NetBackup™ Access Appliance 8.5 Release Notes

October 2025

VERITAS
now part of Cohesity

Access Appliance Release Notes

Last updated: 2025-10-13

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

https://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

https://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Overview of Access Appliance

This chapter includes the following topics:

About this release

This document provides release information about the Access Appliance product, including changes in this release.

Changes in this release

This section shows the major new features and enhancements added in the 8.5 version of Access Appliance.

Advance notification for deprecated functionality in future releases

The following functionality will be deprecated in a future release of Access Appliance:

- Episodic replication
- iSCSI protocol

- Cloud tiering
- Configuring Access Appliance as archival storage with Enterprise Vault
- Volume manager level encryption
- Creating shares (NFS/CIFS) with encryption

Supported NetBackup client versions

The following versions of NetBackup client are supported with Access Appliance 8.5.

- 10.0
- 10.1.1
- 10.2
- 10.3
- 10.4
- 10.5
- 10.5.0.1
- 11.0

The supported NetBackup clients can be installed as add-on packages.

Supported versions of Veritas Data Deduplication

Access Appliance supports multiple versions of Veritas Data Deduplication. You can configure Veritas Data Deduplication version of your choice, which is compatible with the NetBackup primary server version in the domain. You can upgrade from a lower version to a higher version of Veritas Data Deduplication without loss of data.

The following versions of Veritas Data Deduplication are supported in this release:

- 20.4.0.1
- 20.5.0.1
- 21.0

For more details, see *Supported configurations and versions for NetBackup with Veritas Data Deduplication* section in the *Access Appliance Administrator's Guide*.

Access Appliance simple storage service (S3) APIs

See the *Veritas Access Restful API Guide* for more information on simple storage service (S3) APIs.

Chapter 2

Software limitations

This chapter includes the following topics:

Limitations related to CIFS

The following limitations are related to CIFS:

- CIFS as a standalone server is not supported. In this release, CIFS share access is only allowed with FQDN.
  For more details, refer to the *Using Access Appliance as a CIFS server* chapter in the *Veritas Access Appliance Administrator's Guide*.

Limitations related to installation and upgrade

The following limitations are related to installation and upgrade.

Underscore character is not supported for host names

Starting with 7.4.3, underscore (_) is not allowed in a host name. You can however upgrade to 7.4.3 from an earlier version where the host name included an underscore.

Limitation related to cloud tiering

The following limitation is related to cloud tiering.

- Cloud tiering does not work if disaster recovery is configured on Access Appliance.

Limitations related to networking

The following limitations are related to networking:

- A single Access Appliance cluster supports up to 16 VLANs.

Limitations related to Veritas Data Deduplication

The following limitation is related to Veritas Data Deduplication.

- If you want to reconfigure Veritas Deduplication using previously used file systems, you have to use the same credentials that you used during the initial configuration.

  Note: For a containerized version of Veritas Data Deduplication, a password is not required to be provided during reconfiguration.

Kernel-based NFS v4 limitations

The following limitations apply for kernel-based NFS v4:

- NFS v4 ACLs are not supported by Access Appliance.
- NFS v4 share reservations are not supported.

- NFS v4 delegation is not supported.

File system limitation

The following limitations relate to the Access Appliance file system.

- Any direct NLM operations from the Access Appliance command-line interface can lead to system instability
  Do not perform any file system related operations using the Access Appliance command-line interface on the Network Lock Manager (NLM), as it is used for internal purposes. If NLM is used, then Access Appliance cannot guarantee the stability of the cluster.
- On-premises tiering in a cluster file system only supports one primary and one secondary.

Access Appliance S3 server limitation

- For downloading an object with a size more than 100 M, `Range` header should be used and the range should not exceed 100 M.
  The object has to be downloaded in parts.
- If S3 service is enabled with SSL option on Access Appliance with either internal or external certificate, then configuration of MSDP-C is not supported with the `Check certificate revocation` option during disk pool creation.

Long-term data retention (LTR) limitations

The following limitations are related to LTR:

- Access Appliance does not support the HTTPS application protocol for an S3 bucket from the GUI in Veritas NetBackup long-term retention (LTR) use cases.

Limitation related to replication

The following issues relate to replication in Access Appliance.

Limitation related to continuous replication

- Continuous replication does not support changing the mode of replication (synchronous or asynchronous) after replication is configured.

- The Access Appliance file system operations such as grow, shrink, resize, addition or removal of column, mirror, or tier (except cloud tier) are not supported for a file system which is configured under continuous replication.

Limitations related to user management

The following limitations are related to user management:

- Assigning the appliance administrator role to an AD user from trusted domain is not supported.

Chapter 3

Known issues

This chapter includes the following topics:

Access Appliance known issues

The following known issues relate to the Access Appliance commands.

CIFS issues

This section describes known issues related to CIFS.

CIFS share created on Access Appliance 8.x version may not be accessible if all the virtual IPs are on a VLAN device

If you create a CIFS share on Access Appliance 8.x where all the virtual IPs are on a VLAN device, the CIFS share created may not be accessible. This occurs because a dedicated IP has not been specified to be used for the share. For example:

```
cifs> share add <share path> sharename <share_options>
```

If a virtual IP is provided in the share name (segregated CIFS share) , then the created CIFS share is accessible.

(IA-45708)

Workaround:

If you want to create a CIFS share on Access Appliance 8.x, where all the virtual IPs are on a VLAN device, you can use any of following two methods:

```
cifs> share add <share path> sharename[@virtual_ip] <share_options>
```

For example:

```
cifs> share add fs_cifs share1@192.168.10.142  rw,full_acl
```

OR

```
cifs> share add <share path> sharename share_options,ip=<virtual_ip>
```

For example:

```
cifs> share add fs_cifs share1 rw,full_acl,ip=192.168.10.142
```

CIFS share add command fails to add share on the target cluster for a filesystem which is used in the configuration of episodic replication

If episodic replication is configured on the source target cluster and you perform a sync operation after generating data on CIFS share, and then create a CIFS share on the target cluster on the same filesystem using the `cifs share add` command, the operation fails on the target cluster.

This is expected behavior. If required, the contents of the share can be verified after disabling episodic replication.

Workaround:

This is by design and there is no workaround for this issue.

General issues

The following issue relates to all the Access Appliance modules.

Reimaging the appliance from the SSD device fails if a CD with the ISO image is inserted in the CD-ROM

Reimaging from the SSD device fails with the following message if a CD with the ISO image is also inserted in the CD-ROM of the appliance:

Pane is dead. Couldn't open file /tmp/ks_top_customization.cfg.

If you select SSD as the boot device and the CD is also inserted, the installer detects two ISO images with the same label, which results in a conflict.

(APPSOL-157945)

Workaround:

Ensure that the CD with the ISO image is not inserted in the CD-ROM when you select the SSD as boot device from the boot menu options. If the **Pane is dead** error message is displayed, remove the CD from the CD-ROM and try to reimage the appliance from SSD again.

User is not logged out from the command-line interface after running the Cluster> stop all command

If you elevate to root access and run the `Cluster> stop all` command from the Access command-line interface, the console remains accessible though the Access services are down.

(IA-42379)

Workaround:

There is no workaround for this issue.

User account gets locked on a management or non-management console node

If the user account is locked on a management console node because of multiple incorrect login attempts, both SSH and GUI sign-in fail on that node till the account lock period is complete.

If the user account is locked on a non-management console node because of multiple incorrect login attempts, SSH to that specific node is blocked. SSH to all the other nodes and sign-in to the GUI continues to work.

(IA-52652, IA-52654)

Workaround:

Account lock depends on the password policies. Wait for the lock period to get completed.

Addition of a user named 'admin' fails from GUI and CLISH

If the default user, *admin* is logged into the node of the cluster and there is an attempt to create another user named *admin*, the user creation operation fails.

(IA-52639)

Workaround:

Make sure that the default user, *admin* is logged out from all nodes of the cluster before attempting to create a user named *admin* in the cluster.

The displayed proxy server state is inconsistent if the specified proxy server settings are incorrect

The `show alerts callhome` and `show proxy-server` commands display different state for the proxy server. The `show alerts callhome` command validates the settings before setting the proxy server status. If the proxy server configuration details are incorrect, the proxy server status is not updated and shown as Disabled.

The `show proxy-server` command does not verify the settings and displays the proxy server status as Enabled. (AA-610)

Workaround:

1. Enable Call Home.
2. Run the `show alerts callhome-test` command to verify Call Home is set correctly.
3. Specify the correct proxy server configuration details.
4. Verify the proxy server status by running both the `show alerts callhome` and `show proxy-server` commands. Both the commands show the same Enabled status.

GUI issues

The following issues relate to the GUI.

When provisioning storage, the Access web interface or the command-line interface displays storage capacity in MB, GB, TB, or PB

When you provision storage using the Access web interface or the command-line interface, the storage pool size and the size configured for Veritas Data Deduplication are displayed in MB, GB, TB, or PB. However, the storage capacity is actually in MiB, GiB, TiB, or PiB.

(IA-15180)

GUI stops working after ECA deployment

After uploading the ECA certificate, CA Bundle and private key, the GUI stops working. This may happen if incorrect certificates or private key are uploaded. As a result, the ECA configuration fails.

(IA-53643)

Workaround:

Switch to the internal appliance self-signed certificates using the `system certificate mode set internal` command. The GUI comes up. Check the certificates and reconfigure ECA.

Partially uploaded software upgrade package is displayed in the GUI

When you upload an upgrade package by navigating to the **Settings > Software management > Software update** tab and the upload task fails, the partially uploaded package is displayed in the **Downloaded package files** section of the GUI. You can also view the partially uploaded package by running the `system software downloaded` command or in the `/inst/patch/appliance/available` directory.

(IA-55685)

Workaround:

Delete the partially uploaded patch manually from the GUI by selecting the upgrade package and clicking **Remove** from the Actions menu (vertical ellipsis).

Infrastructure issues

The following sections describes the infrastructure-related issues.

The Access Appliance management console is not available after a node is deleted and the remaining node is restarted

If a node is deleted and the only remaining node in the cluster is restarted, the management console's IP gets cleared up. Hence, the service group of the management console goes into a faulted state and then management console becomes unavailable.

Workaround:

Perform the following steps:

- Log on using the Appliance command-line interface as an *admin* user.
- Go to **Support** view.
- Go to **Management** view.
- Elevate to access the prompt. Run the following commands:

```
# /opt/VRTS/bin/hares -clear consoleIP -sys <current node>

# /opt/VRTs/bin/hagrp -online ManagementConsole -any
```

Add node fails if upgrade is performed from 7.4.2.200 or lower version

Add node fails if the cluster is upgraded from 7.4.2.200 or a lower version to 8.5 and the node that is added is directly configured with 8.5. The add node operation fails because of UID-GID mismatch of primary, sysadmin, storage admin (stoadmin), and system storage admin (sysstoadmin) users.

Workaround:

The node that is being added must follow the same upgrade path as that of the cluster.

Installation and configuration issues

The following issues relate to Access Appliance installation and configuration.

When you configure Access Appliance as an iSCSI target, the initiator authentication does not work

This happens because the default algorithm (MD5) used for authentication is disabled in RHEL7. (CXC-7150)

Workaround:

Use a node session algorithm other than MD5 such as SHA1, SHA256 on the iscsi initiator.

If the console node reboots, the install operation fails for inconsistent EEBs

While installing EEBs, if the management console node reboots, the EEBs are in an inconsistent state. If you install all the EEBs to make the EEBs consistent across the cluster, the EEB installation operation fails again.

(APPSOL-177924)

Workaround:

Contact Veritas Technical Support to resolve this issue.

MSDP-C issues

This section describes MSDP-C issues.

MSDP-C duplication job fails with OpenStorage WORM lock error after the file system is grown to100%

MSDP-C duplication job fails if you retry a duplication job after performing `fs grow` operation on the file system from the Access GUI/CLISH after the file system is already 100% full. (IA-39570)

Workaround:

If the bucket file system is already 100% full, grow the file system from Access GUI/CLISH. Restart the NetBackup's pdde services using the following commands from the NetBackup bash before starting backup again.

```
/usr/openv/pdde/pdconfigure/pdde stop
/usr/openv/pdde/pdconfigure/pdde start
```

Networking issues

This section describes known issues related to networking.

The `network ip addr show` command does not display all the FQDN entries for an IP address

The `network ip addr show` command displays a maximum of two FQDN entries though an IP address might be assigned more entries.

(IA-43181)

Workaround:

Use the `network host show command` or the `/etc/hosts` file to view all the FQDN entries that are associated with the IP address.

Unable to log in to IPMI intermittently

IPMI login fails intermittently with an empty caution message.

(APPSOL-178242)

Workaround:

Contact Veritas Technical Support and ask them to refer to 100062710 article.

NFS issues

This section describes NFS issues.

Kernel-NFS v4 lock failover does not happen correctly in case of a node crash

With kernel NFS v4 shares, in case of a node crash, active locks do not failover to another node in the cluster.

(IA-5083)

Workaround:

There is no workaround for this issue.

Kernel-NFS v4 export mount for Netgroup does not work correctly

The Netgroup membership cannot be changed dynamically with kernel NFS v4. The kernel KNFS v4 export mount for Netgroup does not work as expected.

(IA-6672)

Workaround:

Restart the NFS service.

System software share open command displays IPV6 IP on NFS share if the management NIC (eth1) is configured with VLAN

If the management NIC is configured on VLAN, the system software share open command displays the IPv6 IP in IPv4 cluster environment. There is no functional impact due to this NFS share message.

(IA-56590)

Workaround:

Mount the NFS share with the FQDN or IP of the management NIC of that particular node.

ObjectAccess issues

This section describes ObjectAccess issues.

The Object Access server crashes whenever any operation on the Object Access server requires authentication with the AD server using an AD user

Any operation on the Object Access server which requires authentication with the AD server using AD user causes the Object Access server to crash if the AD user's password has expired.

(IA-49775)

Workaround:

The AD server admin can extend the password expiry or change the AD user's password.

Replication issues

This section describes known issues related to replication.

Continuous replication is unable to go to the replicating state if the Storage Replicated Log becomes full

While replicating data from the source cluster to the target cluster, if the Storage Replicated Log (SRL) becomes full, It goes into Data Change Map (DCM) mode. In DCM mode, it does not show the status as `replicating`.

```
Replication> continuous status test_fs
Name                    value
====================  ============================================
Replicated Data Set    rvg_test_fs
Replication Role       Primary
Replication link       link1

Primary Site Info:

Host name           10.10.2.70
RVG state           enabled for I/O

Secondary Site Info:

Host name           10.10.2.72
Configured mode     synchronous-override
Data status         inconsistent
Replication status  resync in progress (dcm resynchronization)
Current mode        asynchronous
Logging to          DCM (contains 551200 Kbytes) (SRL protection logging)
```

Workaround:

Run the following command on the source cluster for continuous data replication.

```
# vxrvg -g <dg_name> resync <rvg_name>
```

The command resynchronizes the source and the target cluster. You can check the status by entering the following command:

```
Replication> continuous status test_fs
Name                    value
=====================  ======================
Replicated Data Set     rvg_test_fs
Replication Role        Primary
Replication link        link1

Primary Site Info:

Host name               10.10.2.70
RVG state               enabled for I/O

Secondary Site Info:

Host name               10.10.2.72
Configured mode         synchronous-override
Data status             consistent, up-to-date
Replication status      replicating (connected)
Current mode            synchronous
Logging to              SRL
Timestamp Information   behind by  0h 0m 0s
```

Unplanned failover and failback in continuous replication may fail if the communication of the IPTABLE rules between the cluster nodes does not happen correctly

In case of unplanned failover and failback, the IPTABLE rules may not get restored properly. The communication between the nodes does not happen correctly.

Workaround:

Flush the IPTABLES on all the nodes in the cluster on the primary as well as the secondary site.

```
# iptables -F
```

STIG issues

This section describes known issues related to STIG.

The changed password is not synchronized across the cluster

When the STIG option is enabled or password policies are set, the user password expires as per the set password policy. After the password expires, the user is prompted to change the password if the user logs on to the system via SSH. If the user changes the password at the prompt, the password is changed only locally and is not synchronized across the cluster.

(IA-29565)

Workaround:

After the password expires, when prompted, do not change the password at the OS prompt. Instead, log on to the GUI with your credentials and change the password from the GUI.

Storage issues

The following issues relate to the Access Appliance Storage commands.

Rollback service group goes in faulted state when respective cache object is full and there is no way to clear the state

This issue relates to I/O errors after cache objects get full. In cases of cache-backed rollbacks, having cache full due to heavy I/O creates I/O errors in snapshots, and snapshots are automatically detached from the main file system. Snapshots go in to a faulted state. The fix for this requires clearing the faulty rollback state and doing rollback refreshes. You cannot handle this case from the Access Appliance command-line interface. Manual intervention by Veritas Technical Support is required to preserve the rollback.

(IA-3251)

Workaround:

There is no workaround.

Event messages are not generated when cache objects get full

This issue is related to customer visible events for rollback cache full scenarios.

(IA-3239)

Workaround:

There is no workaround.

Storage fs addcolumn operation fails but error notification is not sent

`Storage fs addcolumn` operation fails in the background but the notification of the failure is not sent as the error message is not present in the Access Appliance command-line interface. One of the reasons for the failure is not having enough storage in the given pool.

(IA-5434)

Workaround:

If required number of columns are not added, try again after adding enough storage.

Unable to create space-optimized rollback when tiering is present

In a tiered file system, creation of space-optimized rollbacks fails. The failure occurs when the primary tier has `fastresync` enabled while the secondary tier does not have `fastresync` enabled.

The secondary tier has `fastresync` disabled in the following scenarios:

1. The tier is mirrored but `fastresync` is manually disabled.

2. The tier is simple or striped in which case `fastresync` cannot be enabled.

(IA-5690)

Workaround:

If the secondary tier is mirrored, enable `fastresync` on it.

If the secondary tier is simple (or striped) and primary tier is mirrored, add a mirror to the secondary tier.

Ensure that the secondary tier has `fastresync` enabled if the primary tier also has `fastresync` enabled.

The CVM service group goes in to faulted state after you restart the management console node

When the `Cluster> reboot` command is run, sometimes the CVM service group goes into faulted state on the node that was restarted. This issue is usually caused by a minor number conflict between the CVM shared disk group objects, such as

volumes, volume sets or Replicated Volume Groups (RVGs) and the private disk group objects. Confirm that the minor numbers of the private disk group objects do not overlap with the CVM disk group objects on the joining CVM slave node.

https://www.veritas.com/support/en_US/article.000107801

Workaround:

To bring the CVM service group online

1. Run the following command on the node where CVM service group is in faulted state

   ```
   # hastop -local
   ```

2. Offline all the file systems. Run the following command from another node where the management console is online.

   ```
   Storage> fs offline <file system name>
   ```

3. Deport all the disk groups using the following command:

   ```
   # vxdg -s deport <disk_group>
   ```

4. Import all the disk groups using the following command:

   ```
   # vxdg -s import <disk_group>
   ```

5. Start Veritas Cluster Server (VCS).

   ```
   # hastart
   ```

   If the file system does not come online, then run the following command to make all the file systems online:

   ```
   Storage> fs online <file system name>
   ```

After a cluster reboot, the UI shows that the storage is not configured

After rebooting both the cluster nodes, the UI may not show the correct storage details. After the cluster services are up if you navigate to the Dashboard, it shows that the storage is not configured for the cluster.

(IA-55750)

Workaround:

Log on to the UI and run full discovery by navigating to **Settings > Services Management > Storage Services Management > Run full discovery**. Once the discovery completes, the storage details are displayed correctly.

Upgrade issues

This section describes known issues related to upgrade.

The system config import command does not work as expected

The following submodules for import do not work as expected - `all`, `target`, `backup`, `object_access`, `replication storage_quota`, `storage`, `fs_policy`, `cluster_specific`. This occurs because of an issue with the configuration files. So, the `system config import` command does not function as expected.

(IA-43304), (IA-42197)

Workaround:

There is no workaround for this issue.

After multi-step upgrade from 7.4.2 to 8.5 eth1 device is not listed in the network ip add show output

After a mult-step upgrade to 8.5, unable to add the eth1 device to the cluster. (IA-53773)

Workaround:

To add eth1 dev of each node, in Access cluster do the following on both the nodes:

1. Elevate to root shell.
2. Delete following directives from the `/etc/sysconfig/network-scripts/ifcfg-eth1` file on all the nodes of the cluster:
   - IPADDR
   - NETMASK
   - NETWORK
   - GATEWAY

3 Reset the device using the following command:

```
ifdown eth1 && ifup eth1
```

4 Verify if the default route for eth1 has been deleted by using the following command:

```
ip route show
```

5 If the default route for eth1 still persists, run the following command to remove the default route:

```
route del default gw gateway ip dev eth1
```

6 After deleting the default route, delete the entry from the `/opt/VRTSnas/conf/net_globalroutes.conf` file.

7 From the elevated prompt of the node where the management console is running, execute the Access CLISH command as follows:

```
LOGNAME=primary /opt/VRTSnas/clish/bin/clish -u primary
```

8 Bring eth1 under Access management:

```
Network> device add eth1
```

9 Monitor the state of the Phantomgroup_pubethx service group using following command. Ensure that the service group is brought online:

```
hagrp -state | grep Phantomgroup_pubeth
```

10 Add a free IP address from cluster for eth1 using the following command:

```
amigrtionclus> network ip addr add IP NETMASK physical eth1
nodename
```

11 Verify that the IP address is added correctly by checking the output of the following command:

```
amigrtionclus> network ip addr show
```

12 Log out from the Access CLI.

13 Update the `/opt/VRTSnas/conf/net_preexist_dev.conf` file on both the nodes with the entry for eth1

14 Add default global route:

```
amigrationclus> network ip route add all 0.0.0.0 0.0.0.0 via
new_gw dev eth1 scope=global
```

Note: The **scope** parameter is available from 7.4.3 and later versions. If you on version 7.4.2.x, the **scope** parameter is not available and you must use the Linux command instead to add the route.

15 Change the console IP:

```
amigrationclus> network ip addr modify old_ip new_ip new_pub_nm
device
```

Note: The current logged in Access CLISH session is terminated.

Checkpoints might remain in the file systems used by Veritas Data Deduplication (VDD) after the system rolls back after an upgrade failure

VDD checkpoints are not deleted after the rollback leading to stale checkpoints in the system.

(IA-54261)

Workaround:

Contact Veritas Technical Support and ask them to refer to article 100063139.

Upgrade preflight check fails with password expiry error

When an upgrade is performed from Access Appliance 8.3 or lower version to 8.5 version, the preflight check may fail with password expiry error for some users due to incorrect password expiry date in the cluster.

(IA-57313)

Workaround:

Change the password of these users using CLISH/GUI.

Upgrade from Access Appliance version 8.2/8.2.x, 8.3/8.3.x to version 8.5 fails during free space pre-check for "/" partition

Upgrade from Access Appliance version 8.2, 8.2.x, 8.3, 8.3.x to version 8.5 may fail during preflight check for insufficient free space on "/" partition. This issue can be observed in some cases where "/" partition is occupied and not meeting the free space requirement for upgrade to work.

The following error message is seen:

```
[Error] V-409-776-1120: The space / is not enough.
[ERROR] V-409-776-30003: Pre-flight check failed.
```

(IA-58046)

Workaround:

Contact Veritas Technical Support to resolve the issue.

AD is disabled after an upgrade from Access Appliance version 8.3.100 to 8.5

After you perform an upgrade from Access Appliance 8.3.100 version to 8.5 version, AD is in disabled state.

(IA-57992)

Workaround:

Unset the AD server on Access Appliance and set it again using the following steps:

1. Stop the CIFs server.

   ```
   cifs server stop
   ```

2. Unset the AD server.

   ```
   network ad unset
   ```

3. Set the AD server.

   ```
   network ad set <domain> <domaincontroller> <workgroup>
   <domainuser> <idmapupperbound>
   ```

4. Enable the AD server.

   ```
   network ad enable
   ```

5. Start the CIFs server.

```
cifs server start
```

After you upgrade from Access Appliance version 8.2/8.2.002 to version 8.5, the CTDB server and ADClientService goes into PARTIAL state or is not ONLINE on all the nodes

During upgrade, the VCS service groups are brought offline and after upgrading packages they are brought online again. ADClientService and CTDB server groups have a child-parent dependency. During preonline trigger of ADClientService, the CTDB service is started since it is required for startup of winbind service (ADClientService). Since CTDB service is started, the CTDB server resource which is part of CTDB server group might come ONLINE and the CTDB server group might change to PARTIAL. If VCS tries to bring the CTDB server online at a point when the CTDB server's state has already changed to PARTIAL, the CTDB server remains in PARTIAL state.

(IA-58120)

Workaround:

Restart the CIFS server from CLISH.

```
cifs server stop
cifs server start
```

Veritas Data Deduplication issues

This section describes known issues related to Veritas Data Deduplication.

Provisioning for Veritas Data Deduplication is displayed as failed in GUI

If there are any subtasks which are in running state, the provision for Veritas Data Deduplication fails.

(IA-23055)

Workaround:

Check the task details to make sure that no subtask is in running state and check the reason for the failure. Wait for all the subtasks to get completed before retrying the operation.

After upgrade, Veritas Data Deduplication configuration fails as the virtual IP association with deduplication is being used by CIFS

In case of CTDB CIFS share where the IPs are not explicitly mentioned, any free virtual IP is assigned during configuration. As part of upgrade, Veritas Data Deduplication is unconfigured and the virtual IP used for deduplication is released to the network pool. When the CIFS server comes online, it may use the released IP and the virtual IP is stamped in the `vip_service_map.yml` file against a CIFS entry. When Veritas Data Deduplication is reconfigured after upgrade, the virtual IP previously associated with deduplication is already part of yml. This leads to an error and a message is displayed that the virtual IP is already being used for CIFS.

Workaround:

After the upgrade is complete, if you find that the virtual IP previously associated with Veritas Data Deduplication is getting used by the CIFS server, run the following commands:

- `network> ip addr del <dedupe_ip>`
- `network> ip addr add <dedupe_ip> netmask virtual`

This forces the CIFS server to pick up another free virtual IP from the network pool, and then deduplication can be configured with its original virtual IP.

Access Appliance operational notes

This section contains the topics that explain important aspects of Veritas Access Appliance 8.5 operations that may not be documented elsewhere in the documentation.

The following list contains the notes and the known issues that apply to this Access Appliance release:

Access services do not restart properly after storage shelf restart

If the Veritas Access 3340 Appliance loses connectivity to an attached Primary or Expansion storage shelf, the underlying storage connectivity is lost and the VxVM disk group goes into a deported state. This issue occurs whenever a storage shelf intentionally or unintentionally restarts. To correct this issue, you need to restart the Access services.

To restart the Access services after the appliance storage shelves restart

1. Log onto the Access shell menu over the console IP address.
2. Run the following command to import the VxVM disk group and other Access configurations:

   ```
   ltrcluster> storage scanbus
   ```

3. Restart the services that were configured before the storage shelf restart.

   For example, if the S3 server is configured, use the following commands

   ```
   ltrcluster> objectaccess server status
   ObjectAccess Status on ltrcluster_01 : OFFLINE|FAULTED
   ObjectAccess Status on ltrcluster_02 : OFFLINE|FAULTED
   ltrcluster> objectaccess server stop
   ACCESS ObjectAccess ERROR V-493-10-4 ObjectAccess server already stopped.
   ltrcluster> objectaccess server start
   ACCESS ObjectAccess SUCCESS V-493-10-4 ObjectAccess started successfully.
   ltrcluster> objectaccess server status
   ObjectAccess Status on ltrcluster_01 : ONLINE
   ObjectAccess Status on ltrcluster_02 : ONLINE
   ltrcluster>
   ```

Chapter 4

Getting help

This chapter includes the following topics:

Displaying the Online Help

You can access the Online Help through the management console of Access Appliance by clicking the question mark icon.

Displaying the man pages

You can enter Access Appliance commands on the system console or from any host that can access Access Appliance through a session using Secure Socket Shell (SSH).

Access Appliance provides the following features to help you when you enter commands on the command line:

- Command-line help by typing a command and then a question mark (?)
- Command-line man pages by typing `man` and the name of the command
- To exit a man page, type `q` (for quit).

Using the Access Appliance product documentation

The latest version of the Access Appliance product documentation is available on the Veritas Services and Operations Readiness Tools (SORT) website.

https://sort.veritas.com/documents

You need to specify the product and the platform and apply other filters for finding the appropriate document.

Make sure that you are using the current version of documentation. The document version appears on page 2 of each guide. The publication date appears on the title page of each document. The documents are updated periodically for errors or corrections.

The following documents are available for Access Appliance on the SORT site:

- *Access Appliance Administrator's Guide*
- *Access Appliance Cloud Storage Tiering Solutions Guide*
- *Veritas Access Command Reference Guide*
- *Access Appliance Release Notes*
- *Veritas Access RESTful API Guide*
- *Access Appliance Solutions Guide for Enterprise Vault*
- *Access Appliance Solutions Guide for NetBackup*
- *Access Appliance Troubleshooting Guide*
- *Access Appliance Command Reference Guide*
- *Access Appliance Hardware Installation Guide*
- *Access Appliance Initial Configuration Guide*
- *Access Appliance Product Description*
- *Access Appliance Safety and Maintenance Guide*
- *Access Appliance Third-party Legal Notices Guide*
- *Access Appliance Upgrade Guide*