 Access Appliance (7.4.2) release. If you are on an earlier version of the product, please upgrade to 7.4.2 version and then install the patch.

For upgrading Veritas Access 3340 Appliance to 7.4.2.100, refer to the following technote:
https://www.veritas.com/support/en_US/article.100045858.html

New features/enhancements are included in this release:

- Ability to patch the appliance using rolling upgrade
  - Patch individual node before configuration
  - Perform rolling upgrade on the existing cluster
  - Select rpm update as part of the patch
- Separation of management and data network
  - Ability to move appliance management network to a different subnet
  - Ability to move data network to a different subnet
  - Host the Access management on eth1 interface
  - Support multiple network routes
- Support TSM workload over S3
  - S3 bucket management enhancement
  - Performance enhancement
  - SSL (secure) connection related enhancements
- Ability to manage alerts and notifications
  - Ability to add/remove ignore strings
  - Support for additional components for filters

Separating data and management network from the Access CLISH

The following use cases are supported:

Use case 1	Fresh deployment and the management NIC and data NICs are in different subnets
Use case 2	Cluster is already configured with Veritas Access 7.4.2 version and all the data NICs are in the same subnet and you want to move management (eth1) NIC to a different subnet
Use case 3	Cluster is already configured with Veritas Access 7.4.2 version and you want to move the data NICs to a different subnet and the management NIC (eth1) remains in the same subnet

Use case 1: Fresh deployment and the management NICs and data NICs are in different subnets

This section includes the following topics:

- Prerequisites
- Configuring the cluster
- Moving the cluster management console to the management network and adding route for the data network

Prerequisites

- The Veritas Access 7.4.2 GA is installed
- The eth1 interface is connected to the management subnet
- The data NICs, eth4 and eth5 are connected to the data subnet
- Three IPs from the management subnet and nine IPs from data the subnet are required. Out of the nine IPs one IP from the data subnet will get free after the completion of management and data subnet segregation.

Configuring the cluster

1. Login to the first node using the IPMI console. Assign the management network IP to eth1.
   ```
   Main_Menu> Network
   Network> configure <IP> <netmask> <gateway> eth1
   ```
   For example:
   ```
   Network> configure 192.168.101.112 255.255.252.0 192.168.100.1 eth1
   ```

2. Login to the second node using the IPMI console. Assign the management network IP to eth1.
   ```
   Main_Menu> Network
   Network> configure <IP> <netmask> <gateway> eth1
   Network> configure 192.168.101.113 255.255.252.0 192.168.100.1 eth1
   ```

3. Set DNS on both nodes.
   ```
   Network> DNS Add Nameserver <DNS_IP>
   ```

For example:
Network> DNS Add Nameserver 192.168.1.1
Network> DNS Add SearchDomain demodns.com

4. Set the DNS registered hostname on both the nodes.
Network> hostname set <node1> Network> hostname set <node2>

5. Start the cluster configuration.
   - Provide IPs from the data subnet when asked for physical and virtual IPs (IPsfrom 192.168.104.0/24 subnet).
   - Provide the data subnet's netmask when prompted for the netmask for the public IP address.
   - Provide the management subnet's gateway IP when asked for the gateway.

Main_Menu> Manage> Cluster > Configure

```
Before you configure the cluster from this node, note the following:
- The Access cluster configuration is only allowed to run from one node.
Make sure that no other Access cluster configuration process is ongoing on
the current node or other nodes.
- Make sure that you have the node management IP addresses of the appliance
nodes for clustering.
- Make sure that you have reserved enough IP addresses for use as the physical
and the virtual IP addresses of the Access cluster. At least four continuous
IP addresses must be reserved for each type.
Note the following cluster naming rules:
- The cluster name must be at least three and no more than 10 characters
long.
- Allowed characters are lowercase letters, numbers, and hyphens.
- The cluster name must start with a lowercase letter of the alphabet.
- The cluster name must end with a lowercase letter of the alphabet or a
number.
>> Do you want to continue? [yes,no] yes
>> Enter a name for the Veritas Access Cluster: vaclust
>> Enter the IP addresses of the appliance nodes for clustering (separate
with a space): 192.209.101.112 192.168.101.113 (These are IPs which are
assigned to eth1 on nodes)
>> Enter the appliance maintenance user password of the nodes:
>> Do you want to configure network bonding for public networks? [yes,no] no
>> Enter the public IP starting address (reserve a minimum of 4 continuous
IPs addresses): 192.168.104.21 (This IP range is from data subnet)
>> Enter the virtual IP starting address (reserve a minimum of 4 continuous
IPs addresses): 192.168.104.25 (This IP range is from data subnet)
>> Enter the netmask for the public IP address: 255.255.255.0 (Provide
netmask of data subnet)
>> Enter the default gateway IP address: 192.168.100.1 (Provide a gateway of
management subnet)
>> Enter the DNS server IP address: 192.168.1.1
>> Enter the DNS server domain name: demodns.com
>> Enter the console virtual IP address: 192.168.104.30
====================
Summary of the cluster configuration:

Cluster name: vaclust
Appliance nodes for clustering: 192.168.104.12,192.168.104.13 Nodes with
public IP: 192.168.104.14,192.168.104.15,192.168.104.16,192.168.104.17
Netmask for public IP address: 255.255.255.0 Virtual IP addresses:
192.168.104.21,192.168.104.22,192.168.104.23,192.168.104.24
Default gateway IP address: 192.168.100.1 DNS server IP address: 192.168.1.1
```

```
DNS server domain name: demodns.com Console virtual IP address:
192.168.104.25
====================
>> Do you want to continue? [yes,no] yes
```

6. Wait for the cluster configuration to complete.

7. Upgrade the cluster to 7.4.2.100 using the steps here.

Moving the cluster management console to the management network and adding route for the data network

1. Login to the Access Appliance CLISH using its cluster console IP from a client machine which is in the data subnet.

2. Add eth1 network interface to the cluster configuration.
   Network> device add eth1
   If this fails, please contact Veritas Technical Support.

3. Verify that eth1 is added to the cluster configuration.
   Network> ip addr show

```
IP              Netmask/Prefix Device Node       Type          Status
--              -------------- ------ ----       ----          ------
192.168.101.112 255.255.252.0  eth1   vaclust_02 Physical
192.168.101.113 255.255.252.0  eth1   vaclust_01 Physical
192.168.104.21  255.255.255.0  eth4   vaclust_01 Physical
192.168.104.22  255.255.255.0  eth5   vaclust_01 Physical
192.168.104.23  255.255.255.0  eth4   vaclust_02 Physical
192.168.104.24  255.255.255.0  eth5   vaclust_02 Physical
192.168.104.35  255.255.255.0  eth4   vaclust_01 Virtual ONLINE (Con IP)
192.168.104.31  255.255.255.0  eth4   vaclust_02 Virtual ONLINE
192.168.104.32  255.255.255.0  eth4   vaclust_01 Virtual ONLINE
192.168.104.33  255.255.255.0  eth5   vaclust_02 Virtual ONLINE
192.168.104.34  255.255.255.0  eth5   vaclust_01 Virtual ONLINE
```

4. You require a new IP from the management subnet (which will be used as the cluster console IP) to move the cluster console to management subnet. Move the new management console IP to eth1.
   Network> ip addr modify <old_console_IP> <new_console_IP> <netmask> eth1 For example:
   Network> ip addr modify 192.168.104.35 192.168.101.111 255.255.252.0 eth1

```
ACCESS ip addr INFO V-493-10-1468 All existing SSH session will be terminated,
please logon with new Console ip.
```

5. The old session is terminated after you run this command. Login to the Veritas Access CLISH using the console IP and eth1 interface. Verify that the IP is shifted using the **network ip addr show** command.
   Network> ip addr show

```
IP              Netmask/Prefix  Device Node       Type     Status
-------------------------------------------------------------------
192.168.101.112 255.255.252.0   eth1   vaclust_02 Physical
192.168.101.113 255.255.252.0   eth1   vaclust_01 Physical
192.168.104.21  255.255.255.0   eth4   vaclust_01 Physical
192.168.104.22  255.255.255.0   eth5   vaclust_01 Physical
192.168.104.23  255.255.255.0   eth4   vaclust_02 Physical
192.168.104.24  255.255.255.0   eth5   vaclust_02 Physical
```

```
192.168.101.111 255.255.255.0   eth1   vaclust_01 Virtual ONLINE (Con IP)
192.168.104.31  255.255.255.0   eth4   vaclust_02 Virtual ONLINE
192.168.104.32  255.255.255.0   eth4   vaclust_01 Virtual ONLINE
192.168.104.33  255.255.255.0   eth5   vaclust_02 Virtual ONLINE
192.168.104.34  255.255.255.0   eth5   vaclust_01 Virtual ONLINE
```

6. Configure a gateway for the data subnet.
   Network> ip route add all 0.0.0.0 0.0.0.0 via <gateway> dev eth4
   Network> ip route add all 0.0.0.0 0.0.0.0 via <gateway> dev eth5
   You can now provision storage, create shares and mount it from the clients which are in the data subnet.

Use case 2: Cluster is already configured with Veritas Access 7.4.2 version and all the data NICs are in the same subnet and you want to move management (eth1) NIC to a different subnet

This section includes the following topics:

Prerequisites

- The Veritas Access 7.4.2.100 patch is installed
- All the network interfaces should be in the same subnet (data subnet)**.**
- Three new IPs from the management subnet

Configuring the network

Note: Since the network configuration of the cluster is getting changed, some I/O pause/stop/interrupt occurs for all the currently running service on the Access nodes. It is recommended that you stop all the service such as NFS, CIFS, FTP, S3, ISCSI, Veritas Data Deduplication, Cloud Catalyst, and Enterprise Vault.

1. Login to the Veritas Access CLISH using the Access console IP (192.168.100.50) and perform the following steps.

2. Verify if all the IPs are in same subnet (eth1, eth4, eth5) using the **ip addr show** command. Note that all the physical as well as virtual IPs belong to only one network (192.168.100.0) with subnet mask as 255.255.255.0.

```
Network> ip addr show
IP               Netmask/Prefix Device  Node       Type    Status
--               -------------- ------  ----       ----    ------
192.168.100.51   255.255.255.0  eth4    app742_01 Physical
192.168.100.52   255.255.255.0  eth5    app742_01 Physical
192.168.100.53   255.255.255.0  eth4    app742_02 Physical
192.168.100.54   255.255.255.0  eth5    app742_02 Physical
192.168.100.50   255.255.255.0  eth4    app742_01 Virtual   ONLINE (Con IP)
192.168.100.55   255.255.255.0  eth4    app742_02 Virtual   ONLINE
192.168.100.56   255.255.255.0  eth4    app742_01 Virtual   ONLINE
192.168.100.57   255.255.255.0  eth5    app742_02 Virtual   ONLINE
192.168.100.58   255.255.255.0  eth5    app742_01 Virtual   ONLINE
```

3. Add the eth1 network interface to the Veritas Access configuration.

```
Network> device add eth1
100% [#] Success: device eth1 added.
```

Verify that device is added to the configuration using the following command

```
Network> ip addr show
IP               Netmask/Prefix Device  Node       Type    Status
--               -------------- ------  ----       ----    ------
192.168.100.41   255.255.255.0  eth1    app742_01 Physical
192.168.100.42   255.255.255.0  eth1    app742_02 Physical
192.168.100.51   255.255.255.0  eth4    app742_01 Physical
192.168.100.52   255.255.255.0  eth5    app742_01 Physical
192.168.100.53   255.255.255.0  eth4    app742_02 Physical
192.168.100.54   255.255.255.0  eth5    app742_02 Physical
192.168.100.50   255.255.255.0  eth4    app742_01 Virtual   ONLINE (Con IP)
```

```
192.168.100.51   255.255.255.0  eth4   app742_02 Virtual   ONLINE
192.168.100.56   255.255.255.0  eth4   app742_01 Virtual   ONLINE
192.168.100.57   255.255.255.0  eth5   app742_02 Virtual   ONLINE
192.168.100.58   255.255.255.0  eth5   app742_01 Virtual   ONLINE
```

4. Modify the eth1 physical IP from Access CLISH**.**

   Network> ip addr modify <old-eth1-physical-ip> <new_IP> <new_netmask>
   For example:
   Network> ip addr modify 192.168.100.41 192.168.20.25 255.255.255.0
   In this command:
   - The new subnet is 192.168.20.0 which is the management subnet.
   - The old IP address of eth1 is 192.168.100.41
   - The new IP address is the IP which you want to give to eth1 from the new subnetIP (192.168.20.25)
   - Netmask is the new IP's subnet mask (255.255.255.0)

   Note: You are required to modify all the physical IPs of eth1 to IPs of the new subnet. eth1 will not be accessible for some time until we change the physical connections for eth1 and add gateway for new subnet.

5. Add the old eth1 physical IPs as virtual IPs. Use the same old physical IPs of eth1 (192.168.100.41, 192.168.100.42) and add them as virtual IPs using following command:
   Network> ip addr add <old-eth1-physical-ip> <old-eth1-subnetmask> virtual eth1

   Note: This is temporary action. Once the separation of data and management subnet is done, the virtual IPs can be removed.

   For example:
   Network> ip addr add 192.168.100.41 255.255.252.0 eth1 virtual eth1
   ACCESS ip addr SUCCESS V-493-10-1381 ip addr add successful.
   In this command:
   - The IP (192.168.100.41) is the old eth1 physical IP which is free now (after step 4)
   - Netmask is the eth1 IP's subnet mask (255.255.255.0)
   - Device is eth1 because you want to have the virtual IP on eth1

   For example:
   Network> ip addr add 192.168.100.42 255.255.252.0 virtual eth1
   ACCESS ip addr SUCCESS V-493-10-1381 ip addr add successful.
   In this command:
   - The IP (192.168.100.42) is the old eth1 physical IP which is free now (after step 4)
   - Netmask is the eth1 IP's subnet mask (255.255.255.0)
   - Device is eth1 we want to have virtual IP is on eth1

   After both the **ip addr add** operations are complete, verify that both the virtual IPs are on eth1 on both the nodes (app742_01 and app742_02).
   Network> ip addr show

```
IP             Netmask/Prefix Device Node       Type     Status
--             -------------- ------ ----        ----     ------
192.168.20.25  255.255.255.0  eth1   app742_01 Physical
192.168.20.26  255.255.255.0  eth1   app742_02 Physical
192.168.100.51 255.255.255.0  eth4   app742_01 Physical
192.168.100.52 255.255.255.0  eth5   app742_01 Physical
192.168.100.53 255.255.255.0  eth4   app742_02 Physical
```

```
192.168.100.54 255.255.255.0  eth5   app742_02 Physical
192.168.100.50 255.255.255.0  eth4   app742_01 Virtual  ONLINE (Con IP)
192.168.100.55 255.255.255.0  eth4   app742_02 Virtual  ONLINE
192.168.100.56 255.255.255.0  eth4   app742_01 Virtual  ONLINE
192.168.100.57 255.255.255.0  eth5   app742_02 Virtual  ONLINE
192.168.100.58 255.255.255.0  eth5   app742_01 Virtual  ONLINE
192.168.100.41 255.255.255.0  eth1   app742_02 Virtual  ONLINE
192.168.100.42 255.255.255.0  eth1   app742_01 Virtual  ONLINE
```

6. Change the physical network connections for eth1 and connect it to the switch which is in subnet.

7. Login to the Veritas Access node's server console to perform further steps.

8. Use the Appliance CLISH to find the currentAccess management console node by going in maintenance mode from any of the Appliance node.
   /home/maintenance # hagrp -state ManagementConsole

```
#Group            Attribute             System        Value
ManagementConsole State                 app742_01   |OFFLINE|
ManagementConsole State                 app742_02   |ONLINE|
```

   Note: The Access management console is online on the second node (app742_02).

9. Login to the node where the management node is online from the Appliance CLISH and go in to maintenance mode and enterthe following command to open Access CLISH for further route related operations.
   /home/maintenance # /opt/VRTSnas/clish/bin/clish -u admin

10. Once the Access CLISH is open, delete the the global default route of data network.
    Enter the following command to delete the global default gateway:
    Network> ip route del all 0.0.0.0 0.0.0.0 via <gateway> dev eth1 scope=global
    For example:
    Network> ip route del all 0.0.0.0 0.0.0.0 via 192.168.100.1 dev eth1 scope=global
    ACCESS ip route SUCCESS V-493-10-1462 ip route del success

    In this command:
    - Gateway IP is the current default gateway IP (192.168.100.1)
    - Use the **ip route show** command to find the default gateway IP.

11. Add new IP routes. Enter the following command to add the global default gateway:
    Network> ip route add all 0.0.0.0 0.0.0.0 via <gateway> dev eth1 scope=global
    For example:
    Network> ip route add all 0.0.0.0 0.0.0.0 via 192.168.20.1 dev eth1 scope=global
    ACCESS ip route SUCCESS V-493-10-1462 ip route add success

    In this command:
    - Gateway IP is the new subnet's default gateway IP (192.168.20.1)
    - Device Name is eth1 as eth1 is moving to other subnet (management subnet)

12. Delete the virtual IPs assigned to eth1.
    Network> ip addr del <eth1_virtual_ip>

For example:

```
Network> ip addr del 192.168.100.41
ACCESS ip addr SUCCESS V-493-10-1381 ip addr del successful.
```

In this command:

- The current virtual IP address of eth1 (192.168.100.41)

After both the **ip addr del** operations are complete, verify that both the virtual IPs are deleted.

```
Network> ip addr show
IP              Netmask/Prefix Device Node       Type    Status
--              -------------- ------ ----       ----    ------
192.168.20.25   255.255.255.0   eth1   app742_0   Physical
192.168.20.26   255.255.255.0   eth1   app742_02  Physical
192.168.100.51  255.255.255.0   eth4   app742_01  Physical
192.168.100.52  255.255.255.0   eth5   app742_01  Physical
192.168.100.53  255.255.255.0   eth4   app742_02  Physical
192.168.100.54  255.255.255.0   eth5   app742_02  Physical
192.168.100.50  255.255.255.0   eth4   app742_01  Virtual ONLINE (Con IP)
192.168.100.55  255.255.255.0   eth4   app742_02  Virtual ONLINE
192.168.100.56  255.255.255.0   eth4   app742_01  Virtual ONLINE
192.168.100.57  255.255.255.0   eth5   app742_02  Virtual ONLINE
192.168.100.58  255.255.255.0   eth5   app742_01  Virtual ONLINE
```

13. Move the management console IP to eth1.

```
Network> ip addr modify <current_console_ip> <new_IP> <new_netmask> eth1
```

For example:

```
Network> ip addr modify 192.168.100.50 192.168.20.50 255.255.255.0 eth1
ACCESS ip addr INFO V-493-10-1468 All existing SSH session will be terminated,
please logon with new Console ip.
```

In this command:

- Specify new IP address from the management subnet
- Specify netmask from the management subnet
- Device name (Interface connect to the management network, eth1)

14. Login to the Access management Console IP using SSH from any client in the management subnet.

Note: Since all the network configurations of the cluster are updated now, you can start all the services on the Veritas Access nodes which you stopped before updating the network configuration.

Use case 3: Cluster is already configured with Veritas Access 7.4.2 version and you want to move the data NICs to a different subnet and the management NIC (eth1) remains in the same subnet

This section includes the following topics:

Prerequisites

- The Veritas Access 7.4.2.100 patch is installed
- All the network interfaces should be in the same subnet (management subnet).

Configuring the network

Note: Since the network configuration of the cluster is getting changed, some I/O pause/stop/interrupt occurs for all the currently running service on the Access nodes. It is recommended that you stop all the service such as NFS, CIFS, FTP, S3, ISCSI, Veritas Data Deduplication, Cloud Catalyst, and Enterprise Vault.

1. Add the eth1 network interface to the Veritas Access configuration.
```
Network> device add eth1
100% [#] Success: device eth1 added.
```

2. Move the management console IP to eth1.
```
Network> ip addr modify <old_ip> <new_IP> <new_netmask> eth1

ACCESS ip addr INFO V-493-10-1468 All existing SSH session will be terminated,
please logon with new Console ip.
```

3. Login to the Veritas Access CLISH using the console IP and eth1 interface.
```
login as: admin
admin@192.168.10.30's password:

Network> ip addr show
IP             Netmask/Prefix Device Node         Type    Status
--             -------------- ------ ----         ----    ------
192.168.10.12 255.255.255.0   eth1 accessupg_02 Physical
192.168.10.11 255.255.255.0   eth1 accessupg_01 Physical
192.168.10.13 255.255.255.0   eth4 accessupg_01 Physical
192.168.10.14 255.255.255.0   eth5 accessupg_01 Physical
192.168.10.15 255.255.255.0   eth4 accessupg_02 Physical
192.168.10.16 255.255.255.0   eth5 accessupg_02 Physical
192.168.10.30 255.255.255.0   eth1 accessupg_01 Virtual ONLINE (Con IP)
192.168.10.17 255.255.255.0   eth4 accessupg_01 Virtual ONLINE
192.168.10.18 255.255.255.0   eth4 accessupg_02 Virtual ONLINE
192.168.10.19 255.255.255.0   eth5 accessupg_01 Virtual ONLINE
192.168.10.20 255.255.255.0   eth5 accessupg_02 Virtual ONLINE
```

4. Modify the physical and virtual IPs of eth4 and eth5 to the required subnet (which is different from eth1 subnet).
```
Network> ip addr modify <old_ip> <new_IP> <new_netmask>
```
Modify all the IPs for the to which the interfaces eth4 and eth5 are connected.

5. Verify that all the IPs are modified correctly.

```
Network> ip addr show
IP             Netmask/Prefix Device Node          Type    Status
--             -------------- ------ ----          ----    ------
192.168.10.12 255.255.255.0  eth1   accessupg_02 Physical
192.168.10.11 255.255.255.0  eth1   accessupg_01 Physical
192.168.20.13 255.255.255.0  eth4   accessupg_01 Physical
192.168.20.14 255.255.255.0  eth5   accessupg_01 Physical
192.168.20.15 255.255.255.0  eth4   accessupg_02 Physical
192.168.20.16 255.255.255.0  eth5   accessupg_02 Physical
192.168.10.30 255.255.255.0  eth1   accessupg_01 Virtual ONLINE (Con IP)
192.168.20.17 255.255.255.0  eth4   accessupg_01 Virtual ONLINE
192.168.20.18 255.255.255.0  eth4   accessupg_02 Virtual ONLINE
192.168.20.19 255.255.255.0  eth5   accessupg_01 Virtual ONLINE
192.168.20.20 255.255.255.0  eth5   accessupg_02 Virtual ONLINE
```

6. Modify the network connections at the switch level (physical connectivity) for the eth4 and eth5 interfaces.

7. Add the default route entry and new gateway IP for the eth4 and eth5 interfaces.
   ```
   Network> ip route add all 0.0.0.0 0.0.0.0 via <gateway> dev any scope=local
   ACCESS ip route SUCCESS V-493-10-1462 ip route add success
   ```

8. Verify the connectivity of all the IP addresses from the clients of respective subnets.

Reconnecting the protocols after changing the data network to different subnet

After changing the physical cable connections to the respective subnets, you can reconnect the applications.

1. Veritas Data Deduplication:
   Perform the following steps after the patch upgrade is complete.
   - Before changing the IPs of the data network, eth4 and eth5, note down the deduplication user which is used to configure from the Access management console.
     ```
     Dedupe> listuser
     ```
   - Unconfigure the deduplication before modifying the IPs from the Access management console.
     ```
     Dedupe> unconfig
     ACCESS dedupe INFO V-493-10-0 Removing deduplication server configuration...
     ACCESS dedupe INFO V-493-10-0 Deduplication server unconfigured
     successfully.
     ```
   - Configure deduplication using the new virtual IP with the same user which was listed in the previous step.
     ```
     Dedupe> config <filesystem_list> <new_virtual_IP> <username>
     Enter Password:<password>
     ACCESS dedupe INFO V-493-10-0 configuring deduplication server...
     ACCESS dedupe INFO V-493-10-0 Deduplication server configured successfully
     ```
   - Make sure the NetBackup master, media and client servers are connected to the newly added subnets and configured accordingly.
   - If the disk pool is created with a host name, you can modify the DNS entries with new IPs against the host.

2. NFS, CIFS, FTP, ObjectAccess (S3):
   Perform the following steps after the patch upgrade is complete.
   - Unmount the NFS, CIFS and FTP, S3 clients.
   - Modify the physical IP, and virtual IP of eth4 and eth5 to the required subnet. You may get a warning message while changing the virtual IPs.

Network> ip addr modify <old_ip> <new_IP> <new_netmask>

```
ACCESS cifs WARNING V-493-10-258 CIFS share 'cifs_share' will be
redistributed to other virtual IP address due to modification, interruption
for the share access is expected.
ACCESS ip addr SUCCESS V-493-10-1381 ip addr modify successful.
```

- Make sure all the NFS, CIFS, FTP and S3 clients are connected to new subnet.
- Mount the respective clients using the respective protocol commands.

Support for IBM Spectrum® Protect

This release supports using Access S3 as a storage target for IBM Spectrum Protect.
For further information on this solution, please refer to the *Access Appliance 3340 with IBM Spectrum Protect Solution* whitepaper at https://www.veritas.com/protection/access-appliance/resources

IBM Spectrum Protect expects the following configuration information when using Access as an S3 storage target:

- S3 endpoint URL (i.e. s3.<clustername>)
- An S3 bucket to be created. Bucket creation can be done via the Access command line using the **map** function.
- Access keys and secret key
- If using SSL, then the Access certificate needs to be added to the IBM Spectrum Protect keystore.

Refer to the Appendix section of the above whitepaper for an example of how to configure the Access Appliance 3340 as a cloud container storage pool for IBM Spectrum Protect.

Managing alerts and notifications

You can add an email add ignore-string functionality to an existing group as well as delete an existing ignore notification string.

If you want to block specific email notifications, then you can add the notification string to an email group. To add the notification string, enter the following:

```
Report> email add ignore-string <group> <notification-to-ignore>
```

Where *<group>* specifies the group to which the email address is added and *<notification-to-ignore>* specifies the notification that you want to ignore.

If you want to delete an existing ignore notification string in an email group, enter the following:

```
Report> email del ignore-string <group> <string-to-delete>
```

Where *<group>* specifies the group to which the email address is added and *<string-to-delete>* specifies the notification that you want to delete.

Veritas Access also classifies event notifications by type. You can set the event filter to specify which type of events to include in notifications. Notifications are sent only for events matching the given filter. New components have been added to the filters to include options such as, admin, backup, CIFS, cluster, database, FTP, network, NFS, OpenStack, replication, report, SmartIO, storage, support, system and upgrade.

For more details, refer to the *Veritas Access Administrator's Guide* on SORT.

Retrieving and sending debugging information

A new module, **nas-prostacks**, is added that collects stack trace and memory usage for all running process. This module use *collect_memory_stats.sh* script to collect various memory related information in a file which can be used later for analysis.

Known issues

This section documents the known issues of this release.

The PUT operation fails for virtual hosted style requests for AWS signature version 2 and 4.

Workaround:
The S3 clients should use path-based addressing style requests for the PUT operation.

Adding a node to a cluster fails in an environment where management and data subnets are in the same network

Workaround:
If you want to add a node to a cluster which is upgraded to 7.4.2.100, perform the following steps:

1. Assign IP to the eth1 interface of the new node.
2. Upgrade the new node (which is on 7.4.2 version) to 7.4.2.100 using the steps here.
3. Add new node to the cluster using the following command:
   `cluster> add <new node> eth1 <IP>`

The add node operation is not supported in an environment where management and data subnets are on different network

Workaround: If you want to add a node in an environment where you have separate management and data subnets, then call Veritas Support.

Fixed issues in this release

This section includes the issues fixed since the last release.

Fixed issues	Description
3972425	ISSUES fixed in this EEB: IA-17240: disable selective email notifications IA-17163: /etc/pam.d/ files got empty IA-17151: debuginfo appears hung IA-17244: When balancing vipgroups, Veritas Data Deduplication is moved between nodes
3971871	The EEB bundle contains fixes for Veritas Data Deduplication issues on Access 7.4.2
3971580	Fix Access Appliance memory corruption issue
3971549	This EEB fixes following defect: When balancing vipgroups, Veritas Data Deduplication is moved between nodes
3971116	Issues fixed in this EEB: ISSUE1: /etc/pam.d/ files got empty preventing login to the node ISSUE2: debuginfo collection hung
3964974	Fix reboot/shutdown issue in cluster nodes
IA-19171	Not able to create key if multiple admin_endpoints are set
IA-18859	Callhome Test failed due to updated settings conflict with firewall when cluster is setup
IA-18780	Remove 80% storage notification for Licensing in GUI
IA-18615	Network show command does not print the information about all the NIC Statistics
IA-18600	Certificate is not generated from other node if SSL is enabled and management console switches to the other node
IA-18529	NTP add clish command failing
IA-18484	Bucket delete operation failed for mapped bucket
IA-16655	Access - S3 Performance for small range reads of 256K needs to be optimized
APPSOL-95056	Includes the Access Appliance shell menu audit functionalities. Resolves the appliance reboot hung issue. Updates the Access product JSON for AutoSupport.
APPSOL-90738	Resolves the SNMP configuration failure when community string includes '$' or '#'.
APPSOL-98019	After running DataCollect from the Access Appliance shell menu, unable to share DataCollect.zip.
APPSOL-98077	Log 'Share Open' command takes a long time to complete.
APPSOL-102605	Cannot SSH to cluster nodes after configuring Acess in a pure IPv6 environment.

For information on all the other features, refer to the Veritas Access Appliance 7.4.2 documentation which is available online. The latest version of the product documentation is available on the SORT website.

Note: The FPE cache limit is changed from 75% to 50% as part of this patch. Before installing the patch, ensure that you note down the cache limit. If the cache limit is lower than 50% before the patch is applied, the patch application sets the value to 50% after the patch is installed. You must manually change the cache value to the original value after the patch installation if the original value before installation of the patch was lower than 50%.

Veritas recommends the following if you increase the RAM on the Access 3340 appliance:

- If the 3340 cluster nodes each have 350 GB RAM or more, use a value of 25%.
- If the 3340 cluster nodes each have less than 350 GB RAM , use a value of 50%

For more information, refer to https://www.veritas.com/support/en_US/article.100045745.html