

## ***BR418-EN Veeam v12.1 (VMCE) with Storage-Connection***

### **Kurzbeschreibung:**

The course **BR418-EN Veeam v12.1 (VMCE) with Storage-Connection** includes the contents of **BR410-EN Veeam Backup & Replication v12.1(VMCE) Configure, Manage and Recover** and prepares for the Veeam Certified Engineer (VMCE) certification. Additionally, this course provides an in-depth treatment of the course content as well as additional information and exercises on the topic of storage integration with Veeam.

### **Zielgruppe:**

- Systems Engineers / Administratoren
- Backup / Virtualization Administrators
- Pre-sales / post-sales staff
- Solution Architects / Consultants

This course is designed for beginners as well as administrators who want to implement the different levels of storage integration.

Integration will be demonstrated using NetApp systems as examples.

### **Voraussetzungen:**

Participants of the workshop **BR418-EN Veeam v12.1 (VMCE) with Storage-Connection** should have experience in the IT sector, especially with virtual infrastructures.

### **Sonstiges:**

**Dauer:** 5 Tage

**Preis:** 3950 Euro plus Mwst.

### **Ziele:**

In the workshop **BR418-EN Veeam v12.1 (VMCE) with Storage-Connection** you can prepare for the **Veeam Certified Engineer (VMCE) certification exam**.

After successful completion of the course and the exam, you can call yourself a "**Veeam Certified Engineer (VMCE)**".

You can take the exam after the course at a Pearson VUE test centre. It consists of 50 questions that have to be answered in 75 minutes. You need a score of at least 70% to pass the exam. You can find detailed information about the exam [here](#).

You can take a trial test [here](#).

For further exercises, the LABS are still available 10 working days after the course.

## Inhalte/Agenda:

- **◆ What can be protected?**
  - ◆ ◇ Review of Veeam Data Platform and introduction to the class scenario
- **◆ Secure your backup server**
  - ◆ ◇ Describe strategies and tools to secure the Veeam backup server to avoid unauthorized access and data leaks
- **◆ Application consistency with secure authentication**
  - ◆ ◇ Achieve application-consistent backups of virtual machines while maintaining operating system secure authentication
- **◆ Protecting workloads**
  - ◆ ◇ Efficiently protect VMware and Hyper-V virtual machines based on well-defined SLAs through the creation of backup jobs
- **◆ Deploying agents**
  - ◆ ◇ Identify the use of protection groups to automate the installation of Veeam Agents and protecting workloads with agent backup jobs
- **◆ Protecting NAS**
  - ◆ ◇ List required components and features available to protect NAS solutions
- **◆ Optimizing your backups**
  - ◆ ◇ Analyze features and settings that allow backup storage optimization, faster backups and data consistency
- **◆ Immutability**
  - ◆ ◇ Describe backup data protection mechanisms to avoid premature deletion and unwanted modifications
- **◆ Linux Hardened Repository**
  - ◆ ◇ Identify characteristics and deployment steps of Linux Hardened Repositories to achieve backup data immutability
- **◆ Object storage repositories**
  - ◆ ◇ Describe use cases, advantages and considerations to implement object storage solutions as Veeam backup repositories
- **◆ Backup infrastructure optimization**
  - ◆ ◇ List deployment options and additional settings to improve general backup solution performance
- **◆ Replication**
  - ◆ ◇ Describe use cases, architectures and features of replication jobs and continuous data protection (CDP) policies
- **◆ Backup copy Jobs**
  - ◆ ◇ Ensure recoverability and adhere to the 3-2-1 Rule with backup copy jobs
- **◆ Long-term retention**
  - ◆ ◇ List different mechanisms for data archiving, including grandfather-father-son retention policies
- **◆ Scale-out Backup Repository™**
  - ◆ ◇ Describe architecture, placement policies, data tiers and management of Scale-out Backup Repositories (SOBRs)
- **◆ Move and copy backups with VeeamMover**
  - ◆ ◇ Identify use cases for virtual machine and backup migrations with VeeamMover
- **◆ Recovery verification**
  - ◆ ◇ Create automated tests to ensure recoverability from backups and replicas
- **◆ Veeam Backup Enterprise Manager**
  - ◆ ◇ Describe the use cases for Veeam Backup Enterprise Manager
- **◆ Recovery scenario — Virtual machine failure**
  - ◆ ◇ Choose from different methods to recover a virtual machine from the backup
- **◆ Recovery scenario — Ransomware attack**
  - ◆ ◇ Securely restore a server after a ransomware incident with malware scanning of volumes directly from the backup and as part of the restore process
- **◆ Recovery scenario — Agent recovery**
  - ◆ ◇ Explore available options to restore data from agent backups
- **◆ Recovery scenario — Explorer recovery**
  - ◆ ◇ Use Veeam Explorers™ to recover application items directly from image-level backups
- **◆ Recovery scenario — Guest file recovery**
  - ◆ ◇ Restore guest operating system files directly from image-level backups and from diverse guest file systems
- **◆ Recovery scenario — Recovery from replica**
  - ◆ ◇ Describe virtual machine states available when recovering a virtual machine from its replica and mechanisms to avoid data loss and interdependent services recovery
- **◆ Recovery scenario — Instant NAS recovery**
  - ◆ ◇

- ◇ List steps and considerations to instantly recover an entire file share from its backup
- - ◆ **VMware Storage Integration**
    - ◇ Requirements
    - ◇ Installation
    - ◇ Features (such as Snapshot Orchestration, Snapshot Accelerated Backup Jobs, etc.)
    - ◇ Provider comparison
  - ◆ **Agent storage integration**
    - ◇ Requirements
    - ◇ Functions
    - ◇ Configuration
  - ◆ **File-Share Backup**
    - ◇ Basic installation
    - ◇ System preparation
    - ◇ Snapshot integration
  - ◆
  - ◇