SECTION 1 - INTRODUCTION

1.1 – Veeam Products

- a. Availability Suite Capabilities
 - 1. High-Speed Recovery rapid recovery of what you want the way you want it
 - 2. Data Loss Avoidance near-continuous data protection & streamlined disaster recovery
 - 3. Verified Recoverability guaranteed recovery of every file, app, or virtual server
 - 4. Leveraged Data low-risk deployment with a production-like test environment
 - Complete Visibility proactive monitoring & alerting of issues before operational impact

Benefit	Description
High-Speed Recovery	Enables low recovery time objectives (RTOs) of <15 minutes; enables rapid recovery of the data customers want, in the form that they want it
Data Loss Avoidance	Avoids data loss by enabling low recovery point objectives (RPOs) of <15 minutes, and by facilitating off-site data protection
Verified Recoverability	Ensures that files, applications, and virtual servers can be reliably restored when needed; ensures business resiliency through automated backup and DR testing
Leveraged Data	Eliminates the risks associated with application deployment, configuration changes, and other testing scenarios; allows testing of changes in a production-like environment before actually deploying them
Complete Visibility	Provides monitoring and alerting tools so that you can discover and be alerted to issues and potential problems in your IT environment before they have a significant impact on your operations

1.2 – Backup & Replication

- a. An availability, data protection, & DR solution for vSphere & Hyper-V
 - 1. Image-based backup and image-based replication
 - 2. Backup VMs, VM Containers, or VM Disks
 - 3. Replicate on-site (HA) or off-site (DR)
 - 4. Near-CDP
- b. vPower
 - 1. Instant VM Recovery reduced time for VM recovery
 - 2. Verify VM Backup (SureBackup) start/test VMs directly from backups in isolated environment (SureBackup)

- 3. Veeam Explorers & Universal App Item Recovery (U-AIR) restore items (files, dbs, AD objects)
- 4. Multi-OS File Level Recovry (FLR) restore guest OS files directly from both backups & replicas (Windows OS only)
 - a) FLR Restore Wizard restores from FAT, NTFS, or ReFS
 - b) Multi-OS FLR Wizard restores from Linux, Unix, 'Other'
 - c) Instant VM Recovery restore files not supported by file restore wizards

1.3 – Veeam ONE

- a. Monitoring, reporting, capacity planning tool for vSphere/Hyper-V & backup infrastructures
 - 1. Real-time monitoring 24x7 monitoring, alerting with builtin intelligence for fast troubleshooting & problem resolution
 - Documentation & management reporting pre-deployment analysis of b/u requirements, documentation of structure and state of virtual & b/u infrastructures, automated & on-demand reporting
 - 3. Capacity Planning trend analysis, provision recommendations, what-if modeling
 - 4. Chargeback/Billing visibility into IT costs of compute, storage, & b/u resources
 - 5. Business Categorization tech- and business-oriented views of virtual environment
- 1.4 Veeam Management Pack for System Center
 - a. Monitoring, reporting, capacity planning tool for vSphere & Hyper-V
 - 1. Extends System Center's capabilities to both Hyper-V & vSphere
 - 2. Monitors VMs, Hosts, hardware, network, & storage resources
 - 3. Monitors VB&R
 - 4. Provides drill-down view from app > virtualization layer & further to the hardware sensors data
- 1.5 Veeam Add-On for Kaseya
 - a. Allows Managed Service Provideers (MSPs) to remotely monitor their Veeam backup infrastructures and estimate data protection efficiencies for managed virtual environments, within the Kaseya web interface
 - 1. Audit state and performance of Veeam components
 - 2. Analyze VM data protection for managed customer virtual environments
 - 3. See overview of all job types managed by Veeam & monitor job results
 - 4. Receive alerts
 - 5. Generate reports based on data collected from Veeam backup servers

- 6. Monitor backup infrastructure machines & protected VMs, perform basic maintenance, troubleshoot/fix Kaseya Live Connect
- 1.6 Veeam Plug-In for LabTech
 - a. For Service Provideers (SPs) who use LabTech Remote Monitor Management (RMM)
 - b. Single pane of glass view of Veeam backup activity within LabTech Control Center
 - 1. Manage, view, monitor Veeam backup jobs: start, stop, retry, disable jobs
 - 2. Analyze protected/unprotected backup & replica VMs for valid restore points
 - 3. Alerting
 - 4. Perform day-to-day maintenance, troubeshooting, & fix problems
 - 5. Generate reports from data collected by Veeam backup servers & VMs
- 1.7 Veeam Availability Suite
 - a. Combination of VB&R and Veeam ONE
 - b. Capabilities
 - 1. RTPO < 15m for most workloads

1.8 – Key Concepts

a. Details

Concept	Details
Business Continuity (BC)	An activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.
Disaster Recovery (DR)	A process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a natural or human-induced disaster.
Recovery Point Objective (RPO)	The maximum tolerable period in which data might be lost from an IT service due to a major incident. Essentially, it is the acceptable time period data can be backdated to a restore.
Recovery Time Objective (RTO)	The duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. Essentially, it is the amount of time allowable between off-line due to disaster and on-line from recovery.

1.9 - Course Overview

- a. Availabiity for the always-on business (See Section 1.1 chart)
 - 1. High-speed Recovery RTO of < 15m for data customers want in form they want
 - 2. Data Loss Avoidance RPO of < 15m, and facilitating off-site DP
 - 3. Verified Recoverability ensures files, etc can be reliably restored; DR testing

- 4. Leveraged Data eliminates risks associated with app deployment, etc
- 5. Complete Visibility provides monitor/alert tools
- b. Exam Prep
 - 1. Read course handbook and labs guide
 - 2. Read Veeam Availability Suite Release Notes
 - 3. Read Veeam Availability Suite What's New PDF
 - 4. Take practice exams:
 - a) https://veeam.university/vmcepractice
 - b) http://rhyshammond.com
 - c) <u>https://www.perfectcloud.org/practice-exams/veeam-certified-engineer-v9/</u>

SECTION 2 - DEPLOYMENT

2.1 – Core Components

- a. Veeam Backup Server
 - 1. Windows-based machine, physical or virtual
 - 2. "Configuration & control center"
 - 3. Roles:
 - a) Coordinates backup, replication, recovery verification, & restore tasks
 - b) Controls job scheduling and resource allocation
 - c) Sets up & manages backup infrastructure components as well as specify global backup infrastructure settings
 - d) "Point of control" for dispatching jobs to Proxies
 - 4. Services used:
 - a) Veeam Backup Service manages scheduled jobs & serves Enterprise Manager requests
 - b) Veeam Installer Service enables installing, updating, and configuring VB&R components
 - c) Veeam Backup Catalog Service manages guest OS file system indexing for VMs & repliates system index data files to enable search through guest OS files
 - d) Veeam Data Mover Service responsible for deploying & coordinating executable modules acting as 'data movers' & performs main job activities on behalf of VB&R, communicating with VMware Tools, copies VM files, performs data dedup/compression
 - e) Veeam Mount Service mounts backups & replicas for file-level access, browsing VM guest file system, and restoring guest OS & application files
 - f) Veeam Broker Service interacts with virtual infrastructure to collect & cache the virtual infrastructure topology; jobs query this info which in turn accelerates job/task performance
 - 5. Components used:

- a) SQL Database used by Veeam Backup Service, Veeam Backup Catalog Service, & Veeam Backup Shell to store data about the backup infrastructure
- b) Veeam Backup Powershell Snap-In MS Windows Powershell extension; perform backup, replication, & recovery tasks
- b. Backup Proxy (VMware)
 - 1. Sits between data soure & target to process jobs and deliver backup traffic **NOTE:** The Veeam Server is the default Proxy until a dedicated Proxy is implemented
 - 2. <u>PROXY PRIMARY ROLE</u>: provides an optimal route for backup traffic & enables efficient data transfer
 - 3. Windows-based machine, physical or virtual
 - 4. Deployed local (primary) or remote; component install is automated by VB&R
 - 5. Scalable, depending on workload & to optimize performance
 - 6. Tasks:
 - a) Retrieves VM data from production storage
 - b) Compresses & sends data to backup repository (backup) or another proxy (replica)
 - Transport Modes methods used by the Veeam Data Mover Service to read VM data from source & write it to target; job efficiency & completion time mainly depends on mode type, which in turn is dependent on datastore type (FC/ISCSI/NFS/Local) & server type (virtual/physical)
 - a) Direct Storage (san) VB&R reads/writes data directly to/from storage where VM or backup data are located; <u>unification of Direct SAN & Direct NFS</u>
 - 1) Direct SAN

i. Recommended mode for VM disks on shared storage connected via FC, FCoE, ISCSI, NFS, or SAS

ii. Can be used for the following Veeam tasks: backup, replication, VM Copy, Quick Migration, Entire VM Restore (**thick disks only**), VM disk restore, & Replica Failback

iii. For thin disk restores, use hotadd or nbd, or change disk type to thick iv. For FC, use a physical Proxy server

2) Direct NFS

i. Can be used with NFS v3 and v4.1 (v4.1 = with vSphere 6.0+)

ii. Proxy must have root access to NFS Datastore

iii. Proxy must have Read/Write permissions to the NFS Datastore

iv. **Deploys native Veeam NFS client** on Proxy to read/write from/to NFS v. NFS Proxy Selection: Automatic selection = first, Proxy with least hops to NFS datastore, then least busy; Explicit Assignment = least busy Proxy

3) Local storage NOT recommended for FC/iSCSI/NFS

i. If using "hotadd" for local storage, install Proxy VM on every ESXi Host ii. If using NBD for local, install 1 virtual or physical Proxy in environment

- 4) iSCSI/NFS can be physical or virtual for either Direct SAN or "hotadd"
- b) Virtual Appliance (hotadd)
 - 1) Can only be used when Proxy is a VM

- 2) Uses an ESXi Host SCSI Hot-Add capability
- 3) VM data retrieved from storage through ESXi I/O stack
- c) Network (nbd)
 - 1) Only *applicable* mode when Proxy is physical & storage is local
 - 2) Uses VMware VDDK to communicate with ESXi Hosts
 - 3) Method/mode used when WRITING data to target; can't configure other modes for writing... VB&R will auto-select based on Proxy configuration
- Automatic mode selection option Veeam scans the Proxy and determines the optimal mode, if multiple modes are available, it begins with direct storage > virtual appliance > network
- e) ALL modes use VMware's VMware vStorage APIs for Data Protection (VADP), starting from v4
- f) VM disks are processed 1 by 1 OR in parallel depending on global settings
- g) If a VM has several disks on different storage types, VB&R will use different transport modes, so make sure to select the "Falover to network mode if primary mode is unavailable" option when configuring backup jobs
- c. Backup Proxy (Hyper-V)
 - 1. Backup Modes:
 - a) On-Host Backup
 - 1) Data is processed on source host VM resides (this is default mode)
 - 2) Imposes high load on Host > CPU/network overhead
 - b) Off-Host Backup
 - 1) Data processed on dedicated host; acts as 'data mover'
 - 2) Online backup method recommended (i.e. quiescing VMs via VSS)
 - Auto-recovery process is triggered after 2nd (external) VSS (vol) snapshot

 Process on Win2012 & earlier so VM data is consistent at moment of
 backup

ii. For Win2012 R2, Auto-Recovery Checkpoints are used, and taken before the internal snapshot

- iii. Win2016 uses Production Checkpoints
- 4) For Off-Host Backup Mode, VB&R uses 'transportable shadow copies' performed at the SAN layer
- 5) Off-Host Backup Host requirement MS Windows 2008 R2/2012/2012 R2/2016 with Hyper-V enabled; Nano version not supported

NOTE: Proxy Host version must match Host version source data resides

- Services & Components for Backup Proxy (VMware) & Offhost Backup Proxy (Hyper-V)
 - a) Veeam Installer Service
 - b) Veeam Data Mover Service responsible for deploying & coordinating executable modules acting as 'data movers' & performs main job activities on behalf of VB&R (i.e. communicates with VMware Tools, copies VM files, performs data dedup/compression)

- c) Hyper-V Integration Service (Hyper-V only) communicates with VSS framework & performs recovery tasks
- d. Backup Repository
 - 1. Used to store:
 - a) Backup chains
 - b) Backup metadata
 - c) VM Copies (VMware)
 - d) Replica metadata
 - 2. Repository Types:
 - a) Windows server local, DAS, or FC/ISCSI; can use vPower NFS (VMware)
 - b) Linux server local, DAS, NFS, or FC/ISCSI
 - c) **CIFS** <u>Data Mover Service not supported</u>, so data is written from a *Windows Gateway server* (performed by associated Proxy server by default)
 - d) **Dedup appliance** Data Domain, ExaGrid, HPE StoreOnce
 - Fast Clone uses MS Block Cloning on ReFS 3 allowing apps to quickly copy data blocks between different files or within limits of one file via low-cost metadata operation
 - a) Requirements
 - 1) MS Windows 2016 or SMB 3.11
 - 2) ReFS 3.0 file system
 - 3) All backup files must be on the same volume
 - 4) VB&R 9.5 (not upgraded)
 - 5) Repository setting Align Blocks
 - b) Fast Clone is used by default if Repositories meet requirements; can be disabled in Registry via Veeam Support
 - c) File start/end offsets must be aligned to cluster boundaries (4K or 64K); 'Align Data Blocks' setting enabled automatically
 - d) Supported on Simple, SOBR, and Cloud Repositories
 - e) Used for "synthetic operations": merging backups, synthetic fulls, reverse incrementals, compact fulls, archive backup creation
 - 4. Offsite Backup for best performance, install a remote Proxy
 - Scale-Out Backup Repository (SOBR) 'extending' several Repositories (extents) into "one"; used for backups, backup copies, & VeeamZIP
 - a) Data placement policies:
 - 1) Data Locality all backup chain files placed on same extent
 - 2) Performance backup chain files placed on different extents
 - 3) <u>Policy setting changes start on next job run</u>; extent setting changes start after next full backup creation
 - b) View session info to see where VM data are stored (on which extent[s])
 - c) Limitations:
 - 1) Ent (limited extents)/Ent+ only
 - 2) Extent can't be used as standalone Repository until removed from SOBR
 - 3) If downgrade Veeam to Std can only do *restore* operations

- 4) Can't use for config backups, replication, VM copies, or Endpoint backups
- 5) Can't use Repos as extent if unsupported job in #4 is targeted to it, or Repos has data still on it from unsupported job type
- 6) Can't use SOBR as Cloud Repository, or add Cloud Repository as an extent
- 7) Can't use rotated drive Repository as an extent
- 8) Can't add SOBR to another SOBR
- 9) Can add Repos as extent if already an extent
- 10) Can't add Repos as extent if activity is being performed on it (i.e. Backup job)
- 6. Mount Server
 - a) Required if restoring VM guest OS files & apps to original location; acts as a 'mount point' for backups in the Repository
 - b) Routes VM traffic in an optimal way, reducing network load & speeds up restore process
 - c) Created for every Repository and is associated with it
 - d) Requirements:
 - 1) Windows machine, physical or VM
 - 2) Must be 64bit
 - 3) Access to Repository it's assigned to, & original VM
 - e) Role assigned to:
 - 1) For Windows Repositories, the Repository itself
 - 2) For Linux Repositories, the Backup Server
 - 3) Where Veeam Console is installed if machine not registered in config DB
 - 4) Scale-Out Repositories assigned on each extent
 - f) Services and components Veeam Mount Service, .NET 4.5.2
- 7. Proxy Affinity determines what Proxies are eligible to access a specific Repository
 - a) Ent and Ent+ only
 - b) Set at the Repository level (rt-click > Proxy Affinity; or from Ribbon)
 - c) Used on: simple, SOBR (extent level), & Cloud Repositories
 - d) Used for: Backups, VeeamZIP, VM copies, VM restore, hard disk restore
- 2.2 Optional Components
 - a. Veeam Backup Enterprise Manager for distributed environments with multiple VB&R servers to consolidate the view via browser UI
 - Can be physical or virtual; dedicated machine or installed on VB&R server; MUST be x64 bit
 - 2. Central license mgmt for all Backup Servers
 - 3. Tasks:
 - a) Manage b/u & replica jobs
 - b) Edit & clone jobs
 - c) Monitor job state

- d) Reporting
- e) Searching of Windows VMs
- 4. Components:
 - a) Enterprise Manager
 - b) Enterprise Manager DB
 - c) Veeam Backup Catalog Service
- b. Universal Application Item-Level Recovery (U-AIR) Wizard
 - 1. Provides ability to restore special virtualized apps (Exchange, AD, SQL, Oracle) when there's no suitable Veeam Explorer
 - 2. Leverages vPower
 - 3. Standalone component
- c. Veeam Backup Search
 - 1. Used with Enterprise Manager for search performance optimization, run by MOSS Integration Service
 - 2. For frequent searches, recommended to install Veeam Search on dedicated server with MS Search Server
- 2.3 Deployment Scenarios
 - a. Simple Deployment
 - 1. Deployment with all roles (Backup Server, Proxy, Repository, Mount Server, Guest Interaction Proxy) installed on 1 server, physical or VM
 - b. Advanced Deployment offloading Proxy & Repository components to dedicated servers, beit VMware or Hyper-V deployment
 - 1. Jobs can migrate between Proxies if 1 of them becomes overloaded/unavailable
 - 2. Installing components is automated on distributed Proxy/Repository servers
 - c. Distributed Deployment recommended for large, geo-dispersed environments with multiple VB&R servers, using Veeam Enterprise Manager
 - 1. Benefits scalable, no SPOF (redundancy), reduces impact on production, simplifies install, controls storage saturation (via Parallel Processing)
 - 2. Automatically selects optimal resources via the Veeam Backup Service
 - d. Parallel Processing multiple VMs and VM disks processed in parallel optimizing b/u performance and increasing storage efficiency; a **global setting**
 - 1. Each task requires 1 CPU Core
 - 2. Effects following tasks:
 - a) Backups
 - b) Backup Copy
 - c) Replication
 - d) Entire VM Restore
 - e) VM Disk Restore
 - e. Backup I/O (Storage Latency) Control setting limits for all Host datastores; a **global setting**;
 - 1. Enterprise (global only) and Enterprise+ license (allows per datastore setting)

- 2.4 Prerequisites
 - a. Requirements:
 - 1. Enable network ports, if necessary
 - 2. Ensure user accounts have proper permissions (see #20 below)
 - 3. (Virtual) Platform Support
 - a) vSphere and ESX(i) 4.1/5.x/6.x; Free not supported; vCloud Director 5.5+
 - b) Hyper-V Windows 2008 R2 SP1/2012/2012R2/2016/Nano; Free supported
 - c) VM OSs all are supported for both VMware & MS from; application-aware image is supported for 2003SP1+, EXCEPT Nano Server due to no VSS; ReFS is supported with VB&R installed on Windows 2012+
 - d) VMware Tools optional but required for aaplication-aware image processing (AAIP), Win File-Level Restore, & SureBackup (tests)
 - e) Not supported

(VMware)

- 1) VMs with SCSI Bus Sharing not supported (unable to snapshot)
- 2) Physical RDMs
- 3) Independent Disks
- 4) Disks connected via iSCSI Initiator

(Hyper-V)

5) VMs with passthrough disks & connected via iSCSI Initiator

- 4. Backup Server (VB&R) Requirements:
 - a) .NET 4.5.2, Windows Installer 4.5, Visual C++ 2010 SP1, PoSH 2.0 (optional)
 - b) Must be 64bit CPU
 - c) 4GB RAM + 500MB for each concurrent job
 - d) Disk 2GB for install; 4.5GB for .NET 4.5.2
 - e) OS 64bit, MS Win 2008 SP2/R2 SP1, 2012/2012R2, 2016, Win7SP1/8.x/10
 - f) SQL Default = 2012 SP3 Express; or SQL 2008/2008R2, 2012, 2014, 2016
- 5. Backup Proxy Requirements:
 - a) x86 (64bit recommended) ; 2 cores, plus 1 Core for each concurrent task **NOTE:** for VMs on ESXi 5.5+ Proxies must be on 64bit Windows
 - b) 2GB RAM + 200MB for each concurrent task
 - c) 300MB disk space
 - d) 1Gbps NIC for on-site b/u; 1Mbps for off-site
 - e) OS 32b & 64bit supported; same OS's as VB&R + Vista SP2
- 6. Backup Repository Requirements:
 - a) x86 (64bit recommended)
 - b) 4GB RAM + 2GB (32bit) or 4GB (64bit) for each concurrent job
 - c) 1Gbps NIC for on-site b/u; 1Mbps for off-site
 - d) OS 32b & 64bit supported; same OS's as VB&R + Vista SP2, Linux
- 7. Tape Server Requirements (and Cloud Gateway Server)
 - a) x86 (64bit recommended)

- b) 800MB RAM for file > tape backup; 800MB for catalog jobs (i.e. 1.6GB)
- c) 300MB disk space + 10GB temp storage
- d) 1Gbps NIC
- e) OS 32b & 64bit supported; same OS's as VB&R + Vista SP2
- 8. WAN Accelerator
 - a) Must be 64bit CPU
 - b) 8GB RAM
 - c) Disk space = depends on role
 - d) 1Gbps NIC
 - e) OS 32b & 64bit supported; same OS's as VB&R + Vista SP2
- 9. Cloud Gateway see Tape Server
- 10. Backup Target Storage Supported:
 - a) Local on Repository
 - b) DAS connected to Repository (external USB/eSATA/RDM)
 - c) SAN FC, FCoE, ISCSI
 - d) NAS represented as SMB (CIFS) or NFS Share
 - e) Dedup appliances:
 - 1) Dell DataDomain OS 5.4+
 - 2) ExaGrid 4.8.0.351 P28+
 - 3) HPE StoreOnce 3.13.1+
- 11. Storage Integration Systems (VMware)
 - a) Cisco HyperFlex 2.0+
 - b) Dell EMC VNX, VNX2, VNXe, Unity
 - c) HPE 3PAR StoreServ 3.1.2, StoreVirtual (LeftHand 9.5-12.6/ P4000), StoreVirtual VSA
 - d) NetApp FAS, FlexArray (V-Series), Edge VSA, IBM N Series (FAS OEM), ONTAP 8.1-9.2
 - e) Nimble AF/CF-Series 2.3+
- 12. Tape Requirements
 - a) LTO3+ tape libraries (including VTL)
 - b) Tape Device MUST be directly attached to VB&R & Tape Server via SAS/FC/iSCSI (passthrough not supported)
 - c) Tape devices with VENDOR-SPECIFIC drivers for Windows; if not native SCSI commands mode must be enabled
- 13. Veeam Enterprise Manager:
 - a) Must be 64bit CPU
 - b) 4GB RAM
 - c) 2GB install + space for catalog data
 - d) 1Mbps NIC
 - e) OS 64bit, MS Win 2008 SP2/R2 SP1, 2012/2012R2, 2016, Win7SP1/8.1/10
 - f) IIS7+
 - g) Browsers: IE 10+, Edge, latest Chrome/FF
 - h) Excel 2003 (view reports)

- i) SQL see VB&R DB
- 14. Search Server
 - a) For CPU/RAM/DISK/OS see MS Search Server req's
 - b) MS Search Server 2008/2010 Full or Express
- 15. Veeam Explorer Exchange
 - a) x64 DB versions of Exchange 2010SP1/SP2/SP3; 2013/SP1; 2016
 - b) ese.dll file installed with Exchange to open mailboxes
 - c) Optional Outlook 2010/2013/2016 for PST exports
- 16. Veeam Explorer Sharepoint
 - a) Sharepoint 2010/2013/2016 all editions (Foundation, Standard, Enterprise)
 - b) Insalled on VB&R server; all VB&R editions including VB&R FREE supported
 - c) Staging SQL Server can run on VB&R or remote server; must be same or later version of SQL
 - Remote BLOB Stores (RBS) support must be virtualized and included in VB&R backup, or on the local machine running SP Explorer & Staging SQL Svr
- 17. Veeam Explorer SQL
 - a) SQL 2005 SP4, 2008/R2, 2012, 2014, 2016; all editions; Aval Grps 2012+
 - b) Staging SQL Server Default is VB&R SQL; must be same Version/Edition as SQL recovering
- 18. Veeam Explorer Oracle
 - a) Enterprise and Enterprise+ license
 - b) Oracle 11g or 12c; XE supported for Windows only
 - c) Real Application Clusters (RAC) not supported
 - d) Uses staging Oracle server; local staging supported for Windows only; XE can't be used as stage server; ASM restore = must be on stage/target DBs
- 19. Veeam Explorer Active Directory
 - a) DCs Windows 2003SP2/2008/2008R2/2012/2012R2/2016
 - b) All VB&R Editions supported
 - c) PoSH 2.0+
 - d) esent.dll to open AD DB files, located in %SystemRoot% on DC
 - For password restore, make sure %SystemRoot%\System32\Config directory ("registry hive) is available; and same version as AD Domain Services used to create DB files
 - e) .dit used for AD DB restores
 - 1) For imported backup restores, 'registry hive' must be in same folder as the **.dit** file
 - f) For Active Directory DB restores, Explorer must be installed on same Windows OS as source DC OS
- 20. Permissions:
 - a) VB&R and Enterprise Manager setup local admin
 - b) Target/Source Host root or local admin for Hosts/Linux, or admin for vCenter; Write for target folders and shares
 - c) SQL DB Owner

- d) Enterprise Manager Portal Admin, Restore Oper, or Portal User
- e) Backup Search local admin
- f) Exchange Explorer full access to Exchange DB/logs; read/write to files in DB folder
- g) Sharepoint Explorer sysadmin fixed server role on Staging server; Full Control
- 2.5 Upgrading VB&R
 - a. Requirements
 - 1. Minimum VB&R version for direct 9.5 upgrade is 8U3 or 9
 - 2. Upgrade VeeamONE first; supports monitoring VB&R versions 8.0, 9.0, 9.5
 - 3. Minimum SQL 2008+; Windows 2008SP2+ or Win7SP1+ 64bit.. migrate if currently not on supported OS
 - 4. Verify Cloud Connect provider is upgraded to version you're upgrading to
 - 5. No active jobs; disable jobs, and/or stop all Veeam Services
 - 6. Backup config databases (VB&R and Ent Mgr) right before upgrade
 - 7. If using Enterprise Manager, upgrade from it; EM supports VB&R 8.0, 9.0, 9.5
 - b. After upgrade, install latest Update, if available
 - c. Upgrade ancillary components & services (Proxies & Repositories), and standalone Consoles

SECTION 3 – INITIAL CONFIGURATION

- 3.1 Adding Servers
 - a. Managed Server "Roles"
 - 1. Source Host
 - 2. Target (Replication) Host
 - 3. Backup Proxy
 - 4. Backup Repository
 - b. VMware
 - 1. VMware Server (vCenter/ESXi Host)
 - 2. vCloud Director
 - 3. Windows Server
 - 4. Linux Server
 - c. Hyper-V
 - 1. Hyper-V
 - 2. SMB 3 Server
 - 3. Windows Server
 - 4. Linux Server

Added Server Types Used As:

Server Type	Source Host	Target Host	Proxy	Repository
vCenter/ESXi/Hyper-V/Cluster	х	х		
Windows			х	x
Linux				x
vCloud Director	х			
SMB v3	х			

- 3.2 Adding VMware Backup Proxy
 - a. 'Data Mover'; performs main data handling retrieves, processes, transfers data to targets
 - b. Windows server already added to managed servers list
 - c. Backup (VB&R) Server added as "default" Proxy during install
- 3.3 Adding Backup Repositories
 - a. Location for storing data (Backups & VM copies) and auxilliary files (replica & backup metadata)
 - b. <u>Windows</u> or <u>Linux</u> added in managed server list, <u>CIFS</u> share, or <u>Dedup Appliance</u>
 - c. Windows Repositories can fill role of vPower NFS for multi-OS file-level restores, Instant VM Recovery, SureBackup, & U-AIR (VMware only)
 - d. Can be permanently removed from VB&R; data does NOT get deleted upon removal
 - 1. Before removal, Repository has to be removed from any Backup, Replication, or Configuration Backup jobs
- 3.4 Data Location Tagging
 - a. Locations can be added to:
 - 1. Virtual Infrastructure Objects vCenter, Datacenters, Clusters, Hosts
 - 2. Backup Infrastructure Objects Simple Repositories, SOBRs, Tape Libraries, Tape Vaults
 - 3. Agent Management Objects Protection Groups
 - b. Veeam displays data migration info/stats for Backups, VeeamZip, Replication, Failbacks, VM Copies, Quick Migrations, Entire VM Restores, & SureBackups
 - **NOTE:** Veeam does NOT display info about VM data migration for file copies
 - c. Creating and Assigning Locations
 - 1. Rt-click object > Location > Manage Locations; click Add and enter a name
 - d. Editing Locations
 - 1. Same as Assign/Add, but click the Edit button
 - e. Deleting Locations
 - 1. Same as Assign/Edit, but when in Locations, select object > Delete

- f. Export/Import Locations (in XML format)
 - 1. Same area as above > Manage Locations, then click Export; give it a name
 - 2. Same area as above > Manage Locations, then click Import
- 3.5 Performing Configuration Backup & Restore
 - a. Exporting Veeam SQL Database configuration data to a backup file on a Repository
 - b. Retrieval of SQL data written into set of .xml files, then archived to a .bco file
 - c. The objects the configuration data backup contains:

OBJECT	CONTENTS
Backup infrastructure	Hosts, Servers, Proxies, Repositories,
components/objects	WAN Accelerators, jobs, global settings
Backups	Backups, Replicas, Backup Copies
Sessions	Job sessions
Tapes	Connected Tape Libraries

NOTE: If encryption is not enabled in VB&R, passwords are not kept & will need reentered in credential store upon config backup restoration

- d. Default: runs daily & sent to **\\VeeamConfigBackup\%BackupServer%** folder in default Repository
- e. When creating a new Repository, you can select to have this the new target for the config backup. Future job runs will place .bco files here. Previous b/u's can be copied over to retain restore points
- f. Creating Encrypted Configuration Backups
 - 1. Config Backup encryption is required if 1 pwd is created in VB&R Password Manager; if encryption is not enabled, Config Backup is disabled
 - vB&R creates storage keys & metakeys and places them in VB&R DB. If Config Backup doesn't have encryption enabled, these keys can be compromised
- g. Restoring configuration data
 - 1. Data Restore Methods
 - a. **Data Restore** used if config data got corrupted; SQL data got corrupted; roll back DB to point-in-time; restore data for testing
 - b. **Data Migration** used when wanting to move the VB&R server to a new location (offiste), to essentially get a 'replica'
 - 2. Before Restoration (Prerequisites):
 - a) Stop all jobs; restore stops Backup Service and currently running jobs
 - b) Can only restore to VB&R 9.5 from Config Backups v8U3 and v9
 - c) Can ony perform restore from local VB&R server, not a remote VB&R console

- 3.6 Managing Network Traffic
 - a. Setting Network Traffic Throttling Rules preventing Veeam Backup or Replication jobs from utilizing entire bandwidth
 - 1. *Enforced globally*, limiting maximum throughput of traffic between Veeam Data Mover components
 - 2. Throttling is set for a pair of IP ranges & applied to source & target components
 - a) Proxy and Repository (backup to Windows/Linux Repository)
 - b) Proxy and gateway server (backup to SMB share or Dedup appliance)
 - c) Source and target Repositories or gateway server or WAN accelerators (backup copies)
 - d) Source and target Repositories or WAN accelerators (Replication jobs)
 - e) Repository and tape server (backup to Tape)
 - b. Managing Data Transfer Connections
 - 1. Veeam uses 5 multithreaded TCP/IP data transfer connections by default
 - 2. Global setting to change or disable if needed
 - CRC checks are done on data between source & target; CRC calculated on source & recalculated and compared on the target; if failed, data is auto resent without job impact
 - c. Preferred Networks
 - 1. Helpful feature when wanting to route traffic over a non-prod network
 - 2. Preferred networks must be *defined globally*; if can't be reached, VB&R automatically fails over to prod network by default
 - 3. Applied on following components:
 - a) Proxies
 - b) Repositories
 - c) WAN accelerators
 - d) Gateways
 - e) Log shipping servers
 - f) Tape servers
 - d. Network Traffic Encryption (In-Flight Encryption)
 - 1. Between different subnets, traffic encryption is enabled by default (AES-256)
 - 2. For same subnet encryption, create network traffic rule & select to encrypt traffic

Add New Network Traffic Rule	x
Source IP address range: 192 . 168 . 0 . 1 to 192 . 168 . 0 . 255	
Target IP address range: 192 168 0 1 to 192 168 0 255 Action:	
Throttle network traffic	

- 3.7 Global Settings
 - a. Backup I/O Control
 - 1. Ability to set limits on acceptable latency for VMware or Hyper-V Datastores
 - 2. Ent+ > customizable per Datastore
- 3.8 Global Notification Settings
 - a. For Backup & Replica jobs; success, failure or warning
 - b. To receive one email about all jobs in VB&R, configure on Enterprise Manager server
 - c. Events notified on:
 - 1. Low disk space
 - 2. Support contract expire 14 days before expiry
 - 3. New product version available icon in system tray, displayed once a week
 - 4. Hyper-V/Off-host server Windows updates, only if VB&R connected to Internet
- 3.9 Getting To Know the User Interface (UI)
 - Main Menu Upgrade; Manage Credentials, Passwords, Azure; General Options; Users & Roles; Network Rules; Config Backup; Console (PuTTy & PoSH); Theme; Licensing; Help

≣∗		
$\mathbf{\Lambda}$	Upgrade	
R	Manage Credentials	
	Manage Passwords	
	Manage Azure Accounts	
	General Options	
2.	Users and Roles	
8	Network Traffic Rules	
	Configuration Backup	
	Console	
	Color Theme	•
=8	License	
	Help	•
×	Exit	

- b. Navigation Pane left side window central navigation enabling access to VB&R items in organized views
 - 1. Inventory Pane upper pane; hierarchical list of items relevant for specific view
 - 2. Lower Pane buttons to enable switching between VB&R views
- c. Ribbon & Tabs operation commands organized into logical groups; Home tab is always present; has most common operation cmds; & context-sensitive Tabs



- d. Views
 - 1. Backup & Replication (Home) view of VB&R jobs
 - 2. Backup Infrastructure view of VB&R components
 - 3. Virtual Machines (Inventory) vSphere or Hyper-V infrastructure

- 4. Storage Infrastructure
- 5. Tape Infrastructure
- 6. Cloud Infrastructure
- 7. Files list of 'file tree' of servers (VMs), primarily used for file copy tasks
- 8. History view of job stats

П НОМЕ
BACKUP INFRASTRUCTURE
STORAGE INFRASTRUCTURE
TAPE INFRASTRUCTURE
FILES

e. Working Area - 'main (right) window' displays list of items relevant to a given view

SECTION 4 – PROTECT

4.1 – Creating Backup Jobs

- a. 3-2-1 Rule
 - 3 copies of data in different locations (i.e. 2 backups + prod); using 2 different media types (e.g. disk, tape); having at least 1 copy offsite (e.g. cloud or remote locale)
- b. Before Job Creation
 - 1. Verify all VB&R components installed, added, configured
 - 2. Verify enough Repository disk space
 - a) Total size of VM disk(s) being backed up
 - b) Backup frequency
 - c) Retention period (i.e. number of Restore Points needed)
 - d) Job type Forward or Reverse Incremental
 - e) <u>Change rate</u> of all VMs being backed up **avg of 5%** per VM per day
 - f) Dedup & compression ratio avg of 2:1, but "typical" is 3:1

g) Future growth

NOTE: VeeamONE's **VM Change Rate Estimation report** can be used for potential amount of space needed for target Repositories

3. Available objects when adding VMs to jobs:

(VMware)

- a) Everything
- b) Folder
- c) Cluster
- d) Host
- e) Resource Pool
- f) VirtualApp
- g) VM

(Hyper-V)

- h) Everything
- i) Folder
- j) Host Group
- k) SCVMM
- l) Cluster
- m) Host
- n) VM
- c. Retention Policy every *successful* job run creates a "restore point" (RP)
 - 1. Retention = number of restore points to keep or how far to "roll back" to
 - If RP is set to 3, on 4th successful job run, the first (i.e. earliest) RP will be deleted NOTE: some VMs in the job may not have same # of RPs due to not being in job at initial creation (i.e. VM movement to job and/or storage container)
 - 3. Deleted VMs
 - a) By default, deleted VMs remain on Repository UNLESS configured to delete in job settings (Storage > Advanced > Maintenance tab)
 - b) VMs are deleted when, *after a successful backup job*, the following 2 conditions are met:
 - 1) There are no successful b/u's for "N" days (N = delete VM setting)
 - 2) There are no corrupted backup of VM for "N" days
 - c) Free space is not cleared, but is marked as available to be overwritten
 - d) <u>Backup jobs > default = 14 days</u>; <u>Backup Copy jobs > default = 30 days</u>
 - e) Applied on following job types:
 - 1) Reverse Incremental
 - 2) Forever Forward Incremental
 - 3) Forward Incremental where Synthetic Fulls with Transform is enabled
- d. Backup Methods
 - 1. Reverse Incremental
 - a) Full (.vbk) file created on 1st job run, then incremental (.vrb) file created on subsequent runs
 - b) Incremental changes are "injected" into the .vbk so a) it's at the most recent state, b) the most recent RP is always a full (.vbk)
 - c) Once RP is reached, the earliest (.vrb) file will be deleted

d) Number of backup files will always equal the RP setting



- 2. Forever Forward Incremental incremental option withOUT Synthetic or Active full backup options selected (job's Advanced > Storage Settings, Backup tab)
 - a) Full (.vbk) file created on 1st job run, then incremental (.vib) file created on subsequent runs
 - b) Once RP is reached, the earliest RP (.vib) will be merged into the full (.vbk)
 - c) The full then 'moves forward' a day & the earliest .vib is deleted
 - d) Number of backup files will always equal the RP setting
 - e) **3x I/O during merge process** current **.vib** created; earliest **.vib** read; earliest **.vib** merged [written] to **.vbk**



- 3. Forward Incremental
 - a) Full (.vbk) file created on 1st job run, then incremental (.vib) file created on subsequent runs
 - b) For restoration, a .vbk and all chain .vib's need to be on disk
 - c) Because of "b" above, there will be more RPs on disk than what is set in the Retention Policy



- 4. Active Full
 - a) A new .vbk is created on a job run, from the production storage

- b) Subsequent .vib's will use the new .vbk; old .vbk & .vib files are retained until Retention is met
- c) Can be run manually via shortcut menu of a job, or automatically via Advanced (Storage) Settings in a job, Backup tab
- d) Good to use when Repository storage performance is weak, due to this being a sequential write task (i.e. no transforms); although task is time, bandwidth, & resource consuming
- 5. Synthetic Full
 - a) Previous .vbk & subsequent .vib files consolidated into a new .vbk
 - b) Minimizes load on production storage & network; but high load on target
 - c) Subsequent .vib's will use the new .vbk; old .vbk & .vib files are retained until RP is met
 - d) Only schedulable (not manual or shortcut menu); only available for Forever & Forward Incremental job, <u>not available for Reverse Incremental</u>
 - e) **NOTE:** a Synthetic is only run once/day; if a job is re-ran same day, a .vib is created
- 6. Transform (Incremental) Synthetic Full to Reverse
 - a) Option under Synthetic option
 - b) Less space on disk since the earliest .vbk is removed after transform process
 - c) Time-consuming
- e. Changed Block Tracking (CBT)

(VMware)

- 1. Using VMware vStorage API for Data Protection (VADP) to get list of changed blocks since last job run; supported on VMs with hardware v7+
- 2. If not able to be used (VM with earlier h/w ver or CBT disabled on ESXi), Veeam uses a mechanism to track *unchanged* blocks via checksums

(Hyper-V)

- 3. Used for Backup, Replication, Entire VM Restore operations
- 4. For Win2012R2 Hyper-V and earlier, Veeam uses proprietary CBT mechanism
 - a) <u>File system filter drive installed on every Hyper-V Host when added as</u> <u>managed server</u>, then only invoked/activated when a job with CBT enabled addresses that Host
 - b) Changed block info is registered in .ctp files for <u>each VM disk</u>, stored in C:\ProgramData\Veeam\CtpStore folder, with a subfolder for each VM
 - c) A notes.txt is created for each VM containing info such as VM name, ID, etc
 - d) All Hyper-V Hosts in a Cluster (CSV) need to be on/online for CBT to work!
- 5. Win2016 Hyper-V = Resilient Changed Tracking (RCT)
 - a) Native Microsoft CBT mechanism
 - b) Requirements:
 - 1) All Hyper-V Hosts must run or be upgraded to Win2016
 - 2) VMs must be on configuration version 8
 - 3) Process:
 - 1) A checkpoint is created for each VM

- 2) At end of VM processing, the checkpoint is converted to a reference point = point-in-time representation of VM disk state
- 3) When an incremental is run, a new checkpoint is created & is compared to the previous reference point
- 4) VB&R only copies only changes between previous reference point & new checkpoint
- <u>3 bitmaps used to guarantee persistent CBT data</u>: in-memory bitmap; RCT file (< 6MB in size); MRT file

6. To reset CBT, use PoSH cmdlet > Reset-HvVmChangeTracking NOTE: CBT is reset when a product upgrade is performed

- 4.2 Data Size Optimization
 - a. Compression
 - 1. Decreases backup data size but increases time to run backup job
 - 2. Levels (Settings)
 - a) None best when using storage with hardware compression/dedup
 - b) Dedup-friendly low CPU; use to decrease Proxy load
 - c) Optimal (default) best ratio between backup size & duration of backup
 - d) High additonal 10% ratio over Optimal but at cost of 10x higher CPU
 - e) Extreme for smallest backup size; use Proxy with at least 6 cores
 - 3. New compression setting changes are applied after next job run
 - b. Deduplication
 - 1. Identical data blocks or blocks of free space are eliminated from backups
 - 2. Levels (Settings):
 - a) None for storage with compression & deduplication
 - b) Local Target (16TB) for jobs that produce 16TB .vbk files; 4MB block size
 - c) Local Target (default) for backup to DAS, SAN, local; 1MB block size
 - d) LAN Target for NAS & onsite backup; **512KB block size**
 - e) WAN Target for offsite backup; 256KB block size
 - 3. New dedup settings change are applied after new active full created
 - 4. Upgraded VB&R "Local Target (legacy 8MB)"; to change, switch to smaller block size option & create new active full
 - c. Zero Out Dirty Blocks
 - a) Dirty blocks deleted file blocks; blocks marked as deleted on VM guest OS
 1) VB&R can only exclude deleted file blocks on NTFS file systems
 - b) Enabled by default; can configure in Backup/Replication job settings: Storage
 > Advanced button > Maintenance tab, 'Exclude deleted blocks...)'
 - c) Reduces backup file size on disk & increases backup/replica performance
 - d) Enabling/disabling settings take affect at next job run
 - d. Data Encryption
 - 1. Can be used on the following jobs:

- a) Backup
- b) Backup Copy
- c) Backup to Tape
- d) File to Tape
- e) VeeamZIP
- f) Network traffic
- 2. Algorithms used:
 - a) AES-256 for Backup and Backup to Tape
 - b) PKCS#5 v2 for key generated with a password
 - c) Windows Crypto API (FIPS 140) Windows Repositories
 - d) OpenSSL encryption library Linux Repositories
- 3. Process (Backup):
 - a) Enable encryption for the job & provide a password and pwd hint, which are *saved in job settings*
 - b) Veeam generates a user key based on password
 - c) During data encryption, Veeam saves hint to encrypt file
 - d) During decryption, Veeam displays hint needed for the password
 - e) Once password provided, a user key is derived & used to unlock storage key for the encrypted file
 - f) If password is lost or forgot, data can be restored by issuing a request to Veeam Enterprise Manager
- e. Transaction Consistency
 - Quiescing (freezing) VM guest OS to bring file system & app data to consistent state for backup; non-quiescence = "crash-consistent" backup

(VMware)

- 2. <u>Application-Aware Processing (AAIP)</u> utilizes Windows VSS framework
 - a) Limitation VSS freeze cannot take longer than 60secs, 20secs for Exchange; if it does, a VSS timeout occurs & Veeam fails to create a transaction consistent VM backup
 - b) *MS VSS Persistent snapshots* used for the above-mentioned VSS timeout issue, common with high transaction apps like Exchange
 - 1) **THREE REQUIREMENTS**: support only for Exchange 2010/2013/2016; VM cannot be a DC; Exchange DBs/logs cannot be on a system disk
 - 2) Veeam triggers MS VSS to prepare Exchange for backup
 - 3) MS VSS Writer attempts to quiesce Exchange
 - 4) Control passed to native Veeam VSS writer to freeze guest for necessary time
 - 5) Control passed from MS VSS Provider & a persistent snapshot created for non-system disks
 - 6) Backup is performed
 - 7) Veeam triggers MS VSS to remove persistant snapshot, but it remains inside the VM backup

- 8) During restore Veeam recovers data from backup & reverts disks to the persistent snaphot inside the backup resulting in consistent state
- 3. VMware Tools quiesence
 - a) Doesn't support log truncation for Exchange, SQL, or AD apps
- 4. Snapshot Hunter
 - a) Veeam technology used to detect & remove orphaned ("phantom") snapshots remaining after a Backup or Replication job; for VMware ONLY
 - b) Runs in Backup, Backup from Storage Snap, vCD Backup, Replication, Replication from Storage Snap, & VeeamZIP jobs
- 5. Guest-Interaction Proxy (GIP)
 - a) Runtime process <u>deployed</u> to a Windows VM for a Backup or Replication job <u>when AAIP</u>, <u>Guest File System Indexing</u>, or <u>Transaction Log Processing</u> options are <u>enabled</u>
 - b) Requirements:
 - 1) Enterprise or Enterprise+ feature
 - 2) Can only deploy to a Windows VM
 - 3) For other guest OS's or Veeam Standard, the VB&R server is used
 - c) Proxy selection
 - 1) Any Windows VM added to Veeam as managed servers
 - 2) Selected manually or automatically in Backup or Replication job wizard (**Priority Selection Rules:**)
 - 3) Machine in same network as protected VM & not a Backup Server
 - 4) Machine in same network as protected VM & performs as Backup Server
 - 5) Machine in other network & not a Backup Server
 - 6) Machine in other network & performs as Backup Server
 - 7) Several machines of equal priority detected > uses one with less load
 - 8) If GIP fails, Backup Server fills role

(Hyper-V)

- For transactionally consistent backups, Hyper-V uses Hyper-V VSS writer to coordinate with Hyper-V Integration Service inside VMs (aka "<u>Hyper-V Online</u> <u>Backup</u>")
- One of 3 quiesce methods are used <u>online backup</u>, <u>crash-consistent backup</u>, <u>offline backup</u> (last resort)

(Both Hypervisors)

- 8. Pre-Freeze/Post-Thaw Scripts
 - a) Used when apps don't support VSS
 - b) Create and place script on network; VB&R uploads to guest OS before & after VM snapshot
 - c) For Windows, Veeam uploads via network or VIX; for Linux, Veeam uses SSH
- 9. Transaction Log Truncation
 - a) Do Not Truncate VB&R doesn't truncate; can use transaction logs to restore VM to any point in time between backups if using 3rd party backup tool to maintain consistency of DB state

- b) Truncate Logs Upon Successful Backup Veeam truncates logs after successful backup; can only recover a DB at time when the VM was backed up (not any point in time); for non-SQL VMs
- c) Backup Transaction Logs (SQL/Oracle) VB&R backs up VM & Logs to be able to restore VM (DB) to point in time between backups
 - 1) NOTE: <u>SQL</u> Full or Bulk-Logging recovery model enabled; <u>Oracle</u> ARCHIVELOG enabled
- f. Scheduling
 - 1. Automatic
 - a) Performing a job on a regular basis via set schedule; monitored by Backup Service
 - b) Jobs can be run "continuously" or otherwise as low as 1min for near-CDP
 - c) Periodic jobs have priority over regular jobs (i.e. monthly over a daily or weekly)
 - 2. Automatic Retry
 - a) If 1 job session failed & 1 or more VMs not processed
 - b) Default is set to retry 3 times
 - c) No auto retry if: job started manually, job is successful, or job warnings
 - 3. Backup Window
 - a) Used to prevent job overlap or to prevent overload during biz hours; if the job exceeds the window, the job will automatically terminate
 - 4. Stop Job Session
 - a) Stop (i.e. "Immediate") stops session before restore points are created for current processing VMs; already processed VMs have restore points
 - b) Stop After Current VM (i.e "Gracefully") stops after creating restore points for currenlty processing VMs; already processed VMs have restore points
- 4.3 Creating Restore Points With VeeamZIP & Quick Backup
 - a. VeeamZIP
 - 1. Creates a full backup of selected VM(s) and acts an independent restore point
 - Can restore to a Repository, local disk, or network share; shown in Veeam Console under Backups > Disk (VeeamZIP)
 - 3. VB&R Free VeeamZIP offers encryption, retention (see below), compression (all options), & guest OS quiesce (VMware Tools/Native Hyper-V mechanisms)

VeeamZIP 1 VM (11.9 GB)	x			
Destination:	Show VMs			
O Backup repository:				
Default Backup Repository (Created by Veeam Backup)				
12.9 GB free of 79.6 GB				
Ocal or shared folder:				
\\fs1\backups	Browse			
Credentials:	Add			
Manage accounts				
Delete this backup automatically: Never				
Enable backup file encryption				
Password:				
✓ Add				
Manage passwords				
Compression level:				
Optimal (recommended)				
Optimal compression provides for best compression to performance ratio, and lowest backup proxy CPU usage.				
Guest processing:				
Disable guest quiescence (performs crash consistent backup)				
Less << OK	Cancel			

(Retention ["Delete backup"] options)

Never	4
Never	
Tonight	
Tomorrow night	
In 1 week	
In 2 weeks	
In 1 month	
In 3 months	
In 6 months	
In 1 year	

4. NOTE: For Veeam FREE, only 1 VM can be backed up at a time

b. Quick Backup

- 1. On-demand incremental backup for both Incremental & Reverse Increm VMs
- 2. Quick Backup uses an already-configured Backup Job; if job is not found for VM(s), the task is terminated; also, vCD VMs not supported
- 3. If VM(s) part of several Backup jobs, job with most recent restore point is used

- 4. A Quick Backup restore point is *partial* & is 'grouped' with regular backup restore point created after this partial
 - a) The Quick Backup restore point gets deleted when the retention for the regular restore point that follows it is reached

4.3 – Backup Copy

- a. Backup Copy Job
 - 1. Automated job-driven process that copies VMs from existing backup resources
 - a) Since data is taken from an existing Backup, Backup Copy doesn't affect virtual infrastructure resources, require snapshotting, or place load on VMs
 - b) Creates a chain of restore points using Forever Forward Incremental
 - c) Initial run data is copied using all files in source/orig Backup chain to create a current .vbk, unless the source uses Reverse method, then the latest .vbk is copied
 - d) Job can be for 1 or many VMs, part of 1 Backup or many Backup jobs
 - e) Can specify VM backup order, and Copy job copies all VMs in parallel starting with the 1st VM in the list
 - 1) VMs are processed sequentially if data transferred via WAN accelerator
 - 2) If parallel processing for Copy jobs needs disabled for some reason (enabled by default), a registry key change can be done
 - f) Restore points aren't copied if source & target Repositories have different block sizes (error: **Restore is located in backup file with different block size**)
 - 2. GFS Retention
 - a) "Grandfather-Father-Son" data retention tiered retention scheme that allows keeping data for longer periods (up to a year)
 - b) Regular backup according to sync interval (FFwd Backup chain)
 - c) Weekly full backup
 - d) Monthly full backup
 - e) Quarterly full backup
 - f) Yearly full backup
 - 3. Maintenance Settings (Copy job wizard > Target > Advanced)
 - a) Health check of most recent restore point in backup chain (default = last Sat)
 - Remove deleted VMs after "N" days (default = 30 days); doesn't apply to G-F-S chain, only Regular backups
 - c) Periodically compact & defragment **.vbk** (default = last Sun); G-F-S cannot be enabled
 - d) Compact of Full Backup
 - Veeam creates a new .vbk file & copies all data blocks from the original full, resulting in defragmented & descreased file size, increasing reads/writes made to the new file (default = last Sat)

- 4. Active Full Backup Copies
 - a) Built-in feature used when needing to change job settings requiring a new Active Full for changes to take effect, like enabling Encryption or changing encryption pwd
 - b) Applies Forward Incremental backup method; best used with Dedup Devices
- 4.4 Replication
 - a. Exact copy of a production VM, in native format, on a spare Host, & maintains this copy in sync with the original to fail over to in event the primary VM goes down
 - b. First run is full VM image; subsequent runs are incremental snapshot restore points
 - c. Replication path can be **direct**: source Backup Proxy to a target Host; or via 2 WAN Accelerators
 - d. To optimize WAN data transfer, you can implement inline dedup, compression, & network throttling
 - e. Has best RTO because replica is in ready to power on state; used for tier 1 apps
 - f. "Data pipe" all VB&R components used in Replication data transfer
 - g. Besides full VM images and incremental snapshots (restore points), Veeam keeps replica metadata (**.vbm**) files that stores replica digests to quickly detect changed data blocks between replica states
 - h. Reducing Transferred Data
 - 1. Replica from Backup source data is from a Backup and replica state is from time backup was taken; reduces workload on VM & prod environment
 - 2. Replica Seeding a backup file placed at remote site, containing latest state of last backup run; when Replica job runs, only changes are transferred
 - 3. Replica Mapping VM already existing at remote site, containing latest state of last backup run; when Replica job runs, only changes are transferred
 - i. Resume on Disconnect
 - 1. Resume on Network Disconnect if network connection is lost
 - 2. Resume on WAN Disconnect if connection to any WAN Accelerator is lost
 - 3. For Backup, Replication, Backup Copy, Full VM Restore, & Cloud Connect-related tasks, but NOT Tape jobs
- 4.5 Creating VM/File Copy Jobs
 - a. VM Copy helpful if wanting to move a DC or mirror prod environment to a lab for testing
 - 1. Ran on-demand or via scheduling in the VB&R "Infrastructure" view
 - b. File Copy same as VM Copy but for individual files or folders; compression can be used for this to improve performance of the copy process

SECTION 5 - ENTIRE VM RECOVERY

- 5.1 Recovery From a Backup
 - a. Data Recovery Methods
 - 1. Instant VM Recovery (IR)
 - (VMware)
 - a) vPower NFS technology is used to mount a VM to a ESXi Host directly from compressed/dedup'd backup file
 - b) VM image remains in read-only state & changes are written to redo logs
 - 1) To improve performance, you can select to redirect changes to be written to a Datastore (DS) where a snapshot is created, along with metadata files placed in a Veeam IR directory
 - c) <u>Finalize</u> (IR) Recovery options:
 - 1) Use storage vMotion can only be used if changes aren't directed to go to a Datastore; must have vSphere Enterprise license or higher
 - 2) Use cross-Host vMotion requires using vSphere Web Client & VMotion
 - 3) Replication or VM Copy downtime operaton requiring maint. window
 - Quick Migration (VMware ONLY) restoring the VM directly from the backup file

(Hyper-V)

- d) Veeam reads VM config from backup & creates a dummy VM
- e) Protective snapshot taken
- f) Veeam data mover service deployed on backup Repository & target Host to mount the VM disks from the backup file
- g) Veeam proprietary driver started on target Host & redirects request to the file system of the recovered VM
- h) To finalize VM recovery, migrate the VM to production storage
- i) **NOTE:** CBT should be enabled on target Host or driver required for Instant VM Recovery will be disabled
- 2. Full VM Recovery
 - a) Veeam extracts VM data from the Repository (backup file), places on selected storage, registers VM on ESXi/Hyper-V Host, and powers it on
 - b) When restoring to original location, the primary VM is powered off & deleted
 - c) Quick Rollback incremental restore
 - 1) Used by default for VMware

i. Leverages VMware CBT to restore only changed blocks to revert a VM/disk to an earier point in time

ii. Best used when VM issue is at guest OS level, not VM-level

- 2) Limitations
 - i. VM must have CBT enabled
 - ii. VM must be restored to original location
 - iii. VM CBT is reset after restore causing next backup to run 'full'

iv. Direct SAN mode can't be used

- 3. VM File Recovery
 - a) Restoration of such files as .vmdk, .vmx, .vhd, .vhdx, .xml, .log, etc
 - b) Good alternative to Full VM Restore
 - c) Veeam Data Mover ("transport") Service on Repository & Proxy retrieve data (file) from the backup file & sends it to the original or new location
- 4. Restore to MS Azure
 - a) Can restore:
 - 1) Backups of Windows & Linux of vSphere or vCloud Director VMs
 - 2) Windows machines from Endpoint Backup taken at volume level
 - 3) Linux machines from Veeam Agent for Linux taken at volume level
 - b) Windows restore limitations:
 - 1) Must be Windows 2K8/Vista or later; various Linux OS machines
 - 2) Disk size <= 1TB
 - 3) If system disk uses GPT, can't have > 4 partitions; is converted to MBR
 - 4) Restoring to Germany/China regions not supported
 - 5) Azure Hybrid Use Benefit program not supported

NOTE: Verify NTP on Backup Server is accurate or unable to add Azure account to VB&R

- c) Process:
 - 1) VB&R powers on Azure Proxy
 - 2) Converts disks to VHD format & uploads to Azure
 - 3) Mounts loaded disks to Backup Server
 - 4) Prepares disk for VM restore, enabling RDP, configuring f/w rules, prepares MS Azure Agent, etc
 - 5) Disk is unmounted from Backup Server
 - 6) Azure Proxy powered off
 - 7) Registers Azure VM with prepared machine disks, powered on, & Azure Agent installed
- d) Linux restores
 - 1) Helper (Linux) appliance used to mount disks of backed up machine to prepare for restore

i. Helper appliance is persistant > stays powered off in Azure

- 2) Process same as in Windows except prepared disks are mounted to helper appliance instead of Backup Server
- 5.2 Working With Backup & Replication Utilities
 - a. Extract Utility
 - 1. Independent of VB&R, tool to recover FULL BACKUP FILES (i.e. **.vbk**) of VMs if VB&R is unavailable; GUI or CLI
 - 2. Can be used on Windows or Linux

- 3. Utility files are in VB&R install folder (%ProgramFiles%\Veeam\Backup and Replication\Backup):
 - a) Veeam.Backup.Extractor.exe GUI tool for use on Windows
 - b) Extract.exe CLI tool for use on Windows
 - c) Extract CLI tool for use on Linux
- 5.3 Recovery From Replica
 - a. Failover
 - 1. Replica VM takes over role of original VM if it has failed, or for testing purposes
 - 2. An intermediate/temporary step that <u>needs to be finalized</u>:
 - a) **Permanent Failover** switches from orig VM to replica VM; changes are sent to replica; new replica is the original VM
 - b) Undo Failover switches back to orig VM; changes are discarded
 - c) **Failback** switch back to original VM after problem in prod resolved; changes transferred back to original VM
 - 1) Commit Failback (see 3a below)
 - 2) Undo Failback (see 3b below)
 - b. Failback
 - 1. Switching back to the original VM after problem with original VM resolved, or testing complete
 - 2. 3 options:
 - a) Failback to VM in original location; transfers only changes
 - b) Failback to VM restored from a backup in a new location; transfers changes
 - c) Failback to an entirely new location by transferring all replicas to selected destination
 - 3. Temporary stage that needs finalized
 - a) Commit Failback finalizing recovery back to original (prod) VM
 - b) Undo Failback prod VM isn't working as expected; return replica to Failover
 - c. Failover Plan
 - 1. Failover process for group of VMs (i.e. interdependent [app] group)
 - 2. Set order VMs are to be processed & delay time if needed; started manually
 - 3. A temporary step that needs finalized, as mentioned in 'Failover' above
 - 4. Commit Failback (Failover) can only be done individually, not on group; Undo Failover can be done on whole group
 - d. Planned Failover
 - 1. Used for testing, maintenance, & software upgrades/patching
 - 2. Process:
 - a) Replication job triggered to do incremental backup & copy changes to replica
 - b) Original/Primary VM powered off
 - c) Another incremental backup is run to catch any last second changes
 - d) VM is failed over to replica

NOTE: Because this task takes primary VM functions, do not select a restore pt

e) Finalizing needs done as other failovers discussed above (perm, undo, failback)

SECTION 6 – OBJECTS RECOVERY

- 6.1 Application Item Recovery
 - a. Explorer Utilities for Recovery:
 - 1. Veeam Explorer Exchange
 - a) Extract Exchange DB to restore mailboxes, folders (public), contacts, tasks
 - b) Available for ALL VB&R Editions
 - c) Requires full access to the DB
 - d) **NOTE:** Supported for Exchange 2010 SP1 or later only due to Explorer for Exchange leveraging UploadItems operation which is only supported in MS Exchange Web Services starting with 2010 SP1+
 - e) Supports Litigation (even empty containers) & In-Place Hold (non-empty containers)
 - f) Restore options:
 - 1) Restore mailbox folders & items requires Ent/Ent+
 - 2) Export mailbox folders & items to .pst
 - 3) Save mailbox items as .msg docs
 - 4) Send mailbox items as email attachments
 - 5) Recover to online Archive
 - g) Must specify path to ese.dll for access to the Exchange DB (.edb)
 - Exchange 2013: %ProgramFiles%\Microsoft\Exchange Server\V15\Bin (or v14 for 2010)
 - 2) CD:X:\Setup\ServerRoles\Common\ese.dll
 - 2. Veeam Explorer Sharepoint
 - a) Extract Sharepoint .mdb to recover library docs, images, webpages, etc
 - b) Available for ALL VB&R Editions
 - c) For SP DBs larger than 10GB, full vers of SQL (not Express) must be used to mount the DB
 - d) Supported for SP 2010/2013/2016, all Editions (Foundation, Std, Ent)
 - e) MS SQL server is required as a staging location for recovery of SP content
 - f) To work with remote BLOB stores (RBS), make sure the BLOB store is virtualized or running on machine with Staging SQL & Veeam Explorer
 - g) Enable FILESTSREAM at DB level & install RBS Client Library on staging SQL Server
 - 3. Veeam Explorer Active Directory
 - a) Available for ALL VB&R Editions
 - b) Extract MS AD .dit DB file to recover AD objects & containers
 - c) Requires full access to the DB; for lesser access, use U-AIR

- d) Use Compare With Original menu cmd to see changes since last AD backup
- 4. Veeam Explorer SQL
 - a) Restore options:
 - 1) Browse SQL Server instances & DBs
 - 2) Export DBs to a local folder or network drive
 - 3) Restore DB to original location or different server
 - 4) Restore SQL tables
 - b) SQL Log backups are only available in Ent/Ent+
 - 1) Supported for MS SQL 2005 SP4+, all Editions

NOTE: Always-On Availability Groups only supported for SQL 2012+

- 2) Full/Bulk-Logged Recovery Model must be enabled
- 3) Logs are backed up as .VLB files, along with corresponding .vbk/.vib/.vrb
- 4) Log backup job MUST be scheduled or won't be backed up
- c) For restore, Veeam installs **Veeam SQL Restore Service** to the target/staging SQL server for restore activities
 - 1) Operates under LOCAL SYSTEM account
 - 2) Activities logged to Veeam. SQL. Service. <timestamp>.log file
 - 3) Communication with Veeam Explorer via RPC, ports 1025-1034; can change ports in config.xml if needed
- 5. Veeam Explorer Oracle
 - a) Available only with Ent and Ent+
 - b) Restore options:
 - 1) Browse system hierarchy
 - 2) Restore DB to original or different server to 1. current point-in-time, select point-in-time, or point-in-time state before selected transaction
 - c) Process:
 - 1) Veeam Console used to mount Oracle VM file
 - Veeam Mount Server is used & target Oracle server used for staging &
 C:\VeeamFLR folder created
 - 3) Veeam Explorer used to browse the hierarcy
 - d) SYSDBA rights needed for guest processing Oracle Win VM / root for Linux
 - e) Staging server must: have same or higher DB version; if ASM enabled in backup, ASM enabled on staging server; Oracle Express not supported
 - f) Restoring DB to point in time backup Oracle with ARCHIVELOG mode enabled & log truncation disabled
- 6.2 Universal Application-Item Recovery (U-AIR)
 - a. For recovery of application items from within a Virtual Lab **using Veeam vPower technology** directly from compressed/dedup'd backup files
 - b. U-AIR access to the VM is granted through a proxy appliance
 - c. Universal, standalone components, wizard used to start the apps & all components in the Virtual Lab and use native mgmt tools to recover items

- d. App Group, Virtual Lab, & SureBackup job items must be configured to use U-AIR
- 6.3 Guest OS File Recovery
 - a. Guest OS File-Level Recovery (Instant File-Level Recovery [IFLR]) ability to recover a file from a backup or replica directly from an image without having to extract it to a local drive
 - 1. Windows File-Level Recovery (FAT, NTFS, ReFS)
 - a) VM disk(s) mounted to the Backup Server or machine used to recover file that has the VB&R Console installed, in a C: \VeeamFLR\<vmname> folder
 - b) Process
 - 1) VM disks are mounted to VB&R server or machine where Veeam Console is installed/used, using a **Veeam Disk Driver** (VDK) to access the content, *emulating* VMDK disk presence on the Console or VB&R machine
 - 2) Veeam Backup Browser is launched displaying mounted VM disks to browse guest files
 - A 2nd Mount Point is created to route VM data optimally if restoring to original location, using the Mount Server; for 'new location' restore, the Mount Point is on the Backup Server
 - 4) When finished, browser is closed or by timeout, mount points are removed

NOTE: For ReFS support, VB&R needs to be installed on Win2012+

- 2. Multi-OS File-Level Recovery mostly for non-Windows systems
 - a) Linux ext2/3/4, ReiserFS, JFS, XFS, Btrfs
 - b) BSD UFS, UFS2
 - c) MAC HFS, HFS2; volumes up to 2TB
 - d) Solaris UFS, ZFS v0.6.3 (except Oracle)
 - e) Novell OES; Netware NOT supported
 - f) Uses a Linux Helper appliance VM: ZFSonLinux v0.6.3 appliance (50MB disk/1GB RAM)
 - g) Supports: Basic disks, Linux LVM, Windows LDM, & ZFS pools
 - h) Process:
 - 1) Veeam creates Linux helper appliance
 - 2) VM disk is mounted to helper appliance
 - 3) Veeam Backup Browser is launched to browse guest files; FTP can be enabled for end users to restore files themselves
 - 4) When Browser is closed or by timeout, content is unmounted, & appliance unregistered from ESXi
 - 5) If files are recovered directly to Linux, files are recovered with correct permissions
- 3. File-Level Recovery for Any File System
 - a) Done by using Instant VM Recovery to publish the VM to a Host
 - b) Mount disks to any VM that can read the file system

c) Restore guest files/folders using native mgmt tools; e.g. Portlock Explorer

SECTION 7 – VERIFICATION

7.1 – SureBackup Recovery Verification

- a. Ability to "live" test a VM & ensure recoverability in an isolated/test environment
- b. Enterprise and Enterprise+ feature (for VM verification in Veeam Std, use Instant VM Recovery)
 - 1. Leverages Instant VM Recovery to publish a VM in an isolated environment & started directly from the backup file on Repository
 - 2. Tests are ran against the VM (see 'd' below) & changes written to redo logs
 - 3. When complete, the VM is unpublished, redo logs deleted, & a report is run on the VM state & sent to the Backup Admin
- c. vPower NFS Service Windows service that runs on the Repository server (recommended; or any Windows server) to enable it to act as an NFS server
 - 1. Allows Veeam to mount a dedup'd/compressed VMDK to an ESXi Host for direct access to VM images
 - 2. vPower used for:
 - a) SureBackup
 - b) Instant VM Recovery
 - c) On-Demand Sandbox
 - d) Multi-OS File-Level Recovery
 - e) Universal Application-Item Recovery (U-AIR)
 - 3. ESXi Hosts that connect to vPower NFS server must have a VMkernel interface
- d. Recovery Verification Tests tests SKIPPED if VMware Tools/Integ Svcs not installed
 - 1. Heartbeat test heartbeat signal from VMware Tools/Hyper-V Integration Svcs
 - 2. Ping test VB&R tests if VM in virtual lab responds to ping requests
 - 3. Application test VB&R waits for app(s) inside VM to start & runs a script against it/them ("**Probe Port Script**" for apps or "**SQL Checker Script**" for DB instances)
- e. Backup File Validation (Verification)
 - 1. VB&R creates a *checksum* for every data block of a backup file
 - 2. During a validation check, VB&R descompresses the backup file, recalculates checksums for the data blocks, then compares them with the initial checksums
- f. Application Group
 - 1. Creating "surroundings" or dependencies to verify a VM; i.e. DC, DNS, DHCP VMs
 - 2. VMs can be added from: Backups, Replicas, Storage Snapshots or combo of eacha) Can't add a VM twice from different media (e.g. from a Backup & Replica)
 - 3. VMs must be of same platform i.e. all from vSphere or all from Hyper-V
 - 4. Can be configured to 'keep running' for On-Demand Sandbox
 - 5. When setting up the App Group, specify the role of each VM, their boot priority, and tests to perform against them before verifying a VM:

	Verification Options
Role	Startup Options Test Scripts
Selec	t roles:
Role	3
	DNS Server
	Jomain Controller
	àlobal Catalog
	fail Server
	QL Server
	Veb Server
Start base reco	up options and test scripts will be automatically configured id on the roles you have selected. Review and adjust the mmended configuration on the corresponding tabs.
	OK Cancel

- g. Virtual Lab
 - 1. Isolated environment in which Veeam tests & verifies VMs
 - 2. Not solely used for SureBackup, but also for U-AIR & On-Demand Sandbox tasks
 - a) On-Demand Sandbox = an isolated environment used for patch testing or troubleshooting
 - 3. Proxy Appliance a Linux-based auxilliary VM enabling communication between the Virtual Lab and the prod environment; acts as a gateway between the 2
 - a) Optional component; if this appliance is not used, automatic tests are not performed and manual testing via VM Console will need to be done
 - 4. IP Masquerading VM IP in Virtual Lab "masquerades" (or, 'resembles') IP of VM in prod environment (prod IP = 172.16.1.13; VL Masq IP = 172.18.1.13); i.e. it's an entry point for a VM in the VL from the prod environment
 - a) Update routing table either on Backup Server or client PC accessing Lab VM
 - 5. Static IP Mapping using a reserved IP(s) in Prod network for Virtual Lab VM(s)
 - 6. Virtual Lab Configuration
 - a) Basic single-host VL to be used if all testing VMs (app group, verifying VM, Backup Server) are on same network; <u>uses vSphere Standard Switch (vSS)</u>
 - b) Advanced single-host VL used when prod environment has multiple networks; <u>uses vSS</u>
 - c) Advanced multi-host VL when VMs to verify reside on different Hosts (used for SureReplica testing/verification); and <u>uses a vDS</u>; **VMware ONLY**
- h. SureBackup Job
 - Aggregation of all VM verification items (Application Group, Virtual Lab) to verify VMs from Backup

- 2. Linked jobs option ability to start & test up to 3 VMs simultaneously
- 3. Surebackup processing review steps in Handbook
- Stabilization algorithm time to wait for VM to boot to begin testing; methods: (VMware)
 - a) Stabilization by IP with a vNIC, via VMware Tools
 - b) Stabilization by heartbeat via VMware Tools (green or yellow) if no vNIC
 - c) Stabilization by maximum allowed boot time if no vNIC or VMware Tools (Hyper-V)
 - d) Stabilization by IP if vNIC, via Hyper-V Integration Services
 - e) Stabilization by heartbeat via Hyper-V Integration Services if no vNIC
 - f) Stabilization by hybrid IP/heartbeat VB&R uses both IP/heartbeat
 - g) Stabilization by maximum allowed boot time same as above
- i. Manual Recovery Verification
 - 1. Can be done with all PAID VB&R Editions
 - a) Boot test using Instant VM Recovery, power on a VM but don't connect to prod network
 - b) Application test create an isolated network, use Instant VM Recovery & clear 'connect to network' option
 - c) When VM is started, connect it to isolated network
 - d) Repeat for any dependency VMs
- 7.2 SureReplica Recovery Verification
 - a. Validation of DR (replica) environment similar to SureBackup
 - b. Not available for Hyper-V
 - c. Capabilities SureReplica, U-AIR, On-Demand Sandbox
 - d. Since VM doesn't need published, process is faster
 - e. Only available for 'normal state' VMs, not those in Failover/Failback
 - f. Process:
 - 1. Protective Snapshot triggered
 - 2. VM started in isolated environment
 - 3. Tests performed against VM(s)
 - 4. Delta (snapshot) removed, VM powered off, report sent
 - g. Same configs needed as in SureBackup App Group, Virtual Lab, SureBackup Job
 - h. Same tests ping, heartbeat, app scripts are run for SureReplica
 - i. Does NOT require vPower technology
- 7.3 On-Demand Sandbox
 - a. Isolated environment to start 1+ VM from backup, replica, or storage snapshot for testing patches, troubleshooting, or new software install
 - b. Same config as for SureBackup, but what makes this a 'Sandbox' is enabling the 'Keep the application group running once the job completes' option

c. For all Verification tests (SureBackup, SureReplica, On-Demand Sandbox), a Backup or Replication job has priority, so if SureBackup is running when Backup or Replication begins, virtual lab VMs are powered off & the Surebackup job terminated

SECTION 8 - INTRODUCTION TO AGENTS

8.1 – Why Agents

- a. Solves challenges, enabling to:
 - 1. Reduce cost & complexity ensuring availability for Windows & Linux in the Cloud
 - 2. Achieve availability for physical servers and workstations that can't be virtualized
 - 3. Meet RPOs and reduce risk of data loss for desktops, laptops, & tablets outside the corporate network
- 8.2 Veeam Agent for Windows

a. Features/Edition Comparison

	Free	Workstation	Server
Instant Recovery to Microsoft Hyper-V VM	x	x	x
Direct Restore to Microsoft Azure	x	x	x
Source-side encryption	x	x	x
	Free	Workstation	Server
Endpoint protection for mobile users		x	x
Back up directly to Veeam Cloud Connect		x	x
Remote configuration and management API		x	x
Application-aware processing			x
Transaction log backup for databases			x
Guest file indexing and search		x	x
24.7.365 technical support			

8.3 – Veeam Agent for Linux

a. Features/Edition Comparison

	Free	Workstation	Server
Entire computer, volume-level and file-level image- based backup	x	x	x
Built-in volume snapshot and changed block tracking drivers	x	x	x
File-level, volume-level and bare metal recovery (same or different hardware)	x	x	x
Backup and recovery using console UI or command line	x	X	x
Integration with Veeam Backup & Replication	x	x	x
Support for multiple jobs			x
Pre-freeze/post-thaw snapshot scripts for application processing			x
Guest file indexing, catalog search and restore with Veeam Backup Enterprise Manager			x
24.7.365 technical support		x	x

- 8.4 Veeam Agent Management
 - a. Manage Veeam Agent for Windows in VB&R
 - b. Deploy agent remotely from VB&R
 - c. Store backup files created with Veeam Agent in VB&R Repositories, simple or SOBRs
 - d. Veeam Agent job info:
 - 1. Veeam Agent backup job displayed in VB&R job list
 - 2. Backup files shown in Backups > Disk node
 - 3. Peformed job sessions are shown in History View
 - e. VB&R Admins can:
 - 1. Perform data protection operations > i.e. copy Agent backups to secondary locations, and archive to tape
 - 2. Peform restore operations > files/folders, application items, restore computer disks, restore to MS Azure
 - 3. Perform admin tasks > disable & delete jobs, remove Agent backups, etc.

8.5 – Protection Groups

- a. Creating Protection Groups
 - Launch Protection Group wizard from Inventory > Physical & Cloud Infrastructure, then click 'Add Group' from Ribbon or select Create Protection Group from Working Area

NOTE: If you don't wanna create a Protection Group or have small number of computers to manage, you can add computers directly to a job & the computer will automatically be added to "Manually Added' Protection Group container in Veeam

- b. Protection Group Types
 - 1. Individual computers for static computers; when managing small environment
 - 2. Active Directory can select individual or dynamic containers/OUs

NOTE: A MS Failove Cluster can be added if this option is selected ONLY

- 3. CSV file as in AD, this is dynamic in nature; in local folder or network share
- c. Protection Scope see b. above
- d. Discovery & Deployment Options
 - 1. Select discovery, agent deployment server, and options from the Options window in the Protection Group wizard (see all options below)

New Protection Group							
Options Specify host discovery schedule and automatic backup agent deployment options.							
Name	Discovery						
Turne	Rescan protection group every:						
Type	O Daily at this time: 9:00 PM ▲ Everyday ✓ Days						
Computers	Periodically every: 1 V Hours Schedule						
Options	Deployment Minutes						
Review	Distribution server: Continuously						
Apply	nkc-veeam02.nkcschools.org 🗸 🗸						
	Protected computers will download backup agent redistributable from this server.						
Summary	 Install backup agent automatically (recommended) 						
	Auto-update backup agent						
	Install changed block tracking driver on Windows Server OS						
	Perform reboot automatically if required						
	To be able to manage backup agents automatically, we will need the protected computers to have 'File and Printer Sharing' feature enabled.						
	< Previous Next > Finish Cancel						

- 2. Can do Discovery daily, hourly, minutes, or continuous
- 3. Can do Agent auto-update, as well as other options

NOTE: The CBT option is for Windows only

8.6 – Agent Jobs

- a. Agent jobs fall into two types
 - 1. Backup job used or computers permanently connect to Veeam server

2. Backup policy – used for computers with limited connection to Veeam server **NOTE:** Though you can add computers of a different OS to a given job, Veeam will only backup computers for that given job OS (i.e. only back up Windows machines for computers added to a Windows job; same for Linux)

- b. Agent For Windows Job Modes
 - 1. From Home > Backup Job > Windows
 - 2. Types: Workstation, Server, Failover Cluster

- a) Workstations mode can only be set to be 'Managed by Agent'
- b) Server mode can be 'Managed by Backup Server' or 'Agent'
- c) Failover Cluster mode can only be 'Managed by Backup Server'
- 3. When in 'Managed by Backup Server' mode, mgmt can only be done via Veeam Console
- 4. When in 'Managed by Agent' mode, mgmt options are available in the Veeam Agent control panel on remote machine; this essentially creates a Backup Policy
- c. Agent For Linux Job Modes
 - 1. The same info applies for Linux jobs as shown in Windows job in b. above
- 8.7 Administrative Tasks
 - a. Enabling & Disabling Veeam Agent Backup Jobs same procedure as normal Backup jobs (Home > select job > click Disable button; rt-click job > Disable)
 - b. Deleting Veeam Agent Backup Jobs same procedure as normal Backup jobs
 - c. Viewing Veeam Agent Backup Job Statistics same as normal Backup jobs
 - d. Removing Veeam Agent Backups Home > Disk node > select Agent, Remove from Configuration
 - e. Viewing Veeam Agent Backup Statistics in History view (same as normal Backup jobs)
 - f. Configuring Global Settings network throttling & email

SECTION 9 – ADVANCED DATA PROTECTION

- 9.1 WAN Acceleration
 - a. WAN Acceleration
 - 1. Specifically used for: Replication & Backup Copy jobs
 - 2. Requirements:
 - a) Must be **x64 bit**
 - b) Windows machine, physical/virtual
 - c) At both source & remote sites with at least 8GB RAM
 - d) Proxies & Repositories can be used
 - 3. *VeeamWAN* folder on each Accelerator contains:
 - a) Source VeeamWAN folder has digest data for global dedup
 - b) <u>Target</u> VeeamWAN folder <u>has global cache data</u> (can be pre-populated)

9.2 – Tape Device Support

- a. Overview
 - 1. Archive Backup & Backup Copy data to tape, or Windows or Linux files, and Endpoint Backups using **MTF** (MS Tape Format) to write data to tape

- 2. Archive files from any Windows or Linux server, or NAS devices added to VB&R
- b. Restore from Tape options:
 - 1. Restore VMs Full VM Restore from Tape to Virtual Infrastructure
 - 2. Restore backup files restore files or chains from Tape to disk; restored files are registered in VB&R
 - 3. Restore files/folders restore to orig or new location from Tape preserving ownership & permissions
- c. Components used to backup to tape:
 - 1. Source location source data to send to Tape resides: Windows or Linux Repositories, Backups, Backup Copies
 - Data Path via "source-side Data Mover service" and "target-side Data Mover service"; source = Data Mover on Repository, target = on Backup Server the Tape Device is connected to
 - 3. VB&R Server
 - 4. Tape Device physical or virtual tape library; or stand-alone tape drive
 - Tape Server Windows server running Data Mover Service, between data source & tape device, creating a communication channel & routing traffic to tape devices
 - 6. VB&R DB stores Tape Catalog & Data Catalog
- d. Entities used to manage tapes:
 - 1. Media Pools logical units that distribute free tapes for writing data:
 - a) Free Media Pool contains empty tapes
 - b) Unrecognized Media Pool tapes loaded to a tape device needing further identification
 - c) Imported Media Pool non-empty tapes identified by tape catalog job
 - d) Retired Media Pool tapes that have reached max number of re-writes; or, contain some mechanical breakdown
 - e) Veeam GFS Media Pool data stored by VB&R using GFS backup scheme
 - 2. Media Sets separate sets of tapes with data continuously written to them; used to split tape archives into separate tape groups
 - 3. Backup Sets sets of files written to tape within 1 tape job session
 - 4. Media Vaults logical containers for visualizing data stored offline
 - 5. Data Retention user-defined period to protect data
- e. Virtual Full Backup for Tape Jobs (or *Virtual Synthesized Full Backup*) 'splits' tape sets into shorter series between Fulls using **.vsb** files, which contain pointers to data blocks; good for restores so fewer tapes to load
- f. Tape Protection option for "endless tape retention"
- g. Tape Multistreaming ability to write to many tapes drives simultaneously, useful if there's a lot of tape jobs running at same time; <u>not available for a GFS Media Pool</u>
- h. Tape Job Scheduling
 - 1. Simple backup to Tape
 - a) Select "run job automatically" schedule option, otherwise it's manual

- b) Schedule weekdays or monthly, or "After this job completes" & select Backup the tape job should follow; task will run ONLY if source Backup job is started via a schedule, not manually
- c) "As new backup files appear" periodically check jobs for new backups to archive to tape
- d) Best to select a 'timeout' value to check if Backup is still running; if Backup is running when Tape job scheduled, the Tape job will wait till Backup is done for specified time interval configured; otherwise the Tape job will terminate
 - 1) Not available if 'wait after backup completes' or 'look for new backups to appear' options are enabled
- e) Best to select 'Prevent this job from being interrupted' option while it's running if Backup begins while Tape is running; the Backup job will then wait till Tape job is done before running, & the Tape job won't terminate (because Backup job has priority over Tape)
- 2. GFS
 - a) Click to schedule select days of media set, which **starts at 00:00** (midnight) on the selected day
 - b) Can save config as 'default' to use for new GFS jobs
 - c) Best to select to 'Prevent job from being interrupted' option, as noted above
- i. Tape Job Encryption
 - Hardware level encryption library & driver-level provided by tape vendor

 a) Has higher priority than software
 - 2. Software level encryption Veeam-based
 - a) Can only be used if Hardware Encryption is disabled or not supported
 - b) Must be enabled at Media Pool level
 - c) Supported for Backup to Tape & File to Tape jobs
 - Allows double encryption if source backup file is encrypted from Backup job; then backup file encrypted again for Backup to Tape; as a result TWO passwords are required to decrypt
- j. VM Restore From Tape to Infrastructure
 - 1. Restore directly to infrastructure
 - a) Recommended when restoring 1 or small number of VMs from a backup file
 - b) Slow; processes VMs one by one
 - c) Process:
 - 1) VB&R checks Backup Catalog for tapes housing required backup file; loads & reads tapes 3 times
 - 2) Tapes loaded 1st time
 - 3) Metadata is read & gets cached on tape server (~100MB per 1TB)
 - 4) Using cached data VB&R maps data blocks
 - 5) Tapes loaded 2nd time
 - 6) VB&R restores the VM configuration to original/new location
 - 7) Tapes loaded 3rd time
 - 8) VM disks restored; multiple disks restored in parallel

- 2. Restore through a staging Repository
 - a) VB&R temporarily copies whole restore point to Repository or folder on disk, then starts regular VM restore
 - b) Faster process & recommended when needing to restore many VMs
 - c) Process:
 - 1) Veeam starts 2 jobs > backup restore job; VM restore job, simultaneously
 - 2) Backup restore job checks Backup Catalog to discover tapes needed for restore (housing backup file)
 - 3) Backup restore job reads tapes & copies backup file to Repository/folder
 - 4) When complete, Veeam registers VM temporarily as an imported backup
 - 5) Backup restore job finishes
 - 6) VM restore job receives info about the restored backup & launches a standard VM restore process *Entire VM Restore*
 - 7) VM restore process finishes when VM(s) are successfully restored
 - 8) Veeam deletes backup from staging Repository
- k. Automated Drive Cleaning
 - 1. Prevents overlapping of cleaning tasks & tape jobs, which may cause failure
 - 2. Cleaning operation done at beginning of Backup/File to Tape jobs
 - 3. Cleaning does not exceed 2mins for a drive, 5mins total for all drives
 - 4. Cleaning on tapes located in "Unrecognized" Media Pool; worn-out cleaning tapes moved to "Retired" Media Pool
 - 5. Cannot be enabled on standalone tape drives
 - 6. Cannot be started manually
 - 7. **NOTE:** If enabled, disable drive cleaning on tape library device! Enabling also does not affect Media Set creation
- 9.3 Storage Integration (VMware)
 - I. Overview
 - 1. For VMware environments
 - Backup From Storage Snapshots Ent+ ; take backups or replicas from a storage snaphots; NetApp & Nimble can take backup from secondary storage snapshots
 - Veeam Explorer for Storage Snapshots in ALL VB&R Editions; restore VM data directly from storage snapshots
 - 4. Snapshot Jobs using NetApp & Nimble, use VB&R to create storage snapshots
 - 5. On-Demand Sandbox for Storage Snapshots start VMs in On-Demand Sandbox whose disks are hosted on storage for testing, training, troubleshooting
 - 6. Supported systems:
 - a) Cisco HyperFlex 2+
 - b) **DellEMC** VNX, VNX2, VNXe, Unity
 - c) HPE 3PAR StoreServ 3.1.2+; HPE StoreVirtual/VSA (ISCSI only), Lefthand 9.5-12.6
 - d) NetApp FAS, FlexArray, Edge VSA, IBM N Series; ONTAP 8.1-9.2

e) Nimble Stroage AF-Series/CS-Series

					_	_		
Functionality/Storage type	Dell EMC VNX(e)/ Unity	HPE 3PAR StoreServ	HPE StoreVirtual	NetApp	Nimble	Cisco HyperFlex		
Backup from Storage Snapshots								
Backup from primary storage arrays	✓	1	✓	1	1	1		
Backup from secondary storage arrays	x	x	x	1	1	x		
Veeam Explorer from Storage Snapshots								
Restore from primary storage arrays	✓	✓	✓	1	1	x		
Restore from secondary storage arrays	✓	✓	✓	1	1	x		
Snapshot Jobs								
Snapshot-only job	x	x	x	1	1	x		
Snapshot in secondary destination job	x	x	x	1	1	x		
Other Operations								
Storage rescan	*	1	1	1	1	√ (infrastructure only)		
Snapshot creation and deletion (manual)	1	1	1	1	1	×		

m. DellEMC Storage Systems

- 1. VNX
 - a) VB&R suppors LUNs residing on Storage Pools
 - b) VNX snap technology is used, so verify licensing; SnapView is NOT supported
 - c) Read-only checkpoint can have only 1 snap
 - d) Writable snaps are not detected by storage rescan operation & not displayed
- 2. VNXe
 - a) VNXe Gen 2 (3.x.x) supported (not Gen 1)
 - b) Cannot export more than 1 snapshot
 - c) VB&R Priority Levels > restore, backup, rescan (highest to lowest)

(Over NFS)

- d) VMs with vSphere snaps are skipped from backup or replication
- e) Backup from storage snap not used on Windows VMs with VMware Tools installed & 'VMware Tools Quiescience' enabled in Backup job
- n. HPE Storage Systems
 - 1. Volume Snapshots, SmartClone, & VirtualCopies created per-Volume
 - 2. 3PAR Virtual Copy must be licensed or unable to perform backup or restore from storage snapshot
- o. NetApp Storage Systems
 - 1. Uses:
 - a) Traditional LUN Cloning
 - b) FlexClone
 - c) SnapRestore
 - d) NFS Share Copying

- 2. If SnapMirror/SnapVault used (secondary array), backup from secondary storage snap technology can be used
 - a) SnapMirror/Vault configured
 - b) License installed for storage export
 - c) No VMware snaps for VMs using NFS
 - d) Ent+ license
 - e) Properly configured VB&R Proxy with access to Backup Server & 2nd Array
- p. Nimble Storage Systems
 - 1. Schedule Nimble snapshot creation jobs
 - 2. Restore from Nimble snapshots/replications (Entire VM, Guest Files, App Items)
 - 3. Backup from Nimble snapshots or replicated copies
- 9.4 Microsoft Hyper-V Off-Host Backup Proxy
 - a. 'Data Mover'; performs main data handling to remote Host, taking job processing off source (VM) Host
 - b. A Windows server already added to managed servers list
 - c. Requirements review all in Handbook
- 9.5 Support for Deduplicating Storage Systems
 - a. Exagrid
 - 1. ExaGridWorks like using a Linux-based Repository
 - 2. To communicate with the dedup appliance, VB&R deploys the Data Mover (*transport*) Service on it, which in turn communicates with the source Data Mover Service on the Proxy to enable efficient data transfer via LAN or WAN
 - 3. If Per-VM disabled: max concurrent task must be 1; if Per-VM enabled: max concurrent tasks can be set to 10 or less; 10 total overall per Exagrid Server (i.e. if multiple Repositories exist per Exagrid, do not config 10 concurrent tasks per Repository.. the total tasks among ALL Repos's for the Exagrid should not exceed 10 or performance will be affected)
 - b. HPE StoreOnce
 - Uses source or target-side dedup, depending on config/licensing

 a) Source-side provides better performance, less network load, & disk savings
 - 2. Veeam uses source-side dedup leveraging StoreOnce Catalyst technology & 2 StoreOnce components; Catalyst store configured in Low-Bandwidth mode
 - Veeam usees target-side dedup by utilizing StoreOnce as a shared folder, & uses
 2 Data Mover Services; Catalyst store configured in High-Bandwidth mode
 - Gateway Server bridges StoreOnce appliance & Veeam Backup Server; must be x64bit Windows machine & have connection to StoreOnce & Backup Server

- 5. Limitations (integration mode only):
 - a) Backup files are locked by a job/task; starting several at same time, VB&R will perform higher priority task and skip/terminate lower priority tasks; Priority: restore, backup, backup copy
 - b) When creating backup job, VB&R offers to use optimal settings including 4MB (larger) block size, producing smaller metadata table using less RAM/CPU resources
 - c) Always uses 'Per-VM backup files' mode
 - d) Reverse incremental not supported
 - e) 'Defragment/Compact full' not supported
 - f) Repository for VB&R Endpoint Backup not supported
 - g) Can't use as target for file copy jobs
 - h) Can't use as a cloud repository
 - i) Limited number of concurrent open files, thus limited number of **restore points** allowed: **42 max for 6600/7 max for VSA**
- c. EMC DataDomain Boost
 - Distributed Segment Processing data segmentation, filtering, compression done on side of backup application for increased throughput, reduced b/u window, & increased b/u job performance
 - 2. Advanced Load Balancing balance data transfer load & perform auto link failover in case of network outage
 - 3. Link Failover see "2" above
 - 4. Virtual Synthetics lets you synthesize Fulls without physically copying data, using pointers to existing data segments
 - 5. Managed File Replication not supported by VB&R
 - Veeam leverages DD Boost Technology via DD Boost Server (target-side component) & DD Boost Library (source-side component, embedded in Veeam Data Mover Service; installed on *Gateway Server*)
 - 7. Gateway Server bridge between Veeam & DD system
 - 8. No more than 60 restore points allowed
 - 9. Recommended to do Synthetic Fulls when using DD Boost
 - 10. For Backup Copy with GFS, make sure Gateway Server is close to DD Server (i.e. offsite)
 - 11. A VM in multiple jobs has 'Full data' during backup in 1st job; other jobs just backup metadata & changed blocks; helpful for Active Fulls, but restores are longer due to dedup transform process
 - 12. When multiple interfaces used, DD distributes data over all interface connections for improved data transfer performance & additional resiliency
 - 13. Accelerate Entire VM Restore
 - a) Veeam uses sequential data reading from backups & parallel VM disks restore; creating map of data blocks in backup files to read data blocks of VM disks from backup files sequentially; reads data in multiple threads as well

- 14. Backup Proxy for Accelerated Restore
 - a) VB&R restores VM disks through a Proxy
 - b) If configured to use Proxy automatically, Veeam uses one with least load
 - c) Veeam Data Mover Service is started for every VM disk needing restored
 - d) 200MB RAM required for each VM disk restore in parallel
- 15. Limitations for Accelerated Restore
 - a) Only works on Data Domain with DD Boost
 - b) If restoring VM with expanding disks, restore process may be slow
 - c) If using "nbd" to restore, the # of disks restored in parallel can't exceed number of allowed connections to ESXi Host
 - d) When adding to SOBR, the backup file placement policy must be set to "Locality" or 'Parallel VM disk restore' will be disabled
- 9.6 Veeam Cloud Connect
 - a. Overview
 - 1. Tenants using Service Providers (SPs) as Veeam Cloud Repository storage "as a service" (RaaS)
 - 2. Tenants can do following tasks with Cloud Connect:
 - a) Backup VMs to cloud repository
 - b) Copy VM backup files to cloud repository
 - c) Restore VM data from cloud repository (Full VM, VM disk, VM Files, VM Windows guest OS files)
 - d) (Manual, not scheduled) File Copy operations betweent tenant & cloud
 - e) Parallel processing is supported, & is configured by the SP
 - b. Responsibilities:
 - 1. SP
 - a) Installs/configures Veeam Cloud Connect
 - b) Sets up SSL certs to enable secure communication to Cloud
 - c) Creates Cloud Gateways
 - d) Registers tenant user accounts
 - e) Manages tenants
 - f) Installs optional target WAN Accelerator
 - 2. Tenant
 - a) Installs VB&R Server
 - b) Connects to Veeam Cloud Connect infrastructure from VB&R Server
 - c) Configures & runs jobs and restore tasks targeted at cloud repositories
 - d) Installs optional source WAN Accelerator
 - e) Veeam Cloud Connect can be used with any PAID Veeam license (not Free)
 - c. Lease & Quota
 - 1. Set by SP to help them control how tenants consume storage on cloud repositories
 - 2. Quota amt of space, in GB or TB, assigned to a tenant on **1** cloud repository

- 3. Lease period of time which a tenant has access to their cloud repository quota(s)
- d. Licensing for Cloud Repositories
 - 1. Installed by SP on VB&R Server & licensed on per-VM basis
 - Consumed only by *active* VMs successfully backed up/copied VM within last 31 days
 - a) Restore points or jobs for same VM do not count against licensing
 - 3. SP Cloud Connect licensing states:
 - a) Normal active VMs doesn't exceed license amount
 - b) Grace active VMs exceeds license amt; valid for 60 days; tenants can still backup and copy existing and new VMs to the Cloud
 - c) Post-Grace 60-day grace period expired; tenants can only Backup/Copy VMs already being backed up/copied in Normal state
 - d) Recovery done when SP installs new license for more active VM count, or reduces # of active VMs (disable/remove tenants)
- e. v9 Cloud Connect Enhancements
 - 1. Veeam Cloud Connect Replication as a DR solution; mitigates capital expense of having secondary datacenter (DRaaS)
 - a) Hardware Plan provided by SP that defines CPU, memory, storage, & network resources a tenant can use for Veeam Cloud Connect Replication
 - b) Failover options:
 - 1) Full site
 - 2) Partial site
 - c) Otherwise known as "Disaster-Recovery-As-A-Service (DRaaS)"
 - d) Benefits:
 - 1) Ease of use
 - 2) Ease of network config
 - 3) Fully automated upgrading network extension appliances
 - 4) Bandwidth friendly WAN Accelerators, compression, seeding, Replication from Backup
 - 5) Self-service via web portal
- 9.7 Veeam Backup Enterprise Manager
 - a. Veeam Plug-in for vSphere Web Client
 - 1. Installed via Veeam Backup Enterprise Manager: Configuration > vCenter Servers
 - 2. At-a-glance & detailed view of job status & backup resources, as well as capacity planning and unprotected VMs
 - Create Restore Points with VeeamZIP or Quick Backup from the vSphere Web Client (Rt-click on a VM, or go to VM > Manage tab > VeeamZIP; NOTE: There is no tab for Quick Backup.. it'll just auto-start that job using the B/U Job the VM is in on the VB&R Server)



- 4. User permissions Portal Administrator or Restore Operator in Ent Mgr; VirtualMachine.Interact.Backup, Task.Create, Task.Update in vCente
- b. Enterprise Manager (EM) Required Permissions
 - 1. Any of following roles are needed to use EM
 - a) Portal Admin full access
 - b) Restore Operator, Portal User configuration area not accessible
 - 1) Can access their restore scope a list of VMs that can be recovered by appropriate personnel
 - 2) Restore scope is only customizable with Ent+ license
- c. Restore of Application Items
 - 1. Application VMs must have application-consistent backups (i.e. Exchange, SQL)
 - 2. Performed by:
 - a) Exchange = Restore Operator or Portal Admin
 - b) SQL = Restore Operator or Portal User
 - 3. Local app permissions:
 - a) Exchange = Exchange Admin & Admin for mailboxes
 - b) SQL = dbo user
 - c) If admin rights cannot be given, utilize Veeam's U-AIR feature
- d. Self-Restore Portal
 - 1. Web-UI for delegated users for file-level restore capability, given by local admin of Enterprise Manager (EM); URL: http(s)://EntMgrSrvr:9443/selfrestore
- e. Managing Encryption Keys
 - 1. Ability to restore encrypted data in case of lost/forgotten password
 - 2. Best to regulary generate new keys; raises encryption security level
 - a) Keyset Retention Period determines length with which EM keys are used for encryption/decryption
 - 3. 2 matching keysets are generated:
 - a) Public Enterprise Manager Key <u>encrypts</u> storage keys on VB&R Servers connected to Enterprise Manager
 - b) Private Enterprise Manager Key <u>decrypts</u> storage keys in case a password for encrypted backup or tape is lost
 - 4. Keys are created in 'inactive state'; they must be "actviated" for use
 - 5. Regularly backup the keys in the event the EM database gets corrupted, or the EM server is rebuilt and keys, which are stored in EM DB, are no longer available in case a restore of encrypted data is needed in event of lost/forgotten password

- 6. Key Retention Period determines lifetime of EM keyset; once retention is met, keyset marked inactive
- 7. Can export keyset for backup; exported in PEM format
- f. Decrypting Data Without Password
 - 1. Requirements:
 - a) Ent or Ent+ license
 - b) VB&R Server used to encrypt data was previously added to EM
 - c) VB&R Server using to decrypt data is added to EM
 - 2. Use Enterprise Keys Restore Wizard within VB&R and EM to restore encrypted backups with lost passwords
- g. Veeam Backup Enterprise Manager RESTful API
 - 1. EM exposes its objects via Web API based on REST to let dev's communicate with EM to query information about its objects & perform basic operations with them using HTTP/HTTPS
 - 2. Is platform-agnostic
 - 3. EM comes with its own web client for testing the RESTful API (EM Web Client), at URL: http://<emserver>:9399/web
- 9.8 Standalone Console
 - a. Client side component allowing access to the VB&R Server to perform "availability" (DP/DR) operations
 - b. If connection to VB&R server is lost, session is maintained for 5mins
 - c. No limit on number of Console deployments
 - d. Priority on configurations user who saves operation first gets priority; other users prompted to reload window or wizard to get most recent change info
 - e. Components installed with Console:
 - 1. Powershell Snap-In
 - 2. Explorer for AD
 - 3. Explorer for Exchange
 - 4. Explorer for SQL
 - 5. Explorer for Oracle
 - 6. Explorer for SharePoint
 - 7. Mount Server
 - f. Veeam login rights = users must be added to "local users" (or Domain Users) group on VB&R Server
 - g. Install requirements:
 - 1. MS Windows, physical or virtual
 - 2. Can be deployed remotely behind NAT with Veeam server OUTSIDE the NAT
 - h. Limitations:
 - 1. Can not restore config backup via remote console
 - 2. Machine remote console installed on not added as 'Managed Servers' by default so some operations not allowed (e.g. import backups; assign roles)

- 9.9 vCloud Director Support
 - a. Uses vCD API to directly backup from & restore directly to the vCD hierarchy
 - b. vApp container of 1 or more VMs along with parameters defining operational details > vApp metadata
 - c. VB&R captures both VMs and vApp Metadata

SECTION 10 – VEEAM ONE FEATURES AND FUNCTIONALITY

- 10.1 VeeamONE Overview
 - a. Comprised of 3 components:
 - 1. VeeamONE Monitor primary tool to monitor the virtual & backup infrastructure
 - a) Manage, view, & interact with alarms
 - b) Analyze performance of virtual & backup infrastructure components
 - c) Monitor efficiency of data protection operations
 - d) Troubleshooting, generate reports
 - e) Data collected in REAL-TIME
 - 2. VeeamONE Reporter helps verify configuration issues, optimize resource allocation & utilization, & track changes
 - a) Capacity planning
 - b) Track mission-critical VM protection
 - c) Data collected PERIODICALLY (same with Business View)
 - 3. VeeamONE Business View allows grouping virtual infrastructure objects into categories (e.g. SLAs, business unit, purpose, etc)
 - a) Categorization model is applied to the monitoring & reporting functionality
 - b. For use with vSphere, vCloud Director, SCVMM, VB&R servers, or Hyper-V
- 10.2 VeeamONE Components
 - a. Monitoring/Alerting (VeeamONE Monitor)
 - 1. Integration with your virtual & backup infrastructure
 - 2. Heterogenous virtual infrastructure support monitor from single console
 - 3. Support for SCVMM, failover clusters, & Hosts gather data from large environments
 - 4. Integrated for standalone monitoring
 - 5. Client/server architecture supports multi-admin access
 - 6. Alarms set up notifications, SNMP traps, or run scripts
 - 7. Advanced monitoring options view & manage in-guest processes and services, log on to VM console from VeeamONE Monitor

- 8. Custom Shared Volume, SMB, & local storage monitoring
- 9. Historical reports obtain point-in-time view of virtual environment
- 10. Business view categorization
- b. Reporting & Dashboards (VeeamONE Reporter)
 - 1. Virtual Infrastructure (VI) Summary Dashboards:
 - a) VI Summary
 - b) Host Summary
 - c) Local Storage Summary
 - d) SMB Share Summary
 - e) Cluster Shared Volume (CSV) Summary
 - 2. Reports:
 - a) Backup Billing calculates Backup Infrastructure storage costs
 - b) Backup Inventory inventory info for VB&R infrastructure
 - c) Capacity Planning for Backup Repositories analyzes Repository free space
 - d) Job Config Change Tracking records backup job config changes
 - e) Backup Job Historical Info provides backup job session information
 - f) Veeam Cloud Connect User Report overview of storage utilization for Cloud Connect
 - g) SQL Backup Job Historical Info provides info of SQL server backup jobs
 - h) Restore Operator Activity audits info of restore actions
 - i) Protected VMs which VMs have current restore points
 - j) Orphaned VMs VMs in backup files but not in pending backup jobs
 - k) VMs Backed Up By Multiple Jobs
 - I) VM Failover Plan Overview looks at failover plan configs
 - m) VMs With No Archive Copy info on VMs not associated with archive (Copy)
- c. Business Categorization (VeeamONE Business View)
 - 1. Presents data about VMs, Hosts, Storage, Clusters in business terms
 - 2. Allows use of vSphere tags
- d. Autodiscovery of Backup & Virtual Infrastructure
 - 1. Connecting virtual infrastructure to VeeamONE to collect information, either during install or manually afterwards
 - Adding/removing servers to one component propagates add/removal to other VeeamONE components; e.g. adding or removing vSphere from Monitor will auto-add/remove vSphere from Reporter & Business View
 - 3. Data collection:
 - a) Agentless; uses network connection via API calls & OS subsystems
 - b) Monitor data is collected in real-time; Reporter/Business View data can be collected via schedule (hours or days) or manually
 - 4. Multi-user access, allowing simultaneous connection to identical objects/views
 - 5. User permissions can be restricted for 2 inventories:
 - a) vSphere Inventory
 - b) vCloud Director Inventory

- User access can be restricted & delegated views to a biz unit (vSphere) or org (vCD)
- 7. Do not add restricted users to VeeamONE security groups or they will gain global VeeamONE inventory access

10.3 – VeeamONE Deployment

- a. Typical
 - 1. For environments with less than 100 Hosts/1500 VMs
 - 2. All VeeamONE components installed on 1 machine, phys or virtual
 - 3. SQL Server 2012 Express installs with VeeamONE if not already installed or no remote
 - 4. Multi-user access install VeeamONE Monitor Client on separate machines
- b. Advanced
 - 1. For larger environments with **more than 100 Hosts/1500 VMs**, separating roles on different virtual or physical servers:
 - a) VeeamONE Server i.e. SQL
 - b) VeeamONE Web UI Reporter and Business View
 - c) Monitor Client workstation install for client/server model
- 10.4 VeeamONE Assessment Tool
 - a. Assessment Report Pack
 - 1. Ensures VMs are ready to backup & infrastructure assessment reports analyze environment for incompatibilities & config erros; predicts amount of future changes on disks have influence on backup job frequency, etc.
 - b. VMware Infrastructure Assessment Pack (Reports):
 - 1. Datastore Performance Assessment datastore performance info & potential backup issues
 - 2. VM Change Rate Estimation tracks virtual disk change rate, assessing future repository space needs
 - VM Configuration Assessment assesses VM readiness for backup, showing possible issues or limitations that could cause backups to fail (e.g. no VMware Tools or VMs with Independent Disks [which are skipped from backups])
 - c. Hyper-V Infrastructure Assessment Pack (Reports):
 - 4. **Configuration Assessment** analyzes Hyper-V infrastructure against recommended to help mitigate potential issues backing up VMs
 - Performance Assessment evaluates Hyper-V infrastructure for optimal settings to verify its efficiency
 - 6. VM Change Rate Estimation same as VM ware above
 - d. Data Sovereignty
 - 1. Assigning "Location" to virtual infrastructure objects, backup infrastructure objects, or agent management objects (discussed in Section 3.2)

- 2. Two Reports to Track Sovereignty
 - a) Data Sovereignty Overview analyzes location of backups, copies, replicas for a data source
 - b) Data Sovereignty Violations analyzes whether backups, copies, replicas reside in location different from data source

SECTION 11 – PRODUCT EDITIONS

11.1 – Editions Comparison

- a. All Editions are installed by the same setup file
- b. Below is a table of features for <u>VMware</u> and <u>Hyper-V</u>:

VMWARE	MWARE HYPER-V						
Feature	STD	ENT	ENT+		STD	ENT	ENT+
Backup Copy	х	х	х		х	х	х
WAN Acceleration		х	х			х	х
Backup from			Y				
storage snapshots			X				
Native Tape Suppt	limited	х	х		limited	х	х
vCloud Director	limited	limited	х				
U-AIR		х	х			х	х
Surebackup		х	х			х	х
SureReplica		х	х				
On-Demand		limited	v			limitod	v
Sandbox		IIIIIteu	×			IIIIIIteu	X
File System Index	restricted	х	х		restricted	х	х
1-click Restore		х	х			х	х
Delegation & self-							
recovery of			х				х
VMs/guest files							
Job clone/edit		х	х			Х	х
Veeam Explorers	limited	х	х		limited	Х	х
SOBR		limited	х			limited	х
Backup from			v				v
NetApp			^				~
Guest-Int Proxy		х	х			Х	х
Mount Server	х	х	х		х	х	х
Direct NFS	х	х	х		х	х	х
Stndalone console	Х	х	х		Х	х	х

Data Domain/HPE StoreOnce	х	х		х	х
Ent Mgr Web API		х			х

- c. Product Edition Clarifications:
 - 1. vSphere Features Only:
 - a) Quick Migration All Paid Editions
 - b) SureReplica Ent and Ent+
 - c) Backup from Storage Snapshots Ent+
 - d) Backup from NetApp Snapvault/Snapmirror & Nimble Replicated Copies
 - e) vCloud Director Support All Paid Editions
 - f) vSphere Web Client Plugin All Paid Editions
 - g) Veeam Explorer for Storage Snapshots All Editions
 - h) On-Demand Sandbox for Storage Snapshots Ent+
 - 2. Enterprise and Enterprise Plus Only:
 - a) SureBackup
 - b) SureReplica
 - c) Proxy Affinity
 - d) U-AIR
 - e) Scale-Out Backup Repository (Ent = 1 SOBR w/3 active extents & 1 inactive)
 - f) Built-in WAN Acceleration (Ent = Veeam Cloud Connect targets only)
 - g) Backup I/O Control (Ent+ = per-Datastore I/O Control)
 - h) Veeam Explorer for Oracle
 - i) Dedup Storage Integration
 - j) Per-VM Backups for Dedup appliances
 - k) On-Demand Sandbox
 - I) Exchange Item Recovery Portal for Helpdesk
 - m) SQL DB Restore Portal
 - n) 1-Click File/VM Recovery Portal for Helpdesk
 - o) Guest Interaction Proxy
 - 3. Enterprise Plus Only:
 - a) Self-Service File Restore Portal
 - b) Backup from NetApp Snapvault/Snapmirror & Nimble Replicated Copies
 - c) On-Demand Sandbox for Storage Snapshot
 - d) File Recovery Delegation
 - e) Enterprise Manager Restore Scope Customization
 - f) Backup I/O Control per Datastore

11.2 – Product Licensing

a. Product licensed per socket

	Paid	Trial	ProPartner NFR	Free Edition
Number of CPU sockets	Number purchased	32	12	Unlimited
Duration	Perpetual/Subscription	30 days	6 or 12 months	Perpetual
Functionality	Edition purchased	Enterprise Plus	Enterprise Plus	Free Edition
Technical support	Basic or Production Support	Evaluation Support	Limited	Limited

11.3 – Full & Free Functionality Modes

- a. VB&R has 2 Modes > Full & Free
 - 1. To switch to either, Main Menu > View > Free Functionality (or Full Functionality) **NOTE:** the View option is hidden if a valid license is installed
- b. Free Edition limitations
 - 1. No scheduling
 - 2. Only FULL Backups; no incrementals
 - 3. No Replications
 - 4. No vPower; only VeeamZIP (to import backups into paid VB&R versions)
 - 5. Only 1 VM backup

SECTION 12 – TROUBLESHOOTING

12.1 – How to **Identify the Problem**

- a. Most common problems:
 - 1. Error messages Backup job error; error msgs in GUI/program; restore errors
 - Unexpected infrastructure behavior poor server performance (high server load); non-responsive GUI; non-responsive VB&R Server; Veeam Services not starting; incorrect info; BSOD
 - 3. Other environmental challenges poorly tuned VB&R infrastructure

12.2 – Review & Analyze the Issue

- a. Check if issue is common or limited
- b. Common issues:

- 1. Free ESXi not supported "current license or ESXi version prohibits execution of requested operation."
- 2. Licensing issues
- 3. Restore challenges restore speeds; restore failures; alternate options when primary restore option fails
- 4. Bottlenecks source/proxy/(source WAN)/network/(target WAN)/target; stats don't necessarily show a problem, but rather weakest link in the data path
- 12.3 Common Issues & Misconfigurations
 - a. Low Performance (bottlenecks)
 - b. Throttling bottlenect limiting read/write on Repository; network throttling rules
- 12.4 Common VMware Related Issues
 - a. Snapshot creation failure due to certain disk mode/types: SCSI Bus Sharing, Physical RDMs, Independent disks
 - b. Snapshot removal failure
 - c. Snapshot removal stun review the 2 KB URLs in Handbook
 - d. NFC-related errors mainly due to:
 - 1. DNS resolution of target Host
 - 2. Port 902 from Backup Proxy or Server to ESXi Host (& vice versa)
 - 3. Permissions
 - 4. Review Veeam KB1198
- 12.5 Log Files
 - a. Collected from Main menu > Help > Support Information, and select Scope:
 - 1. Export for this job
 - 2. Export for this VM
 - 3. Export ALL logs
 - b. Reference KB1832 for more info on log collection
 - c. Default log file location:
 - 1. Windows: %PROGRAMDATA%\Veeam\Backup
 - 2. Linux: var/log/VeeamBackup or tmp/VeeamBackup
- 12.5 Veeam Support
 - a. Support Programs:
 - 1. Basic Phone/Web support, M-F, 8a-8p, with Upgrades/Updates
 - 2. Production 24x7x365, with Upgrades/Updates
 - 3. Evaluation 60 day eval support, M-F, 8a-5p; no Upgrades/Updates

Service	Evaluation Support	Basic Support	Production Support
Product updates	NA	Yes	Yes
Product upgrades	NA	Yes	Yes
Technical Support	Phone/Web	Phone/Web	Phone/Web
Business Hours (customer local time)	Mon-Fri 8 am – 5 pm	Mon – Fri 8 am – 8 pm	24x7x365

- b. Response Time SLA
 - 1. Severity 1 business critical; 1 or 2hr response (Production vs Basic)
 - 2. Severity 2 adversely impacting production; 3 or 8hr response (")
 - 3. Severity 3 non-production issue; 6 or 12hr response (")
 - 4. Severity 4 minor issue; 8 or 24hr response (")
- c. Contacting Customer Support
 - 1. Info needed by Support:
 - a) Name, Org Name, Phone
 - b) Case #, if applicable
 - c) Product name, Release, maintenance applied to product
 - 2. Logging a Case:
 - a) Issue description, impact on business, severity, exact text/error
 - b) Steps to reproduce error/issue, known workarounds
 - c) Contact #
 - d) Best time to reach
 - 3. Submitting a Case:
 - a) Web via Customer Portal
 - b) Phone phone # listed under "Contacts"; speed at which contacted based on licensing, Support (Basic vs Prod) Program option, and Severity Level
 - c) Three attempts are made to reach customer, on business days, for updates/more info; if no update, case closed without customer consent
- d. Product Lifecycle
 - 1. For older product status: <u>http://www.veeam.com/support/releasestatus.pdf</u>
 - 2. Support of Releases:
 - a) New Releases GA products
 - b) Current Releases
 - c) End of Fix Releases support; existing fixes available; no new fixes
 - d) End of Support/Withdrawal From Market Releases no support
- e. Third Party Software Support
 - 1. Veeam will assist to determine if issue is caused by 3rd Party, & if needed will either request customer open case with vendor, or use TSANet to open case for vendor support

- 12.7 Search For Additional Information
 - d. Community foruns <u>http://forums.veeam.com</u>; maintained/moderated by Veeam Product Mgmt Team; make feature request
 - e. Customer Support Portal <u>http://cp.veeam.com</u>; manage caes; request one-click update; attach logs to existing cases; obtain product downloads/updates; manage licenses
 - f. Knowledgebase (KB) <u>http://www.veeam.com/kb_search_results.html/</u>
 - g. Online documentation <u>http://www.veeam.com/documentation-guides-</u> <u>datasheets.html</u>

SECTION 13 – ADDITIONAL RESOURCES

Shane Williford, Sr. Systems Engineer For Public Use, but please give credit to the author if posted on social media or in blogs