Backup Exec 20.4 Patch Update Release Notes

Description

This Update contains added platform support, critical updates, and enhancements for Backup Exec 20 revision 1188.0, Backup Exec 20.1 revision 1188.1237, Backup Exec 20.2 revision 1188.1650 and 20.3 revision 20.0.1188.1863

This update will patch Backup Exec 20.0 (20.0.1188.0), Backup Exec 20.1 (20.0.1188.1237), Backup Exec 20.2 (20.0.1188.1650), and Backup Exec 20.3 (20.0.1188.1863) to Backup Exec 20.4 (20.0.1188.2217).

New features/enhancements are included in this release (2019-05-06)

- Ransomware Resilience.Backup Exec monitors access to its disk-based storage device locations. Any changes to the disk-based storage device locations can only be done by Backup Exec. No other process can write to the disk storage.
- Support for Resilient Change Tracking (RCT). Backup Exec supports protection of virtual machines hosted on Hyper-V using the Resilient Change Tracking (RCT) method. Resilient Change Tracking (RCT) is available for Hyper-V running on Windows Server 2016 and later.
- Backup for Office 365 with [Veritas SaaS Backup]. Free trial of Veritas SaaS Backup is available for Backup Exec customers for fully automated data protection for Office 365 and other SaaS workloads.
- Support for [Veritas Smart Meter]. Backup Exec users can track their capacity usage and entitlement with Veritas Smart Meter.
- Support for Server Message Block (SMB) and Scale-Out File Server. Backup Exec supports protection of virtual machines hosted on Hyper-V with its disks located on Server Message Block (SMB) and Scale-Out File Servers. SMB and Scale-Out File Server are applicable if the Resilient Change Tracking (RCT) method is selected and Hyper-V is running on Windows Server 2016 and later.
- Support for Microsoft SharePoint Server 2016 with GRT. Backup Exec now adds support for granular restore of individual items (GRT) from SharePoint 2016 backups.
- Backup virtual machine disks selectively - Hyper-V. You can now choose which virtual disks to include or exclude when backing up Hyper-V virtual machines. This feature is applicable for virtual machines hosted on Hyper-V and is already available for VMware virtual machines.
- Backup jobs with debug logging enabled. Backup Exec users can now run a backup or restore job with debug logging enabled. The completed job generates the debug logs that can be sent to technical support.
- Microsoft Exchange 2013 CU 22
- Microsoft Exchange 2016 CU12
- Microsoft Exchange 2019 CU1
- SLES 15
- Oracle Linux (OEL) 6 Update 7, 9, and 10
- RHEL 7.6

- Enterprise Vault 12.4
- XenServer 7.6
- Sharepoint 2016 GRT

Backup Exec 20.4 Patch Update can be downloaded from the Veritas Entitlement Management System (VEMS), the Veritas Download Center or thru Veritas Update.

For more information on what's new in Backup Exec 20.4 Patch Update please refer to the updated Readme document.

IMPORTANT NOTE:

If you are installing for the first time, please be sure you have the latest Backup Exec installation media with Update 4 embedded. To obtain the latest install media, have your serial number available and go to https://vam.veritas.com to download.

If upgrading from Backup Exec 16 or earlier versions, please visit https://vam.veritas.com to obtain the latest install media and upgrade serial numbers.

This patch will be available on Veritas Update approximately 2 weeks after General Availability Release.

Prerequisites

- Administrative privileges are required to install this Feature Pack.
- Backup Exec 20, 20.1, 20.2 or 20.3.

Post requisites

- A full backup is recommended after installing this Feature Pack.
- Remote Agent for Windows Servers will need to be updated after installing this Feature Pack.
- Remote Agent for Linux/Unix Servers (RALUS/RAMS) will need to be updated after installing this Feature Pack.
- Update SDR media.
- Veritas recommends to reboot the system(s) after applying a Hotfix or Feature Pack.

Known issues resolved

- Oracle Database Restore from Duplicate set may fail if duplicate job was configured to use "'Most Recent Full Backup" job option. (100044907)
- VMware backup of the VMware Virtual Machine on Backup Exec 20.3 may skip VMDK backup if Global Excludes configured. (100044320)
- "Hardware [if available, otherwise none]" is logged in Job log though Compression Type for Disk cartridge is "None". (100041297)
- Expired media may not be deleted when capacity information alert is observed with a storage device pool. (100043400)
- Third party processes that access performance monitor may crash after the system with Backup Exec 20.1 or higher service starts. (100044383)
- V-79-57344-5125 - Oracle.exe may crash after Unknown CORBA exception. Unable to contact the Backup Exec server. (100043481)
- Backup Exec 20 backup jobs fail with "0xe000fe30 - A communications failure has occurred" error if the Windows firewall is enabled on the Remote server and the TCP dynamic range has been enabled in "Network and Security". (100044305)
- Exchange 2010 Differential or Incremental backup job to Disk storage takes long time to process GRT metadata. (100033875)
- Duplicate job status is showing "Ready, no idle devices available" even though drives are showing not in use by tape library. (100041579)
- A failed Push Install of Backup Exec Remote Agent might result in files being from the target location. (100045493)
- Backup Exec console error "The query for ASRVM failed"
- Resolved Backup Exec server issue with receiving and displaying Enterprise Vault resource advertising from EV Enterprise Vault server Agent for Windows.
- SDR recovery fails with "A failure occurred creating an object"
- SDR recovery of a remote server fails with the error "Failed to automatically create the critical volumes on the disks".