Table of Contents

Physical Security

Best practices
- Role Based Access Controls on a physical level
- Access to the Datacenter
- Surveillance
- Equipment Racks

Infrastructure Hardening

Detect
- Create a Veeam honeypot server
- Leverage Veeam One alarms

Protect
- Anonymize the infrastructure

Hardening
- Secure by Design
- Remove Unused Components
- Veeam Backup & Replication Server
- Enterprise Manager
- Console Access
- Roles and Users
- Password management policy
- Lockout policy
- Required Permissions
- Patching and Updates
- Encryption
- Segmentation
- Ports
- Visibility
- Recovery Strategy
- The 3-2-1-1-0 backup rule
- Protect backups
- Educate your Staff
Add Veeam to a Workgroup, Domain or Forest? ........................................... 15
  Best Practice .......................................................................................... 16
    Windows Workgroup ............................................................................. 16
    Management Domain ............................................................................ 17
  What type of trust? ................................................................................. 17
Segmentation using Zones ................................................................. 19
  Untrusted Zone ...................................................................................... 21
  DMZ. .................................................................................................... 21
  Management Zone ................................................................................... 22
  Trusted Zone .......................................................................................... 22
  Restricted Zone ....................................................................................... 22
  Audit Zone ............................................................................................. 23
Hardening Backup Repository — Windows ...................................... 24
  Standalone and Physically secured ...................................................... 24
  Local Account with administrative access ...................................... 25
  Set permissions on the repository directory ................................... 27
  Modify the Firewall ............................................................................... 28
  Disable remote RDP services ............................................................. 30
WORM Storage with Hardened Repository ..................................... 31
  Deploy Veeam repository using single use credentials .................. 31
  Disable SSH after deployment ............................................................ 31
  Beware of IPMI .................................................................................... 31
  NTP ...................................................................................................... 31
Physical Security

It is essential that only authorized personnel have physical access to the datacenter. Datacenter’s hold sensitive and crucial information and services. Software-based protections on your server(s) become far less effective or even useless as soon as an attacker gains physical access! Access into a datacenter is limited.

Best practices

- Use Role Based Access Controls (RBAC) on a physical level;
- Multi-factor authentication at the physical level: any authorized person to enter the datacenter has its own digital access key combined with something they know like a pin code and/or biometric measures;
- Prevent from tailgating with solutions such as airlock doors at entry points;
- Make sure there are no exterior windows and relatively few entry points;
- Racks with hardware are by default locked;
- Equipment in the racks is smartly placed;
- Visibility in the current security status is key for an accurate security.

Role Based Access Controls on a physical level

Make sure that anyone that is authorized to enter the datacenter can only access those parts they are entitled to. Follow the principle of least privilege, give people the correct rights to do their job properly, nothing more nothing less. For example, an UPS and generator engineer does not need access to any of the racks in the datacenter and a Compute engineer should not have access to the UPS and generators.

Access to the Datacenter

An important part of a layered security defence is always knowing who entered the Datacenter and that access is being logged. Any authorized person to enter the datacenter has its own digital access key combined with something they know like a pin code and/or biometric measures. Make sure people are screened before they become an authorized person to access the datacenter. Prevent tailgating and unauthorized access by enforcing CCTV monitored airlock doors.

Surveillance

It is crucial to protect a datacenter from external threats and attacks and to make sure only authorized personnel has access to the areas where they need to be. Monitor for suspicious activity using footage from surveillance cameras (CCTV) installed along the outside perimeter but also inside the datacenter.
Equipment Racks

By placing and using locks per 19-inch rack you can shrink the physical security domain from the whole datacenter to a 19-inch rack. By smartly placing the different hardware components and their specific roles in different racks you can enable RBAC rights to that particular security domain. For example, do not place the Veeam Repositories in the same racks as the production storage or the hypervisor hardware.

Important: Even though you do not have your own Datacentre's and are renting space or even just Infrastructure as a Service, always check how the physical security is arranged and if it fits your security policy.

Infrastructure Hardening

This provides practical advice to help administrators to harden their infrastructure. It follows security best practices so that customers reduce chances of being compromised.

Hardening is about securing the infrastructure against attacks, by reducing its attack surface and thus eliminating as many risks as possible. One of the main measures in hardening is removing all non-essential software programs and utilities from the deployed Veeam components. While these components may offer useful features to the administrator, if they provide additional access to the system, they must be removed during the hardening process.

But also, creating visibility in what goes on in the infrastructure is part of hardening your infrastructure. Making sure you will notice when an attack may/is/or has taken place and then making sure logs and traces are saved for law-enforcement and security specialists when needed.

Detect

Being able to detect an attack before it takes place or when it takes place can considerably mitigate the impact.

Create a Veeam honeypot server

Honeypot servers with authentication monitoring will help detecting attacks that target your Veeam Infrastructure.

Leverage Veeam One alarms

Veeam One offers the possibility to monitor possible ransomware activity through a set of predefined alarms such as “immutability state”, “possible ransomware activity”, “Immutability change tracking”.

© 2022 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.
Protect

Protecting your infrastructure successfully is all about understanding the current attack vectors; what and whom you are protecting your Veeam infrastructure against. Knowing what and whom you are protecting against makes it easier to take the correct countermeasures. One of those countermeasures is hardening.

Looking at the different Veeam Backup & Replication components you must protect the following components:

- Veeam Backup Server
- User Accounts
- Backup repositories
- Backup data flows

Consider the Veeam Backup & Replication Server to be the Number 1 target on your infrastructure and it should have very restricted access. As a rule the backup server is the single greatest target a hacker can claim on your network. Also, the backup repositories which hold the backup files are a primary target.

Anonymize the infrastructure

Name your backup infrastructure servers using non backup related names. Avoid names containing acronyms like “bkp”, “pxy”, “repo”, “vbr” or anything that could ease the task of an attacker.

On the other hand, the honeypot server should be easily identifiable on the network.

Hardening

Within the hardening process of your Veeam infrastructure there are a few steps everyone should always consider and act upon, namely:

- Secure by Design
- Remove Unused Components
- Console Access
- Roles and Users
- Required Permissions
- Encryption
- Backup and Replication Database
- Segmentation
- Visibility
- Recovery Strategy
Secure by Design

Overly complex designs become harder for the IT team to manage, also it makes it easier for an attacker to exploit and stay in the shadows. Simpler designs that can be easily overviewed are in basis more secure. Use the K.I.S.S.¹ (Keep It Simple and Straightforward) principle for your designs.

Adding security to an already existing infrastructure is much harder and costly than thinking about it while designing a new or refreshing an existing infrastructure. In a virtual infrastructure, it is good use to build up a Master image which has been hardened from the start. Removing all known attack vectors and only open access when Veeam components are added and needs specific (port) openings or extra software to function properly. This way, all builds are consistent and kept up to date which makes it secure in the basis.

Consider the Veeam Backup & Replication server to be the Number 1 target on your infrastructure and it should have very restricted access. As a rule, the backup server is the single greatest target a hacker can claim on your network.

¹ KISS is an acronym for "Keep it simple, stupid" as a design principle noted by the U.S. Navy in 1960. The KISS principle states that most systems work best if they are kept simple rather than made complicated; therefore, simplicity should be a key goal in design and unnecessary complexity should be avoided. A simple design is easier to overview and to secure. https://en.wikipedia.org/wiki/KISS_principle

Remove Unused Components

Remove all non-essential software programs and utilities from the deployed Veeam components. While these programs may offer useful features to the administrator, if they provide additional access ("back-doors") to the system, they must be removed during the hardening process. Think about additional software like web browsers, java, adobe reader and such. All parts which do not belong to the operating system or to active Veeam components, remove it. It will make maintaining an up-to-date patch level much easier.

Also disable remote desktop access, even on Veeam Backup & Replication server, which should only be accessible through Veeam Backup & Replication Console.

Veeam Backup & Replication Server

• Access to Veeam Backup & Replication Server should be limited to the Veeam Backup & Replication Console with MFA enabled, through a dedicated management server.

• No remote access protocol should be allowed.

• Backup & Replication Console should be removed from the Veeam Backup & Replication Server when possible. The console is installed locally on the backup server by default.

• Switch off the Veeam vPower NFS Service if you do not plan on using the following Veeam features: SureBackup, Instant Recovery, or Other-OS File Level Recovery (FLR) operations.
Follow these steps to remove the Veeam Backup & Replication Console:

The Console cannot be removed through the installer or by using Add/Remove in Windows. Open a cmd prompt with administrative access. On the command prompt type: wmic product list brief > installed.txt this will create a text document with all installed products and their respective Product Codes.

For uninstalling Veeam Backup & Replication Console, first de-install all Veeam Explorers:

- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft SQL
- Veeam Explorer for Oracle

You can uninstall these components by using: msiexec /x {ProductCode}

Example for uninstalling the Veeam Backup & Replication console is: msiexec /x {D0BCF408-A05D-45AA-A982-5ACC74ADFD8A}

Uninstalling Veeam Backup and Replication console removes PowerShell module and makes using Veeam Backup PowerShell cmdlets impossible. This may affect automation scripts or products that rely on PowerShell for interacting with Veeam Backup and Replication, for example Veeam Disaster Recovery Orchestrator (Veeam Availability Orchestrator).

**Enterprise Manager**

When Enterprise Manager is not used de-install it and remove it from your environment.

**Console Access**

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. The console lets several backup operators and admins log in to Veeam Backup & Replication simultaneously and perform all kind of data protection and disaster recovery operations as if you work on the backup server.

Prefer installing the Veeam Backup & Replication Console on a central management server, positioned in a secure network zone and protected with 2-factor authentication rather than installing the console on the local desktops of backup & recovery admins. Always enforce MFA when authenticating to the Veeam Backup and Replication Console itself (supported starting v12).
Roles and Users

Deploy an Access Control policy, managing access to management components is crucial for a good protection. Use the **principle of least privilege**. Provide the minimal privilege needed for some operation to occur. An attacker who gained high-privilege access to backup infrastructure servers can get credentials of user accounts and compromise other systems in your environment. Make sure that all accounts have a specific role and that they are added to that specific group.

Enforce containment to keep the attackers from moving around too easily. Some standard measures and policies are:

- Do not use user accounts for admin access, reducing incidents and accidents
- Give every Veeam admin his own admin account or add their admin account to the appropriate security group within Veeam, for traceability and easy adding and removal
- Only give out access to what is needed for the job
- Limit users who can log in using Remote Desktop and/or Veeam Backup Console
- Add 2-factor authentication to highly valuable assets
- Monitor your accounts for suspicious activity

A role assigned to the user defines the user activity scope: what operations in Veeam Backup & Replication the user can perform.

Learn more about roles and operations at [https://helpcenter.veeam.com/docs/backup/vsphere/users_roles.html](https://helpcenter.veeam.com/docs/backup/vsphere/users_roles.html)

Password management policy

Use a clever Password management policy, which works for your organization. Enforcing the use of strong passwords across your infrastructure is a valuable control. It's more challenging for attackers to guess passwords/crack hashes to gain unauthorized access to critical systems.

Selecting passwords of 10 characters with a mixture of upper and lowercase letters, numbers and special characters is a good start for user accounts.

Make sure default accounts and passwords have been modified on all your equipment.

For Admin accounts adding 2-factor authentication is also a must to secure the infrastructure.

And for service accounts use 25+ characters combined with a password tool for easier management. An Admin can copy and paste the password when needed, increasing security of the service accounts.
Make sure the password tool and database are available from a recovery site in order to have it available in case a disaster occurs. Keep in mind that a recent backup of your password tool and database must reside on an air-gapped media, such as DVD, CD-ROM, tape. The most crucial is the Veeam Repository password that will allow to restore from the backup files.

**Lockout policy**

Use a Lockout policy that complements a clever password management policy. Accounts will be locked after a small number of incorrect attempts. This can stop password guessing attacks dead in the water. But be careful that this can also lock everyone out of the backup & replication system for a period! For service accounts, sometimes it is better just to raise alarms fast. Instead of locking the accounts. This way you gain visibility into suspicious behaviour towards your data/infrastructure.

**Required Permissions**

Use the principle of least privilege. Provide the minimal required permissions needed for the accounts to run.

The accounts used for installing and using Veeam Backup & Replication must have the permissions detailed.

If VMware vCenter Server is added to the backup infrastructure, an account with reduced permissions can be used. Use the minimum permissions for your use-case. For example Hot-Add backup requires the “delete disk” permission. You can also consider elevating permissions for restores. See details here.

Backup proxies must be considered the target for compromise. During backup, proxies obtain from the backup server credentials required to access virtual infrastructure servers. A person having administrator privileges on a backup proxy can intercept the credentials and use them to access the virtual infrastructure.

**Patching and Updates**

Patch operating systems, software, and firmware on Veeam components. Most hacks succeed because there is vulnerable software in use which is not up to date with current patch levels. Make sure all software and hardware where Veeam components are running are up to date. One of the most possible causes of a credential theft are missing guest OS updates and use of outdated authentication protocols.
To mitigate risks, follow these guidelines:

- Ensure timely guest OS updates on backup infrastructure servers.
- Install the latest updates and patches on backup infrastructure servers to minimize the risk of exploiting guest OS vulnerabilities by attackers.

Choose strong encryption algorithms for SSH. To communicate with Linux servers deployed as part of the backup infrastructure, Veeam Backup & Replication uses SSH. Make sure that for the SSH tunnel you use a strong and proven encryption algorithm, with sufficient key length. Ensure that private keys are kept in a highly secure place and cannot be uncovered by a 3rd party.

**Encryption**

Backup and replica data is a highly potential source of vulnerability. To secure data stored in backups and replicas, follow these guidelines:

- Ensure physical security of target servers. Check that only authorized personnel have access to the room where your target servers (backup repositories and hosts) reside.
- Restrict user access to backups and replicas. Check that only authorized users have permissions to access backups and replicas on target servers.

Encryption Best Practices from Veeam Backup & Replication user guide:

Backup and replica data can be intercepted in-transit, when it is communicated from source to target over a network. To secure the communication channel for backup traffic, consider these guidelines:

- Isolate backup traffic. Use an isolated network to transport data between backup infrastructure components — backup server, backup proxies, repositories and so on. (Also see segmentation)
- Encrypt network traffic. By default, Veeam Backup & Replication encrypts network traffic traveling between public networks. To ensure secure communication of sensitive data within the boundaries of the same network, you can also encrypt backup traffic in private networks. For details, see Enabling Network Data Encryption.

Enabling Network Encryption from Veeam Backup & Replication user guide:
https://helpcenter.veeam.com/docs/backup/vsphere/enable_network_encryption.html
Backup and Replication Database

The Backup & Replication configuration database stores credentials to connect to virtual servers and other systems in the backup & replication infrastructure. All passwords stored in the database are encrypted. However, a user with administrator privileges on the backup server can decrypt the passwords, which presents a potential threat.

To secure the Backup & Replication configuration database, follow these guidelines:

- Restrict user access to the database. Check that only authorized users can access the backup server and the server that hosts the Veeam Backup & Replication configuration database (if the database runs on a remote server).

- Encrypt data in configuration backups as a best practice. Enable data encryption for configuration backup to secure data stored in the configuration database. Please note that user accounts and passwords are not stored in configuration backups when encryption is not active.

Segmentation

Add local protection mechanics, in addition to the border firewalls, intrusion detection, patching and such. You can make use of local mechanisms, like up-to-date anti-malware, firewalls and network segmentation. This way you create different rings-of-defence slowing an attacker down. A great way to strategically use segmentation is by implementing Zones.

A good practice is to place the backup repositories in a special segment not accessible by any user. Like for instance the production storage is only available to the virtual infrastructure components and application servers. Not directly accessible by any user!

To segment your infrastructure and Veeam Backup & Replication components, make sure the firewalls on the local server installations have the correct ports opened.

More information from Veeam Backup & Replication user guide:
https://helpcenter.veeam.com/docs/backup/vsphere/used_ports.html

You can also deploy solutions such as VMware NSX, as a counter measure with micro-segmentation to make sure the attack surface is as narrow as possible without blocking everyone to use the services. Visibility into the network and all data flows is crucial to help you protect all different rings/cells within your infrastructure. You can add the Veeam components to NSX policies to make sure they can communicate with each other without opening it up to any user.
Ports

Try not to use obscure ports and other tricks to try and hide Veeam ports and protocols in use, while this may look like a good choice. In practice this often makes the infrastructure harder to manage which opens other possibilities for attackers. Obscurity is not security!

You can check which ports are in use by which service on a Windows system by using:

```
netstat -bona > portlist.txt
```

you can open the text file with for instance notepad portlist.txt

Visibility

To know when you are under attack or have been breached it is vital to have visibility in the whole data flow path. You should be able to know what a ‘normal behaviour’ is and what is NOT. Monitor your accounts and Veeam infrastructure for suspicious activity. Place virtual tripwires, like e.g. creating a non-used admin account with alarms tied to it. When any activity on that account is observed, it will trigger a red alert instantly. There are several systems out there that can help you by alerting suspicious behaviour, so you get aware that someone is snooping around and is trying to gain access to your infrastructure. Visibility is Key!

It is important to get alerts as soon as possible while defending against other attacks like viruses, malware and ransomware. The biggest fear of these attacks is that they may propagate to other systems fast. Having visibility into for e.g. potential ransomware activity is a big deal.

Example Systems that could help you create visibility are:

- The “Possible ransomware activity” alarm in Veeam ONE
- The “Suspicious incremental backup size” alarm in Veeam ONE
- VMware vRealize Network Insight can take VMs, objects, groupings and their physical elements and easily fingerprint the application and determine the internal and external flows, the client connections, etc. this way you get an analysis of what is ‘normal’ behaviour and what is not.
- VMware vCenter with alerts that are triggered on virtual tripwires.

Links to Veeam One reports in user guide:

- [https://helpcenter.veeam.com/docs/one/alarms/backup_alarms_events.html](https://helpcenter.veeam.com/docs/one/alarms/backup_alarms_events.html)
- [https://helpcenter.veeam.com/docs/one/alarms/vsphere_alarms_events.html?zoom_highlight=ransomware](https://helpcenter.veeam.com/docs/one/alarms/vsphere_alarms_events.html?zoom_highlight=ransomware)
- [https://helpcenter.veeam.com/docs/one/alarms/hyperv_alarms_events.html?zoom_highlight=ransomware](https://helpcenter.veeam.com/docs/one/alarms/hyperv_alarms_events.html?zoom_highlight=ransomware)
Recovery Strategy

Have a recovery strategy in place, before you find out your infrastructure is breached you should know what to do when being compromised through attacks. Backup your data and make sure the backups cannot be accessed by an attacker to wipe them out. An offsite copy (airgap) or read-only on any media is highly recommended to survive any attack.

Furthermore, you must be aware that in case of a breach it is very likely that your assets will be sealed by government entities for analysis and forensic and they won’t be available for recovery. You should rely on dedicated recovery hardware in addition to keep off-site copies.

Preparation is the key. You must have tested recovery keeping in mind you will have to restart from nothing but backup files and a blank infrastructure.

• Get the task force ready

• Know your assets, to prioritize recovery. First perimeter is the surrounding environment, such as phone, mail, domain controllers, DNS etc etc... Then your core applications shall restart immediately after

• Extensively use testing automation tools, such as Veeam SureBackup or Disaster Recovery Orchestrator

The 3-2-1-1-0 backup rule

The 3-2-1 rule is very general, it works for all data types (individual and corporate) and all environment types (physical and virtual). When backing up your environments with Veeam, this rule becomes the “3-2-1-1-0 backup rule” where 1 media is offsite, 1 media is air-gapped, immutable or offline. 0 means “0 errors“ when enforcing the automatic recoverability verification of every backup with Veeam’s SureBackup.

Veeam Backup & Replication™ can help you to fulfil each 3-2-1-1-0 backup rule requirements.

• Have at least three copies of data: production, primary backup, backup copy.

• Store the copies on two different media: Veeam is storage-agnostic, meaning it supports tapes, disks, cloud storage and more. You can store your backups to any of the listed media.

• Keep one backup copy offsite: setup Backup Copy Jobs to transfer your backup offsite faster with built-in WAN acceleration or use Scale-Out-Repositories’ capacity tier to copy data to (cloud) object storage.

• Keep copies of your backups on immutable, air-gaped or offline medias.

By following the rule, you create multiple layers of resiliency and according security. Data and workloads will be made immutable (protection against deletion and modification), stored offline (protected against insider threats), air-gapped (protected against insider and other business continuity disasters e.g. fire, flood, earthquake, etc).
Protect backups

Veeam offers many ways to keep data out of reach of attackers. A properly designed backup infrastructure must include a data protection mechanism.

This can be offered by features such as

- Storage deduplication appliances through proprietary mechanism such as immutability or protected snapshots
- Object storage through immutability
- Tape through real air gapping
- Hardened Linux repository through WORM mechanisms as described later.

Ideally, all retentions shall be protected through air gap or immutability. But since the dwell time of the attackers is approximately one month average, it is fundamental to protect at least four weeks of restore points to mitigate the attack.

Educate your Staff

By deploying an employee awareness training, you make sure that your employees are aware of strange behaviour and of their critical roles in protecting the organization's services and data. This is not only for the IT department, but for everyone within the organization, because every organization is becoming an IT company rapidly, and everyone in a company can be targeted for social engineering and can potentially open a breach.
Add Veeam to a Workgroup, Domain or Forest?

Microsoft Active Directory is the heart of the IT infrastructure for nearly every organization. When setting up the Veeam Availability infrastructure keep in mind the principle that a data protection system should not rely on the environment it is meant to protect in any way! This is because when your production environment goes down along with its domain controllers, it will impact your ability to perform actual restores due to the backup server’s dependency on those domain controllers for backup console authentication, DNS for name resolution, etc.

Microsoft Active Directory consists of Forests and Domains.

A forest is a collection of one or more Active Directory domains that share a common logical structure, directory schema (class and attribute definitions), directory configuration (site and replication information), and global catalogue (forest-wide search capabilities). Domains in the same forest are automatically linked with two-way, transitive trust relationships.

A domain is a partition in an Active Directory Forest. Partitioning data enables organizations to replicate data only to where it is needed. In this way, the directory can scale globally over a network that has limited available bandwidth.

Security Domains Overview

When securing administrative accounts and the Veeam Availability Infrastructure installation you have a few options from most secure to less secure:

- Add the Veeam components to a management domain that resides in a separate Active Directory Forest and protect the administrative accounts with two-factor authentication mechanics.

- Add the Veeam components to a separate workgroup and place the components on a separate network where applicable.

- Add the Veeam components to the production domain but make sure the accounts with administrative privileges are protected with two-factor authentication.
Best Practice

For the most secure deployment add the Veeam components to a management domain that resides in a separate Active Directory Forest and protect the administrative accounts with two-factor authentication mechanics. This way the Veeam Availability Infrastructure does not rely on the environment it is meant to protect.

Windows Workgroup

When using a Workgroup, you will need to have everything carefully documented because of management and compliancy reasons. Every system needs to be configured independently per system with a local security policy, as well as users, permissions, etc. If you have multiple Veeam servers and users, this could become extremely cumbersome in larger environments. Also forget about Kerberos authentication with a workgroup server, you will be using NLTM instead.

Be aware though that a Workgroup is harder to defend against threats from the inside like a disgruntled employee, because you will be using local accounts on the workgroup servers, and you cannot just switch off a single AD account locking out that specific employee from the critical infrastructure. Also, it is harder to proof for compliancy reasons that the systems are safe and being utilized as they should be. A Workgroup setup is a good solution for small environments.

Pros

• Fast and easy to setup
• Separates Veeam accounts from Domain privileged accounts (helps against keyloggers and breach of the production domain)
• Does not rely on the environment it is meant to protect
• No additional infrastructure servers required like: Domain Controllers, NTP and DNS

Cons

• Large management overhead in large(r) environments
• No Kerberos communication when logging into a standalone server (workgroup) only NTLM
• Harder to become compliant, do compliancy checks and proof to be compliant as an organization
Management Domain

While this approach does add a forest to an Active Directory environment, the cost and complexity are limited by the fixed design, small hardware/software footprint, and small number of users. Enabling central management of policies, user rights and permissions makes management easy. It also enables one-click deactivation of a single AD account when you face an inside threat. Setting up a separate Forest with a management domain is a great solution for large(r) environments. You can also add multi-Factor authentication on the domain to protect the administrative accounts even further, blocking man in the middle attacks and key loggers.

Pros

• Easy to manage
• One-click deactivation of a single AD account
• Does not rely on the environment it is meant to protect
• Secure Kerberos communication between different Veeam components
• Use group policies to control the domain and fulfil compliancy easier
• Can integrate Multi-Factor Authentication (MFA) for extra layer of security

Cons

• Will need extra infrastructure components
• Needs more knowledge to set it up correctly

What type of trust?

Forest trusts help you to manage a segmented Active Directory Domain Services (AD DS) infrastructure and support access to resources and other objects across multiple forests. Forests trusts are useful for companies seeking a solution for administrative autonomy. Using forest trusts, you can link two different forests to form a one-way or two-way transitive trust relationship. A forest trust allows administrators to connect two AD DS forests with a single trust relationship to provide a seamless authentication and authorization experience across the forests.
If a one-way forest trust is created between two forests, members of the trusted forest can utilize resources located in the trusting forest. However, the trust operates in only one direction. In this example you want the production domain to trust the management domain with a one-way forest trust. You will have an incoming one-way forest trust on the management domain.
Segmentation using Zones

Ultimately, all security is about protecting assets, in this case it is Data, but that protection involves a defence-in-depth strategy that includes all layers. To do a defence-in-depth, you should identify the most valuable data and build layers of defence around it to protect its availability, integrity and confidentiality.

A zone is an area having a particular characteristic, purpose, use and/or subject to restrictions. By using zones, you have an effective strategy for reducing many types of risks. While securing your environment much granular and better, you will also lower costs associated with it. Instead of protecting everything with the same level of protection, you associate systems and information to specific zones. As a side effect, systems that are subject to regulatory compliance can be grouped in subzones to limit the scope of compliance checking and therefore, reduce costs and time needed to complete long-winded audit processes.

Think about the importance of the data and systems in that zone and who should have access to it. Communication is only allowed between systems in adjacent zones. A common data classification for a zone is about shared availability, confidentiality, integrity, access controls, audit, logging and monitoring requirements.

These common characteristics and requirements inherently lead to some level of isolation, but this isolation occurs not just between zones, but also within zones called subzones.

The attack surface of data and systems within a zone can be significantly reduced by exposing a limited number of services through the zone’s perimeter and implementing strict access controls to limit access to specific groups of users. A potential attacker would have to gain access to all the outer zones before getting to the restricted zone where the critical data is stored, reducing the likelihood of data theft or data mutilation. In addition, you are increasing the availability of these critical systems.

You could use a zone model as a strategic defence model which divides the different Veeam components into separate zones. Keep the following rules in mind while designing:

1. Secure by Design
2. Know what is important to secure and rank it
3. Know your attack vectors and possible ways to secure them
4. Use the principle of least privilege
5. Have insight in costs and benefits

**Important:** Be aware that there is no silver bullet that will solve all your security needs at once. There are numerous ways to achieve your goal. Security is a state of mind and needs to be looked after every single day. If you think you are secure, because you followed all best practices you got a false sense of protection. Look at your organization needs and then choose the best way that fits your organization taking into consideration money (budget), risks (attack vectors) and possible outcome (how does it fit in, what would be the damage).
Example using Zones

Implementing zones can be done in numerous ways depending on the approach you choose. But keep in mind that most of the threats nowadays are coming from the inside. Dividing your infrastructure into zones is a great way to provide better visibility into parts of greater importance. Without visibility it is sheer impossible to gain control and detect threats early. For hardening the Veeam Availability infrastructure components we place them in several logical zones.

One of the highest sought-after attack vectors will be gaining access to management accounts and components. This will allow an attacker to gain access to most parts of the infrastructure instantly. While overlooking the major Veeam Backup & Replication components you will notice that there are three management components available.

Let's place all major Veeam Availability components into the defined zones:

- The Veeam Backup & Replication Console also referred to as Console
- The Veeam Backup & Replication Server which is the core component orchestrating all different jobs and ordering movement of data through the infrastructure
- The Veeam Backup Enterprise Manager who federates multiple Backup Servers into a single pane of glass.
**Untrusted Zone**

To keep a balance between security and operational efficiency you do not want to install the Veeam Backup & Replication Console on any system outside your organization infrastructure. But for operational efficiency you want to give your administrators the ability to connect to the infrastructure from any device and any location through remote access with only keyboard, mouse and video to their disposal.

For operational efficiency, you do not want to install Veeam Backup Console on machines on poor connections/long distance, there can be between 50-400 MB of data transferred between the console and backup repository when starting the console. If the first file mount is performed over a slow connection, it may take a considerable time to load the file-level recovery wizard.

If there is significant latency between the backup repository and console, it is recommended to deploy an instance of the console on or closer to the repository server.

Deploy a firewall on the perimeter between the untrusted zone and the DMZ zone. On the firewall and/or dedicated RDS Gateway server add 2-factor authentication for remote administrators to access the RDS Gateway. Deny the mapping of drives, printers, clipboard etc. on the RDS Gateway to secure your infrastructure against dropping of content or files from any remote machine.

**DMZ**

The DMZ houses systems that require exposure to the untrusted zone. This zone proxies access between systems in the DMZ and the Management Zone. Also, all traffic should be funneled through systems in the DMZ to reach Internet resources. The systems deployed in this zone should be tightly controlled and hardened to reduce attack surface.

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. The console lets several backup operators and admins log in to Veeam Backup & Replication simultaneous and perform all kind of data protection and disaster recovery operations as if you work on the backup server.

Install the Veeam Backup & Replication console on a central management server that is positioned in the DMZ zone and make sure it’s protected with 2-factor authentication. You can also install other infrastructure tools on this management server like for instance the Microsoft VMM Console and/or VMware vSphere Client to manage your hypervisor deployment.

The Veeam Enterprise Manager will also be in the DMZ zone, because it serves as a Self-Service portal for specific user-groups in the organization.
Management Zone

In the management zone, you place infrastructure services like DNS, Active Directory and SMTP. But also, the VMware vCenter server and/or Microsoft System Center Virtual Machine Manager (SCVMM). From the Veeam components the Veeam Backup & Replication Server(s) will be in this Management zone. The Veeam Backup Server will orchestrate all jobs and update all Veeam components in the different zones from a central location.

The Microsoft SQL Database server, which is needed to host the Veeam Backup Database and the Veeam Enterprise Backup Database should be placed in this zone if it is dedicated just for Veeam. It is a good practice to use a dedicated SQL server which hosts the different SQL instances for infrastructure components and a different SQL server for SQL instances for business processes. The Veeam Backup & Replication server is a heavy user of the SQL server and placing the SQL database server close by gains you operational efficiency.

The VMware vCloud Director is part of a subzone within the management zone and controls the vAPP’s running in subzones within the Trusted Zone.

The management zone requires secure and controlled access to the internet to download licenses and updates for different components in the infrastructure. It is highly recommended to use an Internet Proxy or Reverse Proxy situated in the DMZ as a controlled gateway to the internet.

All types of Cloud Repositories should be placed in subzones within the Untrusted zone. Organization data is leaving the security boundaries so make sure that, as an extra precaution, data towards these cloud repositories is encrypted during transport and when stored in the cloud repository. The Veeam Backup & Replication server will communicate with the Cloud Gateway service for transport of data to the Cloud Provider, Azure Proxy or AWS deployment.

Trusted Zone

The trusted zone will be populated with hypervisor hosts like VMware ESXi and/or Microsoft Hyper-V hosts. All components in the Trusted zone will need access to different services in the Management zone. The Veeam Proxy servers, which are the data movers, are part of the trusted zone.

Veeam Proxies can back up the VMs without having access to the Guest OSes themselves. If you back up or replicate running VMs, you can enable guest processing options. Guest processing options are advanced tasks that require Veeam Backup & Replication to communicate with the VM guest OS. When VMs are separated in subzones you can deploy and leverage the Veeam Guest Interaction Proxy (GIP) in the Trusted Subzone, which will have secure access and deploys the needed runtime in the VM for guest processing tasks.
In the case that different business units or customers are running in the trusted zone you should think about running them in subzones of the trusted zone. But be aware that overly complex designs can be counterproductive and give a misplaced feeling of being safe.

VMware vCloud Director vAPP’s are also part of the Trusted Zone and would normally be divided in subzones per business unit or tenant. Veeam can capture whole vAPP and vCloud Director configurations within the backup jobs.

**Restricted Zone**

Primary storage, where production data and VM’s reside, but also other components which store data should be placed in this restricted zone. This zone should never be accessible by any user directly. Only available to the virtual infrastructure components and application servers and administrators with strict rights. Also, the Veeam Scale Out Backup Repository (SOBR), Simple Repository, Deduplication devices or Cloud Repository when used in combination with Veeam Cloud Connect for Enterprise (VCC-E) should be part of this zone. For organizations using VCC-E it is possible to define cloud repositories on top of their SOBR or as separate defined cloud repositories in a Restricted Zone subzone.

**Audit Zone**

Visibility is key to protect, detect and contain threats early. In this zone monitoring solutions like Veeam ONE and/or Veeam Management Pack in combination with Microsoft System Center are placed. IDS and IPS systems should be placed in this Audit zone.
Hardening Backup Repository — Windows

If you have no choice but using a windows repository beside a strongly secured repository, there are still some rules to secure it as much as possible.

A good way of hardening the backup repository is by running it on a standalone Windows Server with storage attached to it. Create/Use a local account with administrative access and make sure only this (newly created) account has access rights to the location where the backup files are being stored. Veeam needs a local account with administrative access to function properly.

Best Practices for Hardening Veeam Backup Repositories based on Windows are:

1. K.I.S.S. design — Keep It Simple and Straightforward.
2. Use a standalone Windows Server which is not part of any Active Directory Domain.
3. Make sure the repository servers are physically secured.
4. Use a local account with administrative access
5. Set permissions on the repository directory to only that local account.
6. Modify the Firewall, with dedicated rules for Veeam to allow access to specific ports.
7. Disable remote RDP services to the repository servers.
8. Use Veeam encryption while storing backups on the repository.

Standalone and Physically secured

When protecting the whole environment, you do not want the Veeam repository to be tied to the same Windows Active Directory domain you are protecting with the backup. Otherwise, if everything is lost you could have a chicken and egg problem around accounts wanting to authenticate against a domain which is no longer available.

Furthermore, if a Domain Admin account is compromised you do not want that account to be able to overrule a backup repository account password so the hacker gets access to the backup files together with access to the whole environment.

Place the repository servers in a Restricted Zone, because these servers contain a 100% copy of your production environment! The repository servers should be physical secured and have appropriate access control systems in place. This way access is restricted, who does have access is registered and monitored at certain specified levels.
Local Account with administrative access

The easiest and best way to leverage a local account with administrative access to the repository server is by using the built-in Local Administrator account. As an extra precaution make sure you rename the account, so a potential hacker has to guess the account name and the password. By using local Account specific per Veeam Backup Repository server you increase the level of protection. If one of those accounts get compromised the other repository servers stay secure.

When your organisation does not allow you (e.g. global security policy) to use the built-in local administrator account, you can create a new local account and give it administrative access. Make sure the Local Administrator account is highly secure in this case.

Note: UAC affects connections for nondomain/local user accounts. If you connect to a remote computer using a nondomain/local user account included in the local Administrators group of the remote computer, then you must explicitly grant remote DCOM access, activation, and launch rights to the account. User Account Control (UAC) access-token filtering can affect which operations are allowed or what data is returned. Under UAC, all accounts in the local Administrators group run with a standard user access token, also known as UAC access-token filtering. An administrator account can run a script with an elevated privilege “Run as Administrator”. Some securable objects may not allow a standard user to perform tasks and offer no means to alter the default security. In this case, you may need to disable UAC so that the local user account is not filtered and instead becomes a full administrator. One important thing to know is that UAC is not a security boundary. UAC helps people be more secure, but it is not a cure all. UAC helps most by being the prompt before software is installed. This part of UAC is in full force when the “Notify me only when...” setting is used. UAC also prompts for other system wide changes that require administrator privileges which, considered in the abstract, would seem to be an effective countermeasure to malware after it is running, but the practical experience is that its effect is limited. For example, clever malware will avoid operations that require elevation. Be aware that for security reasons, disabling UAC should be a last resort.

The downside of creating a newly administrative local account is that you will need to disable Remote User Account Control (UAC) because this Windows function prevents local accounts from running in an elevated mode when connecting from the network. Veeam accesses the ADMIN$ and C$ through the Installer Service with the local account you presented while adding the Windows server to Infrastructure in Veeam Backup & Replication.

The connection will fail with the following error message: Access is denied -tr:Error code: 0x000000051 -tr:Failed to create persistent connection to ADMIN$ shared folder on host [host name or ip-address] -tr:Failed to install service [VeeamDeploySvc] was not installed on the host [host name or ip-address] when Remote UAC is Enabled on the Windows Server.
UAC Error 0x00000005

or with the error message: RPC Client is not a member of built-in Administrators group. -tr:Error code: 0x80070005 when the server was already added as a Veeam Backup Repository through Infrastructure within Veeam Backup & Replication.

RPC Error 0x80070005

The Veeam Installer service pushes the Veeam binaries through the ADMIN$ and C$ share on the target machine. It also uses administrative shares later for other jobs.

You can disable Remote UAC on the repository server by using REGEDT32 to navigate to the following registry path:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Add a new Key with type DWORD (32-bit) Value and name it LocalAccountTokenFilterPolicy give it a value of 1. No restart is needed.

Set permissions on the repository directory

Login with the newly created local account or with the renamed local administrator and open File Explorer, locate the disk(s) where the backup files will be placed (or are already there in an existing deployment). Open the properties of the disk and Add the used account and give it Full access. Tick all Allow boxes.

Remove all accounts except the SYSTEM and the account you are using.

**Important:** the SYSTEM group account can also be removed, but then the Veeam services need to start with the local administrative account used instead of Local System otherwise the backups will fail. Keep the K.I.S.S. principle in mind here.

After adding the used administrative account on the security tab of the disk(s) where backups will reside. Open the advanced security settings and Change the Owner. When there are already backup files on this disk make sure to tick the box: Replace all child objects permissions entries with inheritable permissions entries from this object.
Modify the Firewall

You have three options to make the first install of Veeam components, pushed from the Veeam Backup & Replication server, a success. From most preferred to least preferred option:

2. Keep Windows Firewall On and manual install the Veeam Installer Service (VeeamDeploySvc)
3. Switch Windows Firewall Off and enable File and Printer Sharing during the first install

Option 1 — Windows Firewall On and add three new firewall rules From a command prompt run the following three commands to add three new rules to the Windows Firewall:

```
netsh advfirewall firewall add rule name="Veeam (DCOM-in)" dir=in action=allow protocol=TCP LocalPort=135 enable=yes program="%systemroot%\system32\svchost.exe" service=RPCSS remoteip=<VBR Server IP-address>
```

```
netsh advfirewall firewall add rule name="Veeam (SMB-in)" dir=in action=allow protocol=TCP LocalPort=445 enable=yes program="System" remoteip=<VBR Server IP-address>
```
After adding these firewall rules nothing else has to be done to the Windows server to be added to the Veeam Infrastructure components. You also do not have to switch on File and Printer Sharing specifically.

**Tip:** You can also store these three commands in a windows bat file and run that on every Windows server you are preparing to use as a Veeam Infrastructure component.

**Option 2** — Windows Firewall On and manual install of Veeam Deployment Service

Open the CMD utility on the repository server and create a folder C:\Windows\Veeam\Backup

```bash
mkdir C:\Windows\Veeam\Backup
```

Copy two files named: VeeamDeploymentDll.dll & VeeamDeploymentSvc.exe from the Veeam Backup & Repository server path C:\Program Files\Veeam\Backup and Replication\Backup\Packages

**Tip:** Use TAB key for auto completion.

Run on the Veeam repository server in the directory C:\Windows\Veeam\Backup through CMD the following command: VeeamDeploymentSvc.exe -install this way the Veeam installer service will be installed. Veeam will add Firewall rules for Veeam during installation, which are visible as Veeam Networking in the firewall under Allowed apps and features.

Veeam Network Firewall Rules

**Tip:** This manual install process can be interesting for so called ‘Dark Sites’. With the command: VeeamDeploymentSvc.exe -uninstall you can remove the installation services.

**Option 3** — Windows Firewall Off and enable File and Printer Sharing

Disable the Windows Firewall for the Private Networks during the initial Veeam installation. This way the right binaries gets pushed to the Windows repository server. Veeam will add Firewall rules for Veeam during installation, which are visible as Veeam Networking in the firewall under Allowed apps and features. After the process completed successful make sure you enable the Windows Firewall again!
Disable remote RDP services

Veeam Backup Repositories are (most) often physical. An extra security measure is to disable any remote RDP access in Windows and use a KVM-over-IP switch to access this machine remotely in the datacenter.

1. Error code 0x00000005 refers to Remote UAC and local administrative account but not the original local administrator, code 0x00000040 refers to Server service stopped/crashed no administrative shares available, 0x00000057 multiple same usernames in Veeam credentials manager with different passwords.
WORM Storage with Hardened Repository

Veeam Hardened Repository is a WORM storage solution that protects against unwanted changes to the backup files. It's available since version 11. Veeam Hardened Repository passed an external audit for WORM storage and meets highest compliance standards.

For general information on the Hardened Repository on Linux, please see the user guide.

As a reminder or complement to the user guide, consider the following actions to create a hardened repository.

Deploy Veeam repository using single use credentials

Veeam will not store repository root account, keeping backup files safe if the Veeam Backup server is compromised.

Do not forget to remove the user from sudoers group after installation.

Disable SSH after deployment

SSH connection is necessary only for deployment or upgrade of Veeam data mover. After Veeam has been deployed, it is possible to disable SSH for better security.

If you keep SSH enabled, then MFA on SSH shall be considered.

Beware of IPMI

Any management tool, such as ILO or DRAC can be used to access the repository, and even to wipe the hard drives. It is strongly recommended to unplug these tools from the network when not in use.

NTP

Time management is crucial when speaking about immutability.

It is not advised to use public NTP servers, since it would mean internet exposure of the repository server. Using your own NTP server is an option, but still a security breach in case an attacker takes control of it.

Using CMOS clock is an advised option, but the counterpart is to regularly check and manually set system time. Also, a time difference between the repository and the backup server would make logs analysis more complex by forensics.

A second advised and interesting option is to use a DCF77 (or locally equivalent) dongle with XNTP package to synchronize the repository on long wave signal.