c

Veritas Access Appliance

7.4.2.200 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 (7.4.2/7.4.2.100) 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 7.4.2.200, refer to the following technote:
https://www.veritas.com/support/en_US/article.100046753.html

New features and enhancements included in this release:

- Access base licenses can be stacked to support additional storage capacity. You can combine multiple licenses on the same appliance to increase the licensed storage capacity. The cumulative licensed capacity is displayed when you obtain and register additional Access base licenses.
- Deployment enhancements include:
    - Ability to configure a separate management and data network during Access cluster configuration
    - Support for non-contiguous physical and virtual IP addresses for the data network
    - Option to specify the number of virtual IP addresses for each network interface in the data network
    - Option to specify a private IP address range to configure a different private network other than the default private network (172.16.x.x)
    - Option to configure the NTP server to synchronize the time across the cluster nodes
    - Support a maximum of 55 characters for cluster and host names
- Support for multiple data subnets
- Support for multiple domains across networks for Veritas Data Deduplication
- New enhancements to the alerts framework
- Storage expansion options for the appliance include:
    - Adding a storage shelf with 10-TB disks to an appliance that uses a storage shelf of 4-TB disks.
    - Adding a storage shelf with 4-TB disks to an appliance that uses a storage shelf of 4-TB disk.

  With 4-TB disk drives, a storage shelf provides 254.4TiB (280 TB) of usable data storage capacity. You can now add a storage shelf of 10-TB disk drives to increase the storage capacity by 636TiB (700 TB) or add a storage shelf with 4-TB disks to increase the storage capacity by 254.4TiB (280 TB).

Licensing updates

You can procure only an Access base license to increase the licensed storage capacity. You need to purchase additional Access base licenses when you add storage shelves to increase the appliance storage capacity.

Starting with Access Appliance version 7.4.2.200, Access base licenses can be stacked, and you can view the cumulative licensed storage capacity in the Access web interface. Previously, stacking of license keys was not supported, which resulted in suppression of the existing license when a new license was registered. Instead of the cumulative storage capacity, the storage capacity of only the newly added license was displayed.

If you have a valid Veritas Data Deduplication license from a prior release, you can view the storage capacity of the Data Deduplication license in the Access command-line interface and the web interface. The following scenarios show how the Veritas Data Deduplication licenses registered prior to 7.4.2.200 are displayed in version 7.4.2.200 where only stacking of Access base licenses is supported:

Scenario 1: Access base license is registered, and a new Access base license key is added
When the new Access base license is registered, the cumulative licensed capacity of existing license and newly added license is displayed.

Scenario 2: Access base license with an add-on license to use the Veritas Data Deduplication service is registered and a new Access base license is added
When the new Access base license is registered, the cumulative licensed capacity of the existing base license and the newly added Access base license is displayed. Existing licensed capacity for the add-on Veritas Data Deduplication is displayed. The licensed capacity of the add-on Veritas Data Deduplication license is not included in the cumulative licensed capacity.

Scenario 3: Access base license which includes the add-on license to use the Veritas Data Deduplication service is registered, and a new Access base license is added
When the new base license is added, the cumulative licensed capacity of the existing base license and the newly added Access base license is displayed. Existing licensed capacity for the add-on Veritas Data Deduplication is displayed. The licensed capacity of the add-on Veritas Data Deduplication license is not included in the cumulative licensed capacity.

The Trialware license, which is a built-in evaluation license activates automatically after you complete the appliance initial configuration and can be used for 60 days. Veritas recommends that you register a perpetual license if the Trialware license expires or register additional perpetual licenses of appropriate capacity when you expand the appliance storage capacity. If you exceed the storage capacity, the product usage is not affected and there is no disruption of Access services. However, Veritas recommends that you procure a new license or renew your license to a higher storage capacity.

If the Trialware license expires or you exceed the licensed storage capacity, frequent notifications about using the trialware license beyond its evaluation period or exceeding the storage capacity are displayed in the Access web interface. If the appliance is configured for AutoSupport, alerts are generated for the following events :

- License has expired
- Storage utilization exceeds the total licensed capacity

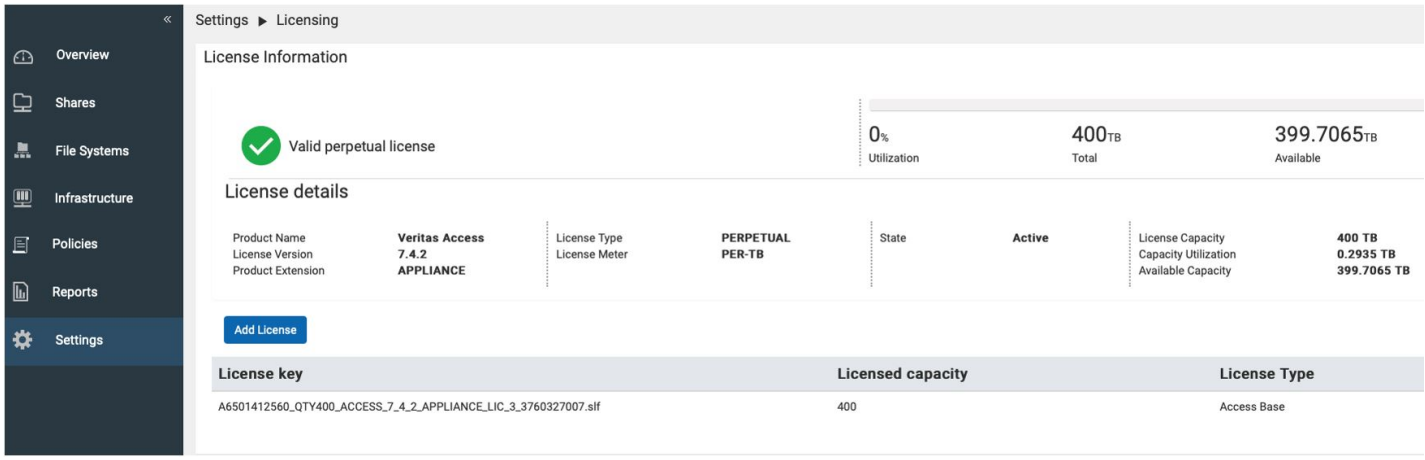
When you upgrade from version 7.4.2 or 7.4.2.100 to version 7.4.2.200, the existing licenses are not affected. You can continue to use the licenses that were valid prior to the upgrade after you upgrade to the newer version.

Registering a license using the Access web interface

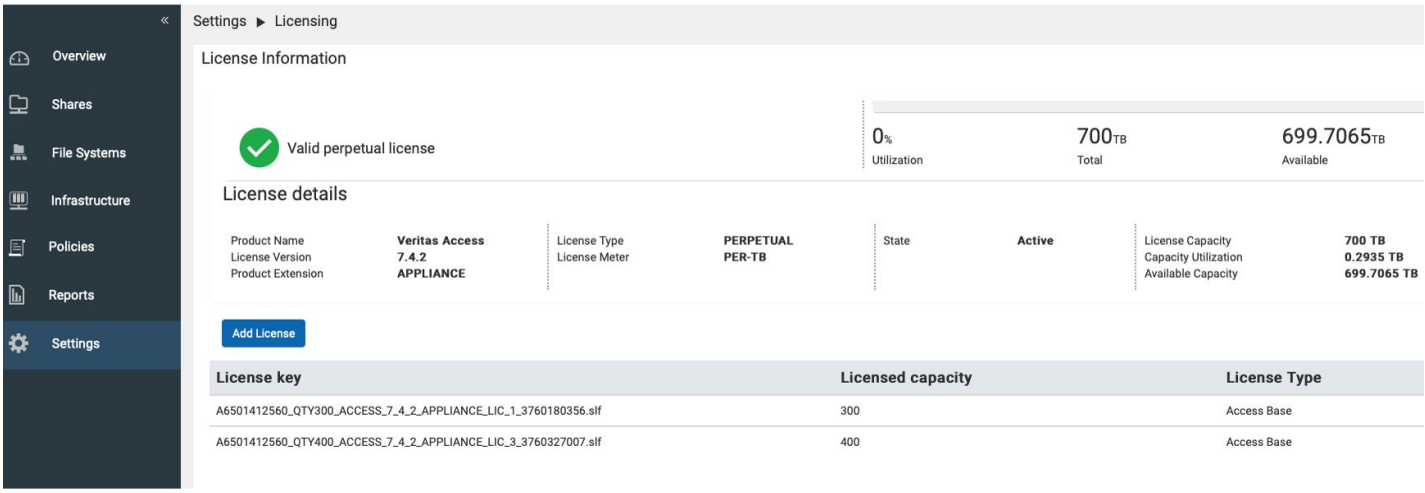
1. Log in to the Access web interface using the http://consoleIP:14161/ URL where *console IP* is the management console IP address that hosts the Access GUI after the cluster is configured.
2. In the Access web interface, in the left navigation, click **Settings**.
3. Click **Licensing**, and then click **Add License**.
4. In the **Add License** dialog box, click Browse to select the .slf license key and click **Add**.

You can view the details of the registered licenses on the **Settings > Licensing** page of the Access web interface. The licensed storage capacity and utilization graph is displayed for a perpetual license and the duration and expiry date for the built-in Trialware license. You can view additional details such as the cumulative licensed storage, license type and status, and license key details.

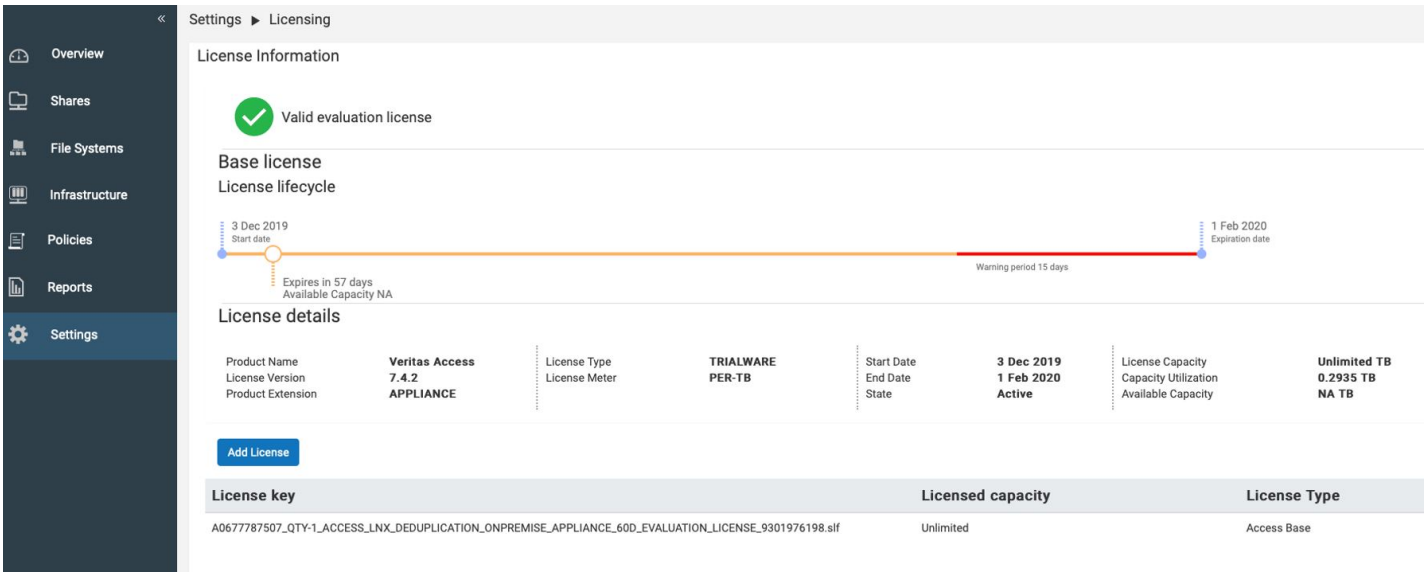
The following figure shows the details that are displayed when a perpetual license of 400 TB is registered:



The following figure shows the details that are displayed when an additional perpetual 300 TB Access base license is registered:



The following figure shows the details that are displayed for the built-in Trialware license:



Registering a license using the Access command-line interface

You can add a license by using the **System> license add** command and view the details for each of the registered license keys using the **System> license list** command. The **System> license list details** command shows cumulative licensed storage for all the registered license keys.

The following sample output shows the details that are displayed when you run the **System> license list** and **System> license list details** commands when perpetual Access base licenses of 400 TB and 300 TB are stacked to get a cumulative licensed storage of 700 TB:

```
app> system license list details
Product name    Version  Product Extension  License Type  License Meter  State   License Capacity  Raw Capacity
==============  =======  =================  ============  =============  ======  ================  ============
Veritas Access  7.4.2    APPLIANCE          PERPETUAL     PER-TB         Active  700               3.7471
app>
app> system license list
State   License Key                                                  License Capacity  License Type  Start Date  End Date
======  =========================================================  ================  ============  ==========  ========
Active  A6501412560_QTY300_ACCESS_7_4_2_APPLIANCE_LIC_1_3760180356.slf  300               Access Base   NA          NA
Active  A6501412560_QTY400_ACCESS_7_4_2_APPLIANCE_LIC_3_3760327007.slf  400               Access Base   NA          NA
```

The following sample output shows the details that are displayed when you run the **System> license list** and **System> license list details** commands when a built-in Trialware license is activated:

```
app> system license list details
Product name    Version  Product Extension  License Type  License Meter  State   License Capacity  Raw Capacity
==============  =======  =================  ============  =============  ======  ================  ============
Veritas Access  7.4.2    APPLIANCE          TRIALWARE     PER-TB         Active  Unlimited         3.7471
app>
app> system license list
State   License Key                                                                                License Capacity  License Type  Start Date  End Date
======  =============================================================================================  ================  ============  ==========  ==========
Active  A0677787507_QTY-1_ACCESS_LNX_ONPREMISE_APPLIANCE_60D_EVALUATION_LICENSE_1219604512.slf  Unlimited         Access Base   2019-10-25  2019-12-23
```

Configuring a separate management and data network during cluster configuration

When you configure the Access cluster, you can configure a separate management and data network if the management NIC and the public NICs are in different subnets. Previously, separation of networks was not possible during the initial configuration. If you choose to configure a separate management and data network, ensure that you specify a console IP, which is in the management network IP range.

Prerequisites

- The Veritas Access 7.4.2.200 release update is installed
- The eth1 NIC is connected to the management subnet
- The data NICs eth4 and eth5 are connected to the data subnet

The following example shows how to configure a separate management and data network during cluster configuration. The deployment enhancements, which are new in this release are highlighted in bold:

```
sclinslnxq15vm01p0.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 at least four physical and virtual IP addresses are reserved for the
Access cluster.

Note the following cluster naming rules:

- The cluster name must be at least three characters long and no more than 55
characters in length.

- 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: vaupg
>> Enter the IP addresses of the appliance nodes for clustering (separated by a space):
10.209.192.206 10.209.192.208
>> Enter the maintenance user password of the appliance nodes:
>> Do you want to configure network bonding for public networks? [yes,no] no
>> Enter the starting public IP address or 4 individual public IP addresses separated
by a comma or a space for the data network (The IP addresses can be IPv4 or IPv6 and
need not be contiguous. An IPv4 range is supported. For example, 10.200.0.5-10):
192.168.10.2,192.168.10.5,192.168.10.10,192.168.10.13
>> Enter the number of virtual IP addresses to assign to each network interface in the
data network (0): 1
```

```
>> Enter the starting virtual IP address, or 4 individual virtual IP addresses
separated by a comma or a space (The virtual IP addresses can be IPv4 or IPv6 and need
not be contiguous. An IPv4 range is supported. For example, 10.200.0.5-10):
192.168.10.22,192.168.10.25,192.168.10.28,192.168.10.30
>> Enter the subnet mask for the data network (255.255.248.0): 255.255.255.0
>> Enter the IP address of the gateway of the data network (10.84.144.1): 192.168.10.1
>> Enter the console virtual IP address: 10.209.194.38
>> Enter the DNS server IP address: 172.16.8.12
>> Enter the DNS server domain name: engba.veritas.com
>> Do you want to configure an NTP server? [yes,no] no

[Info] To set up the cluster, the time between the appliance nodes must be
synchronized. Use the Network > Date and the Network > TimeZone commands to synchronize
the time, and then continue with the cluster configuration; or go to Settings > Service
Management in the Access web interface to synchronize the time after the cluster is
configured.
>> Enter the starting private IP address (172.16.0.3): 180.20.0.6

====================
Summary of the cluster configuration:
Cluster name: vaupg
Appliance nodes for clustering: 10.209.192.206, 10.209.192.208
Nodes with public IP: 192.168.10.2,192.168.10.5,192.168.10.10,192.168.10.13
Virtual IP addresses: 192.168.10.22,192.168.10.25,192.168.10.28,192.168.10.30
Netmask for data network IP address: 255.255.255.0
Data network gateway IP address: 192.168.10.1
DNS server IP address: 172.16.8.12
DNS server domain name: engba.veritas.com
Console virtual IP address: 10.209.194.38
Netmask for management network IP address: 255.255.248.0
Management network gateway IP address: 10.84.144.1
Private IP starting address: 180.20.0.6
====================
>> Do you want to continue? [yes,no]
```

Wait for the cluster configuration to complete.

After the cluster is configured successfully, the network configuration is as shown below:

```
vaupg> network ip addr show

IP              Netmask/Prefix  Device     Node       Type      Status
--              --------------  ------     ----       ----      ------
192.168.10.5    255.255.255.0   eth5       vaupg_01   Physical
192.168.10.13   255.255.255.0   eth5       vaupg_02   Physical
192.168.10.2    255.255.255.0   eth4       vaupg_01   Physical
192.168.10.10   255.255.255.0   eth4       vaupg_02   Physical
10.209.192.206 255.255.252.0   eth1       vaupg_01   Physical
10.209.192.208 255.255.252.0   eth1       vaupg_02   Physical
10.209.194.38   255.255.252.0   eth1       vaupg_01   Virtual   ONLINE (Con IP)
192.168.10.22   255.255.255.0   eth5       vaupg_01   Virtual   ONLINE
192.168.10.25   255.255.255.0   eth5       vaupg_02   Virtual   ONLINE
192.168.10.28   255.255.255.0   eth4       vaupg_02   Virtual   ONLINE
192.168.10.30   255.255.255.0   eth4       vaupg_01   Virtual   ONLINE
```

Support for multiple data subnets

Access Appliance now supports multiple data subnets. This is applicable to all the protocols that the Access Appliance supports. If you have different subnets, you can access the services of the Access Appliance cluster via those subnets. The protocol specific entities and features decide how the subnets are utilized by the individual protocol. Multiple subnets can be configured with or without multiple VLANs.

Note: Data network isolation depends on the customer network configuration. The application configuration in Access Appliance does not restrict the customer from using the same network for multiple protocols.

If you have multiple subnets and you want to create multiple VLANs for each subnet, then Veritas recommends the following:

- For each subnet, add the required number of IPs as physical IPs to create the VLAN. The required number of IPs is equal to the number of nodes that are present. Do not add extra IPs.
- Create the VLAN using the **network> vlan add** command. The IPs that you added are automatically picked for VLAN creation.
- Add a route for the newly created subnet, if required.

If you want to create another VLAN, repeat the above steps.

Note: If the IPs are not added in the correct sequence, the **network> vlan add** command may pick IPs which belong to different subnets.

For example:

```
Network ip addr show

IP              Netmask/Prefix   Device   Node      Type      Status
--              --------------   ------   ----      ----      ------
192.168.10.5    255.255.255.0    eth5     vaupg_01  Physical
192.168.10.13   255.255.255.0    eth5     vaupg_02  Physical
192.168.10.2    255.255.255.0    eth4     vaupg_01  Physical
192.168.10.10   255.255.255.0    eth4     vaupg_02  Physical
10.209.192.206  255.255.252.0    eth1     vaupg_01  Physical
10.209.192.208  255.255.252.0    eth1     vaupg_02  Physical
10.209.194.38   255.255.252.0    eth1     vaupg_01  Virtual   ONLINE (Con IP)
192.168.10.22   255.255.255.0    eth5     vaupg_01  Virtual   ONLINE
192.168.10.25   255.255.255.0    eth5     vaupg_02  Virtual   ONLINE
192.168.10.28   255.255.255.0    eth4     vaupg_02  Virtual   ONLINE
192.168.10.30   255.255.255.0    eth4     vaupg_01  Virtual   ONLINE


Network> ip addr modify 192.168.10.2 192.168.30.2 255.255.255.0
ACCESS ip addr WARNING V-493-10-0 Given IP (192.168.10.2) is not a virtual ip.
ACCESS ip addr SUCCESS V-493-10-1381 ip addr modify successful.

Network> ip addr modify 192.168.10.10 192.168.30.10 255.255.255.0
ACCESS ip addr WARNING V-493-10-0 Given IP (192.168.10.10) is not a virtual ip.
ACCESS ip addr SUCCESS V-493-10-1381 ip addr modify successful.

Network> ip addr modify 192.168.10.28 192.168.30.15 255.255.255.0
ACCESS ip addr SUCCESS V-493-10-1381 ip addr modify successful.

Network> ip addr modify 192.168.10.30 192.168.30.20 255.255.255.0
```

```
ACCESS ip addr SUCCESS V-493-10-1381 ip addr modify successful.

Network> ip addr show
IP              Netmask/Prefix  Device  Node     Type     Status
--              --------------  ------  ----     ----     ------
192.168.10.5    255.255.255.0   eth5    vaupg_01 Physical
192.168.10.13   255.255.255.0   eth5    vaupg_02 Physical
192.168.30.2    255.255.255.0   eth4    vaupg_01 Physical
192.168.30.10   255.255.255.0   eth4    vaupg_02 Physical
10.209.192.206 255.255.252.0   eth1    vaupg_01 Physical
10.209.192.208 255.255.252.0   eth1    vaupg_02 Physical
10.209.194.38   255.255.252.0   eth1    vaupg_01 Virtual  ONLINE (Con IP)
192.168.10.22   255.255.255.0   eth5    vaupg_01 Virtual  ONLINE
192.168.10.25   255.255.255.0   eth5    vaupg_02 Virtual  ONLINE
192.168.30.15   255.255.255.0   eth4    vaupg_02 Virtual  ONLINE
192.168.30.20   255.255.255.0   eth4    vaupg_01 Virtual  ONLINE

Network> ip route show
vaupg_01
----------------
IPv4 routing table: main
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0         10.209.192.1    0.0.0.0         UG     0    0       0     eth1
10.209.192.0    0.0.0.0         255.255.252.0   U      0    0       0     eth1
180.20.0.0      0.0.0.0         255.255.255.0   U      0    0       0     eth2
192.168.10.0    0.0.0.0         255.255.255.0   U      0    0       0     eth5
192.168.30.0    0.0.0.0         255.255.255.0   U      0    0       0     eth4
192.168.229.0   0.0.0.0         255.255.255.0   U      0    0       0     eth0

IPv4 routing table: 3
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
0.0.0.0         10.209.192.1    0.0.0.0         UG     0    0       0     eth1
10.209.192.0    0.0.0.0         255.255.252.0   U      0    0       0     eth1

IPv4 routing table: 2
================================================================================
Destination     Gateway  Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
192.168.30.0    0.0.0.0  255.255.255.0   U      0    0       0     eth4

IPv4 routing table: 1
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0         192.168.10.1    0.0.0.0         UG     0    0       0     eth5
192.168.10.0    0.0.0.0         255.255.255.0   U      0    0       0     eth5

vaupg_02
----------------
IPv4 routing table: main
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0         10.209.192.1    0.0.0.0         UG     0    0       0     eth1
10.209.192.0    0.0.0.0         255.255.252.0   U      0    0       0     eth1
```

```
180.20.0.0      0.0.0.0         255.255.255.0   U       0    0        0      eth2
192.168.10.0    0.0.0.0         255.255.255.0   U       0    0        0      eth5
192.168.30.0    0.0.0.0         255.255.255.0   U       0    0        0      eth4
192.168.229.0   0.0.0.0         255.255.255.0   U       0    0        0      eth0

IPv4 routing table: 3
================================================================================
Destination    Gateway        Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0        10.209.192.1   0.0.0.0         UG     0    0       0     eth1
10.209.192.0   0.0.0.0        255.255.252.0   U      0    0       0     eth1

IPv4 routing table: 2
================================================================================
Destination    Gateway   Genmask         Flags  MSS  Window  irtt  Iface
192.168.30.0   0.0.0.0   255.255.255.0   U      0    0       0     eth4

IPv4 routing table: 1
================================================================================
Destination    Gateway        Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0        192.168.10.1   0.0.0.0         UG     0    0       0     eth5
192.168.10.0   0.0.0.0        255.255.255.0   U      0    0       0     eth5

Network> ip route add all 0.0.0.0 0.0.0.0 via 192.168.30.1 dev any scope=local
ACCESS ip route SUCCESS V-493-10-1462 ip route add success

Network> ip route show
vaupg_01
----------------
IPv4 routing table: main
================================================================================
Destination     Gateway        Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0         10.209.192.1   0.0.0.0         UG     0    0       0     eth1
10.209.192.0    0.0.0.0        255.255.252.0   U      0    0       0     eth1
180.20.0.0      0.0.0.0        255.255.255.0   U      0    0       0     eth2
192.168.10.0    0.0.0.0        255.255.255.0   U      0    0       0     eth5
192.168.30.0    0.0.0.0        255.255.255.0   U      0    0       0     eth4
192.168.229.0   0.0.0.0        255.255.255.0   U      0    0       0     eth0

IPv4 routing table: 3
================================================================================
Destination    Gateway        Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0        10.209.192.1   0.0.0.0         UG     0    0       0     eth1
10.209.192.0   0.0.0.0        255.255.252.0   U      0    0       0     eth1

IPv4 routing table: 2
================================================================================
Destination    Gateway        Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0        192.168.30.1   0.0.0.0         UG     0    0       0     eth4
192.168.30.0   0.0.0.0        255.255.255.0   U      0    0       0     eth4

IPv4 routing table: 1
================================================================================
Destination    Gateway        Genmask         Flags  MSS  Window  irtt  Iface
```

```
================================================================================
0.0.0.0         192.168.10.1    0.0.0.0         UG      0    0        0      eth5
192.168.10.0    0.0.0.0         255.255.255.0   U       0    0        0      eth5

vaupg_02
----------------
IPv4 routing table: main
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0         10.209.192.1    0.0.0.0         UG      0    0        0      eth1
10.209.192.0    0.0.0.0         255.255.252.0   U       0    0        0      eth1
180.20.0.0      0.0.0.0         255.255.255.0   U       0    0        0      eth2
192.168.10.0    0.0.0.0         255.255.255.0   U       0    0        0      eth5
192.168.30.0    0.0.0.0         255.255.255.0   U       0    0        0      eth4
192.168.229.0   0.0.0.0         255.255.255.0   U       0    0        0      eth0

IPv4 routing table: 3
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0         10.209.192.1    0.0.0.0         UG      0    0        0      eth1
10.209.192.0    0.0.0.0         255.255.252.0   U       0    0        0      eth1

IPv4 routing table: 2
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
================================================================================
0.0.0.0         192.168.30.1    0.0.0.0         UG      0    0        0      eth4
192.168.30.0    0.0.0.0         255.255.255.0   U       0    0        0      eth4

IPv4 routing table: 1
================================================================================
Destination     Gateway         Genmask         Flags  MSS  Window  irtt  Iface
============    ============    ==============  =====  ===  ======  ====  =====
0.0.0.0         192.168.10.1    0.0.0.0         UG      0    0        0      eth5
192.168.10.0    0.0.0.0         255.255.255.0   U       0    0        0      eth5
```

Support for multiple domains across networks for Veritas Data Deduplication

You can use a single deduplication pool to back up data from multiple NetBackup domains. The Veritas Data Deduplication server deduplicates backups originating from different subnets.

Use the **network> ip addr show** command to list the multiple subnets that have been created.

```
Network> ip addr show

IP              Netmask/Prefix  Device  Node     Type     Status
--              --------------  ------  ----     ----     ------
192.168.10.5    255.255.255.0   eth5    vaupg_01 Physical
192.168.10.13   255.255.255.0   eth5    vaupg_02 Physical
192.168.30.2    255.255.255.0   eth4    vaupg_01 Physical
192.168.30.10   255.255.255.0   eth4    vaupg_02 Physical
10.209.192.206 255.255.252.0   eth1    vaupg_01 Physical
10.209.192.208 255.255.252.0   eth1    vaupg_02 Physical
10.209.194.38   255.255.252.0   eth1    vaupg_01 Virtual  ONLINE (Con IP)
192.168.10.22   255.255.255.0   eth5    vaupg_01 Virtual  ONLINE
192.168.10.25   255.255.255.0   eth5    vaupg_02 Virtual  ONLINE
192.168.30.15   255.255.255.0   eth4    vaupg_02 Virtual  ONLINE
192.168.30.20   255.255.255.0   eth4    vaupg_01 Virtual  ONLINE
```

You can use the following command to configure the deduplication server with a virtual IP.

```
Dedupe> config fs_dedupe <IPaddress> root
```

For example:

```
Dedupe> config fs1 192.168.10.22 root
Enter Password:
ACCESS dedupe INFO V-493-10-0 configuring deduplication server...
ACCESS dedupe INFO V-493-10-0 Deduplication server configured successfully
```

You can verify that the IP has been added successfully using the dedupe> show command.

```
Dedupe> show
Parameter                    Value
=======================      ======
Percentage_Memory_Usage      4.58%
Hostname                     vaupg_01
Max_Cache_Size               50%
Server_Status                ONLINE
Virtual_IP                   192.168.10.22
Filesystem                   fs1
Deduplication_Storage_Size_GB 50
```

You can add another IP from a different subnet.

```
Dedupe> addip <IPaddress>
```

For example:

```
Dedupe> addip 192.168.10.25
ACCESS dedupe INFO V-493-10-0 IP has been successfully added to the deduplication
server.

Dedupe> addip 192.168.30.15
ACCESS dedupe INFO V-493-10-0 IP has been successfully added to the deduplication
server.
```

```
Dedupe> addip 192.168.30.20
ACCESS dedupe INFO V-493-10-0 IP has been successfully added to the deduplication
server.
```

You can verify that the virtual IP is added successfully. The **dedupe> show** command is used to display information about the deduplication server that has been configured. The output of this command includes the file system(s) being used, deduplication server status, storage capacity, secondary IPs used, percentage of memory usage, maximum cache size, and the IP and the cluster node on which the server is running.

```
Dedupe> show
Parameter                     Value
============                  =============
Secondary_IP                  192.168.10.25, 192.168.30.15, 192.168.30.20
Percentage_Memory_Usage       4.79%
Hostname                      vaupg_01
Max_Cache_Size                50%
Server_Status                 ONLINE
Virtual_IP                    192.168.10.22
Filesystem                    fs1
Deduplication_Storage_Size_GB 50
```

Use the **network> ip addr show** command to list the multiple subnets that have been created.

```
Network> ip addr show

IP              Netmask/Prefix  Device  Node              Type     Status
--              --------------  ------  ----              ----     ------
192.168.10.5    255.255.255.0   eth5    vaupg_01 Physical
192.168.10.13   255.255.255.0   eth5    vaupg_02 Physical
192.168.30.2    255.255.255.0   eth4    vaupg_01 Physical
192.168.30.10   255.255.255.0   eth4    vaupg_02 Physical
10.209.192.206 255.255.252.0    eth1    vaupg_01 Physical
10.209.192.208 255.255.252.0    eth1    vaupg_02 Physical
10.209.194.38   255.255.252.0   eth1    vaupg_01 Virtual  ONLINE (Con IP)
192.168.10.22   255.255.255.0   eth5    vaupg_01 Virtual  ONLINE (Dedupe IP)
192.168.10.25   255.255.255.0   eth5    vaupg_01 Virtual  ONLINE (Dedupe IP)
192.168.30.15   255.255.255.0   eth4    vaupg_01 Virtual  ONLINE (Dedupe IP)
192.168.30.20   255.255.255.0   eth4    vaupg_01 Virtual  ONLINE (Dedupe IP)
```

You can also add a second user. The second user is used to add the second NetBackup domain, if required. You should use a different user for every new NetBackup domain.

```
Dedupe> adduser root2
Enter Password:
Confirm Password:
ACCESS dedupe INFO V-493-10-0 Adding new user root2 to deduplication server...
ACCESS dedupe INFO V-493-10-0 Added new user root2 to deduplication server successfully.
```

You can perform backup and restore operations from the NetBackup domains from the two subnets.

Note: You can remove the virtual IP that you added later after the initial configuration. But you cannot remove the virtual IP specified during the initial configuration.

```
Dedupe> removeip <IPaddress>
```

For example:

```
Dedupe> removeip 192.168.30.15

ACCESS dedupe INFO V-493-10-0 IP has been successfully removed from the deduplication
server.
```

You can verify that the second virtual IP has been removed from the configuration using the **dedupe> show** command.

```
Dedupe> show
Parameter                     Value
============                  =============
Secondary_IP                  192.168.10.25, 192.168.30.20
Percentage_Memory_Usage       4.79%
Hostname                      vaupg_01
Max_Cache_Size                50%
Server_Status                 ONLINE
Virtual_IP                    192.168.10.22
Filesystem                    fs1
Deduplication_Storage_Size_GB 50
```

You can use the **dedupe> unconfig** command to free up all the virtual IPs added to the deduplication server. This command also unconfigures Veritas Data Deduplication from the cluster.

```
Dedupe> unconfig
ACCESS dedupe INFO V-493-10-0 Removing deduplication server configuration...
ACCESS dedupe INFO V-493-10-0 Deduplication server unconfigured successfully.
```

Upgrade considerations

You cannot use the same virtual IP for both the CIFS and Veritas Data Deduplication server. So, if a virtual IP is used by the Veritas Data Deduplication server, then you cannot use the same virtual IP for adding CIFS shares or setting the CIFS home directory.

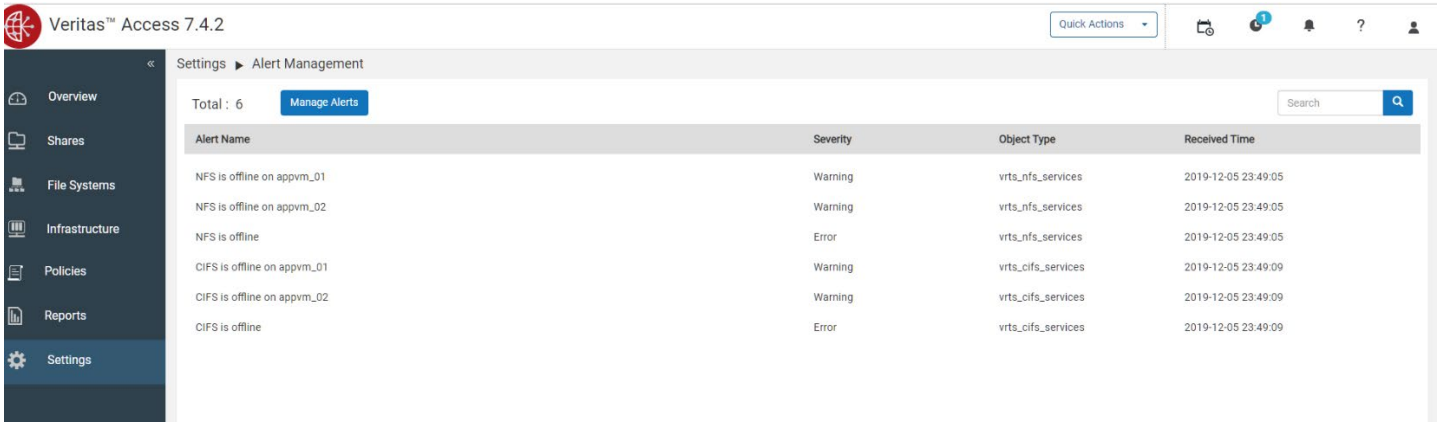
Note: If Veritas Access 7.4.2 or 7.4.2.100 is installed in your system and the same virtual IP is being shared by both the CIFS and Veritas Data Deduplication server, and you want to upgrade to Veritas Access 7.4.2.200, ensure that an additional free virtual IP is available in the configuration.

During the upgrade, the virtual IP which is shared between CIFS and Veritas Data Deduplication server is removed from the CIFS configuration and the next available free virtual IP is assigned to the CIFS server.

- If a free virtual IP is available, the deduplication continues to work without any issues once the upgrade is complete.
- If there is no free virtual IP, then the upgrade fails. You can add a free virtual IP to the configuration and try to upgrade again.
- If the virtual IP is shared between the Veritas Data Deduplication server and a segregated CIFS share, then the upgrade fails even if an additional free virtual IP is available in the configuration. You can move the segregated CIFS share to different virtual IP and try the upgrade again.

Alerts framework enhancements

Starting from this release, some of the alerts are now suppressed by default. When the user starts a service, the corresponding alerts get enabled. But if the user chooses to suppress an alert from the GUI, it does not get enabled when the user starts the service.



Alerts raised by the following services are suppressed by default if the services are not configured in the cluster:

- NFS
- CIFS
- S3
- Veritas Data Deduplication service
- NTP

Access 7.4.2.200 alert list

Alert ID	Description	Type	Default state
DEDUPE_SERVICE_DOWN	Veritas deduplication service offline	Autosupport	Suppressed
NFS_NODE_OFFLINE	NFS is offline on node	Autosupport	Suppressed
CIFS_NODE_OFFLINE	CIFS is offline on node	Autosupport	Suppressed
CIFS_SERVICE_DOWN	CIFS service is down	Autosupport	Suppressed
S3_NODE_OFFLINE	S3 is offline on node	Autosupport	Suppressed
S3_SERVICE_DOWN	S3 service is down	Autosupport	Suppressed
NFS_SERVICE_DOWN	NFS service is down	Autosupport	Suppressed
NTP_SERVICE_DOWN	NTP service is disabled	Autosupport	Suppressed
DEDUPE_MEM_USAGE	Memory usage of Veritas Data Deduplication service is more than 75% of total RAM	Autosupport	Suppressed

Veritas Access 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. A new filter, **none**, has been added in this release. If the filter is set to **none**, no notifications are triggered.

A new alert appears in the GUI when the memory usage of the Veritas Data Deduplication server is more than 75%.

The alert displays the amount of memory used and the total RAM usage. If the situation persists for more than 24 hours, an AutoSupport alert is raised and an email is sent.

If you receive this alert, go to **Settings** > **Veritas Data Deduplication** and restart the service once you reach this threshold.
For information about the issues that are caused when the Veritas Data Deduplication service consumes large amount of memory, see https://www.veritas.com/support/en_US/article.100045745.

Default storage layout

From this release, by default, the Access Appliance GUI creates a 5-way striped file system layout for storage provisioning. The previous default layout was simple (concatenated). The default layout has been changed to increase the efficiency of storage utilization.

After you perform an upgrade, the storage provisioning that is created with the previous default layout remains unchanged.

Known issues

Upgrade fails if shares are configured but NFS service is not in running state (IA-22678)

The procedure which brings the NFS shares online waits for a long time (900 sec) which causes a timeout in the upgrade process. But since the NFS server has been stopped, the NFS shares do not come online.

Workaround:
If you have exported NFS share, ensure that the NFS server is started before you perform an upgrade.

After an upgrade to Veritas Access 7.4.2.200 with VVR configured, replication continuous failover/failback commands fail (IA-22867)

When a failover is performed from CLISH, the status of the replicated volume groups associated with the file system is checked using the vradmin repstatus command. This command shows configuration errors (vradmind not reachable on cluster peer) and hence, the failover operation fails.

Workaround:
1. Verify if the file system is online using **storage fs list** command. If the status of file system is online go to step 3.
2. If the file system is not online, bring the file system online on the source cluster using the **storage fs online <fs-name>** command.

3. Restart the VVR services on both the source and target clusters using the following commands:
   ```
   replication continuous service stop
   replication continuous service start
   ```

Fixed issues in this release

This section includes the issues fixed since the last release.

Fixed Issues	Description
APPSOL-96125	Support NTP configuration during cluster setup
APPSOL-107525	Support inconsistent PIP and VIP input when setting up the cluster
APPSOL-107526	Resolve the issue where an original SFP module with some PN number triggers an unexpected alarm indicating that this SFP module is not supported
APPSOL-107948	Support eth1 configuration checking before setting up the cluster
APPSOL-108894	SDCS logs grow rapidly and are maintained for a long duration
APPSOL-109124	Unable retrieve hardware health/error when eth2 is configured to use a private IP other than the default IP when setting up the cluster
APPSOL-110109	Support unique hostname checking before setting up the cluster
IA-15478	VDD policy talks about TFS instead of CFS
IA-17105	pam.d files are zeroed out after reboot
IA-18623	Unable to stop objectaccess server if it is in OFFLINE|STARTING or OFFLINE|FAULTED state
IA-18709	Deduplication IP goes to offline state when the NIC of that virtual IP is added to the bond as slave device
IA-18812	Even after pool destroy operation, diskgroup does not get deleted.
IA-19274	S3 software test uses default bucket size, regardless of existing buckets
IA-19769	Cannot allow group access to CIFS share when name has spaces
IA-20752	Debuginfo does not collect kernel dump information from crash
IA-20931	"Add cloud Subscription" from GUI fails on Access
IA-20939	Storage rollback cache create failed and left behind the underlying volumes
IA-20942	Qlogic card driver Kernel 3.10.0-693.37.4.el7.x86_64 not yet supported
IA-20972	Unable to mount NFS filesystem stale file handle
IA-20973	RESTgroup failed to online during fresh install
IA-20978	Debuginfo run from non-root users keeps asking for password continuously
IA-20995	Loadbalance configuration is removed by reboot
IA-21008	Network module import/export fails if bond is already present on VA-7.4.1.100 in the migration scenario
IA-21010	VLAN creation fails for non-bonded NICs in case of migration scenario
IA-21071	NTP service not persistent after install or reboot
IA-21072	NTP gets disabled on reboot
IA-21568	Node is not in running state after upgrade of phase1, phase2 due to TFSMount type missing
IA-21600	InfoScale security patch for Access
IA-21723	Fix for various security vulnerabilities on 7.4.2.100 3340 appliance
IA-22127	Security vulnerability for Access 7.4 and 7.2 to cve-2013-5211
IA-22440	/sys collected twice unnecessarily in debuginfo_collector.sh script

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.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at veritas.com or follow us on Twitter at @veritastechllc.

Veritas World
Headquarters 2625
Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices
and contact numbers,
please visit our website.

The truth in information.