NetBackup Appliance 3.3.0.1 MR2 Release Notes

VERITAS
The truth in information.

14-Apr-2021

Overview

NetBackup Appliance 3.3.0.1 Maintenance Release 2 (henceforth also referred as MR2) provides critical product and security fixes. **It is strongly recommended that all existing 3.3.0.1 customers or those planning to upgrade to 3.3.0.1 install MR2. MR2 includes 3.3.0.1 GA content** and NetBackup Appliance 3.3.0.1 Maintenance Release 1 (MR1) content. (3.3.0.1 GA was released on October 5, 2020; MR1 was released on December 3, 2020).

MR2 is meant to be installed only on the following NetBackup Appliance releases:

NetBackup Appliance 3.3.0.1 (any 3.3.0.1 revision level)

NetBackup Appliance 3.2 (any 3.2 revision level)

> **By installing MR2 on 3.2, the appliance is upgraded directly to 3.3.0.1 MR2 in a single upgrade step, without having to upgrade first to 3.3.0.1 GA.**

Customers can download MR2 **(SYMC_NBAPP_update_MaintenanceRelease-3.3.0.1-20210401003530.x86_64.rpm)** from the following Veritas Download Center link:

https://www.veritas.com/content/support/en_US/downloads/update.UPD498269

Always refer to the Read me section in the above link for important new updates after the Release Notes have been published.

Upgrading from 3.3.0.1 MR2 to 4.0 GA is not supported.

Upgrading from 3.3.0.1 MR2 to the first 4.0 Maintenance Release (4.0.0.1 Maintenance Release 1) will be supported.

Appliance Management Server (AMS) Support

AMS 1.4.1 supports upgrading from 3.3.0.1 to MR2.

There is no AMS support for upgrading from 3.2 to MR2. This support will be provided in a future release of AMS.

Pre-Installation steps

For installation on master server:

- Confirm that no backup jobs are scheduled during the upgrade period
- Deactivate all policies to ensure no backups will target the appliance that is being upgraded
- Cancel all active jobs from the NetBackup Java Administration Console or log in to the appliance as a NetBackupCLI user and run the following command: bpdbjobs -cancel

For installation on media server:

- Deactivate all policies to ensure no backups will target the appliance that is being upgraded
- Cancel all active jobs running
- Disable all Storage Life Cycle Policies that duplicate to/from the appliance on which MR2 is being installed

Installation Instructions

If installing on 3.2, make sure to review and follow the 3.3.0.1 pre-upgrade checklist (*NetBackupAppliance_Pre_Upgrade_Checklist_3301.pdf*), which can be found here. Do not run the AURA mentioned in this checklist. Instead, run the following AURA, which is available here:

SYMC_NBAPP_update_MaintenanceReleaseReadinessAnalyzer-3.3.0.1-20210401003530.noarch.rpm

Note that AURA needs to be run only if installing MR2 on 3.2.

Before installing MR2, note the following:

- Refer to the following article for installation instructions

  https://www.veritas.com/support/en_US/article.100023444

- A reboot occurs automatically around halfway through the installation

- Installation requires IPMI connectivity to the appliance.
- If the installation is successful, an email notification is sent (if emails notifications are configured) and the following broadcast message is broadcasted:

NetBackup Appliance has upgraded successfully!

The new release version can be checked using either of the following commands.

Expected output of each command is also listed

Manage > Software > UpgradeStatus

The appliance version is 3.3.0.1 Maintenance Release 2 and not in upgrade state.

Manage > Software > List Version

Appliance Version: 3.3.0.1

NetBackup Version: 8.3.0.1

Build Date: 3.3.0.1-20210325032937

Maintenance Release Version: 2

Appliance > Status

Appliance Model is NetBackup Appliance 5xxx.

Appliance Version is 3.3.0.1 Maintenance Release 2.

Note: During installation, the appliance reboot status can be monitored from the Remote Management Module (RMM) console. However, if the status is frozen or appliance appears to be rebooting for more than 30 minutes, appliance can be manually rebooted using the Support > Reboot command through an SSH session. Resetting the Remote Management Module (RMM) console will also force a reboot.

The MR2 Installer automatically uninstalls any Firmware update tool EEB, if found. This action does not roll back any previous firmware upgrades.

Additional instructions for installing in a NetBackup Appliance 5330/5340 High Availability (HA) setup

Before installing MR2 on both nodes, ensure that the two-node HA setup is fully configured. The HA status can be checked by using the following command:

Manage > HighAvailability > Status

If the HA services status not as follows, contact Veritas Support for assistance.

Ss	Status on Primary node	Status on Partner node
AdvancedDisk	Online	Online
Fingerprint calculation	Online	Online
MSDP	Online	Offline
Virtual IP	Virtual IP	Offline

For information on configuring a two-node HA setup, see the *Veritas NetBackup Appliance High Availability Reference Guide.*

Ensure that MR2 is installed on a node only if it is offline. Refer to following article for more information about how a node can be put in offline status:

https://www.veritas.com/content/support/en_US/doc/75895731-130448786-0/v124983164-130448786

1. Install MR2 on the partner node where the virtual IP is offline.

   It is normal for the appliance to reboot automatically around midway through MR2 installation.

2. Perform a switchover operation using the *Manage > HighAvailability > Switchover* command to bring the Virtual IP online on the node installed with MR2.

3. After the switchover, install MR2 on the other node, where the virtual IP is now offline.

4. Test the switchover to the original node to ensure correct functionality.

Post-Installation Instructions

If installing on 3.2, make sure to review and follow the 3.3.0.1 post-upgrade checklist (*NetBackupAppliance_Post_Upgrade_Checklist_3301.pdf*), which can be found here.

After installing MR2, install the MSDP EEB Bundle.

If any EEB was uninstalled on 3.3.0.1 GA/3.3.0.1 MR1, before installing MR2, reinstall it.

Enhancements in MR2

All enhancements in 3.3.0.1 GA, and the following post 3.3.0.1 GA enhancements:

- Support patching of Appliances with less than 450 MB boot space
- Automatic rollback support for installation failures
- Correctly handling fixes, included in this Maintenance Release, that are already installed on Appliance
- All installed Firmware update tool EEBs will be removed. This will not rollback the firmware changes.
- VxFS and MSDP file locking performance enhancement that can result in a significant reduction in backup and replication times. This requires version 7 or above of the MSDP EEB Bundle.

Enhancements in 3.3.0.1 GA can be found here

Product Fixes included in MR2

All fixes in 3.3.0.1 GA. The following included fixes (included post 3.3.0.1 GA) are not available on Veritas Download Center:

- ET4016348 – Appliances report false alert on MSDP for the 'Not Available' Status shown in CLISH
- **Updated VRTSVxFS fixes**
  - ET4004883 - FS corruption after multiple reboots due to fsck failure
  - ET4016881 - Abrupt power cycle can cause FS inconsistency
- **Updated VRTSVxVM fixes**
  - ET3986211 - CFS mountsq in hang state

  - ET4016898 - Crash found on secondary node
  - ET4016897 - RVG recovery may hang due to incorrect sibling/generation values
  - ET4016892 – Delay in starting vxesd process in case of large number of LUNs
  - ET4016906 - VxVM installation failure due to improper creation of links in VEKI installation
- ET4015366 - Latest Seagate fwdownloader RPM to stop sg_map
- ET4007567 - SASCable connections fail when too many getstatus calls are made.
- ET4018872 - Collector reporting failed SSD Component during CLISH Hardware ShowHealth.
- ET4015302 – Add support for 10GB card on 5250 (for 3.3.0.1 version)
- ET4019790 – Add support for 10GBase-T in 5250 Appliance with Intel NIC X540 Config "G"
- **All fixes in the following technote:** https://www.veritas.com/support/en_US/article.100034008

ETrack numbers (ETXXXXXXX) are for Veritas Support reference only.

Vulnerabilities Fixed in MR2

Vulnerabilities fixed in 3.3.0.1 GA and the following vulnerabilities fixed post 3.3.0.1 GA:

CVE-2020-10713, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15705, CVE-2020-15706, CVE-2020-15707, CVE-2020-10757, CVE-2020-12653, CVE-2020-12654, CVE-2020-8616, CVE-2020-8617, CVE-2017-18595, CVE-2019-19768, CVE-2020-10711, CVE-2019-11487, CVE-2019-17666, CVE-2019-19338, CVE-2019-14816, CVE-2019-14895, CVE-2019-14898, CVE-2019-17133, CVE-2019-0155, CVE-2018-20856, CVE-2019-10126, CVE-2019-3846, CVE-2019-9506, CVE-2019-14835, CVE-2019-1125, CVE-2019-9500, CVE-2018-10853, CVE-2018-18281, CVE-2019-11599, CVE-2019-11810, CVE-2019-3900, CVE-2019-5489, CVE-2018-18066, CVE-2018-19985, CVE-2018-20169, CVE-2018-7191, CVE-2019-13233, CVE-2019-15916, CVE-2019-18660, CVE-2019-3901, CVE-2019-16056, CVE-2019-5436, CVE-2020-12888, CVE-2020-0543, CVE-2020-0548, CVE-2020-0549, CVE-2020-8608, CVE-2019-13232, CVE-2020-7039, CVE-2018-10360, CVE-2019-14821, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2015-9251, CVE-2019-11358, CVE-2020-11023, CVE-2020-11022, CVE-2016-10707, CVE-2020-11612, CVE-2019-20444, CVE-2019-20445, CVE-2019-16869, CVE-2018-1000613, CVE-2018-1000180, CVE-2017-18640, CVE-2020-24750, CVE-2020-24616, CVE-2020-14195, CVE-2020-14062, CVE-2020-14061, CVE-2020-14060, CVE-2020-5398, CVE-2019-0230, CVE-2019-0233, CVE-2019-17041, CVE-2019-17042, CVE-2018-4300, CVE-2018-14567, CVE-2020-2922, CVE-2019-3820, CVE-2021-3156, CVE-2020-1971, CVE-2020-15862, CVE-2020-8695, CVE-2020-8696, CVE-2020-8698, CVE-2020-8622, CVE-2020-8623, CVE-2020-8624, CVE-2019-20907, CVE-2020-8177, CVE-2020-12351, CVE-2020-12352, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-1472, CVE-2020-14318, CVE-2020-14323, CVE-2020-25637, CVE-2020-14363, CVE-2020-15999, CVE-2019-10744, CVE-2013-7285,CVE-2019-10173,CVE-2020-17530,CVE-2020-25649,CVE-2020-35490,CVE-2020-35491,CVE-2020-35728,CVE-2020-36181,CVE-2020-36184,CVE-2020-36185,CVE-2020-36186,CVE-2020-36187,CVE-2020-36188,CVE-2020-36189,CVE-2020-36179,CVE-2020-36180,CVE-2020-36182,CVE-2020-36183,CVE-2021-20190,CVE-2018-20801,CVE-2020-8203,CVE-2018-1258,CVE-2018-15756,CVE-2020-5398,CVE-2017-15288,CVE-2020-28488,CVE-2020-26217,CVE-2020-26258,CVE-2019-10768,CVE-2018-3721,CVE-2018-16487,CVE-2019-1010266,CVE-2018-1257,CVE-2018-11039,CVE-2018-11040,CVE-2016-7103,CVE-2020-26259,CVE-2020-7676, CVE-2020-15862,CVE-2020-1472,CVE-2020-14323,CVE-2020-25637,CVE-2020-10543,CVE-2020-10878,CVE-2020-12723

Vulnerabilities fixed in 3.3.0.1 GA can be found here.