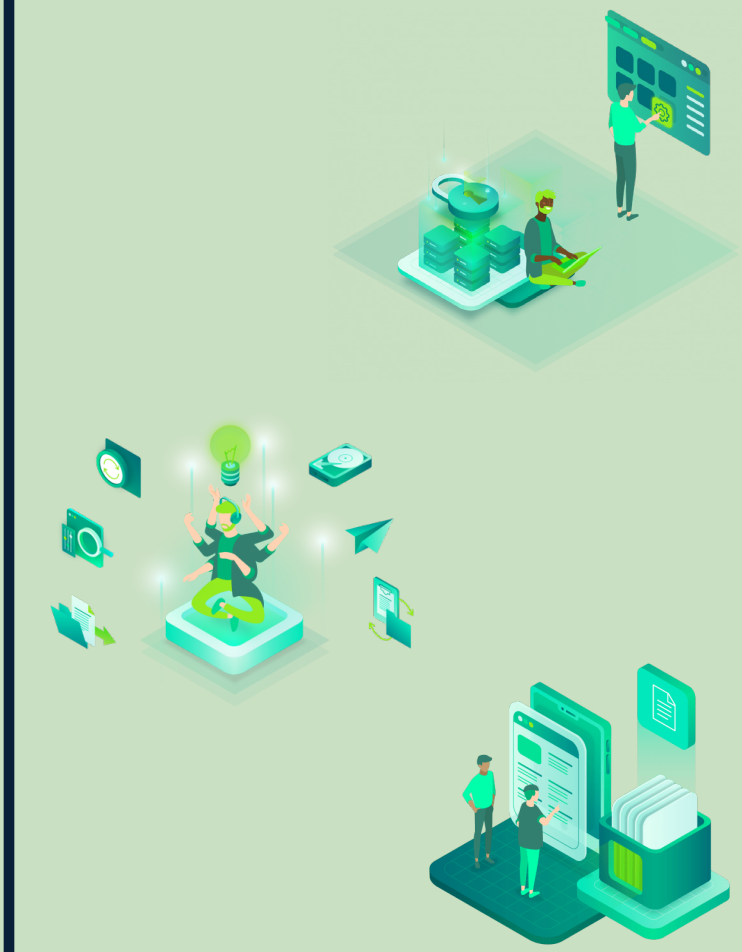
CCN-CERT

BP/34



Security Recommendations on Veeam Data Platform

BEST PRACTICE REPORT

APRIL 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional

Edited by:

Date of issue: april 2024

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained herein, expressly rejecting any type of implicit guarantee that may be related to it. Under no circumstances can the National Cryptologic Centre be held responsible for direct, indirect, fortuitous or extraordinary damage derived from the use of the information and software indicated, even when warned of such a possibility.

LEGAL NOTICE

The reproduction of all or part of this document by any means or process, including reprography and computer processing, and the distribution of copies by public rental or loan, is strictly prohibited without the written authorisation of the National Cryptologic Centre, subject to the penalties established by law.

Foreward

In an increasingly complex and globalised world, in which information and communication technologies (ICTs) play an extremely important role, we must be aware that the proper management of cybersecurity is a collective challenge that we must necessarily face. It is necessary to ensure the protection of our country's economic, technological and political capacity, especially when the proliferation of targeted attacks and the theft of sensitive information is an undeniable reality.It is therefore essential to keep abreast of the threats and vulnerabilities associated with the use of new technologies. Knowledge of the risks that loom over cyberspace must serve to implement with guarantees the measures, both procedural and technical and organisational, that allow for a safe and reliable environment.

Law 11/2002, of 6 May, regulating the National Intelligence Centre (CNI), entrusts the National Intelligence Centre with the exercise of functions relating to the security of information technologies and the protection of classified information, while at the same time conferring on its Secretary of State Director the responsibility of directing the National Cryptologic Centre (CCN).Based on the CNI's knowledge and experience of threats and vulnerabilities in terms of emerging risks, the Centre carries out, through the National Cryptologic Centre, regulated by Royal Decree 421/2004 of 12 March, various activities directly related to ICT security, aimed at training expert personnel, the use of appropriate security technologies and the application of security policies and procedures.

We must be aware that the proper management of cybersecurity is a collective challenge that we must necessarily face.

Precisely, this series of CCN-STIC documents is a clear reflection of the work that this body carries out in terms of security implementation, enabling the application of policies and procedures, as the guides have been drawn up with a clear objective: to improve the degree of cybersecurity of organisations, aware of the importance of establishing a reference framework in this area to support government staff in carrying out the difficult task of providing security for the ICT systems under their responsibility.

With this series of documents, the National Cryptologic Centre, in compliance with its tasks and with what is reflected in Royal Decree 3/2010 regulating the National Security Scheme in the field of electronic administration, contributes to improving Spanish cybersecurity and maintaining the infrastructures and information systems of all public administrations with optimal levels of security. The aim is to generate confidence and guarantees in the use of these technologies, protecting the confidentiality of data and guaranteeing its authenticity, integrity and availability.

April 2024

Esperanza Casteleiro Llamazares

Secretary of State
Director of the National Cryptologic Centre

Index

1. Introduction

Veeam provides enterprises and organisations with a unified platform for protecting cloud, virtual, physical, SaaS and Kubernetes environments.

It provides a unified platform for the protection of diverse environments, centrally managed and adaptable to different architectures.

The main elements that make up the solution are:

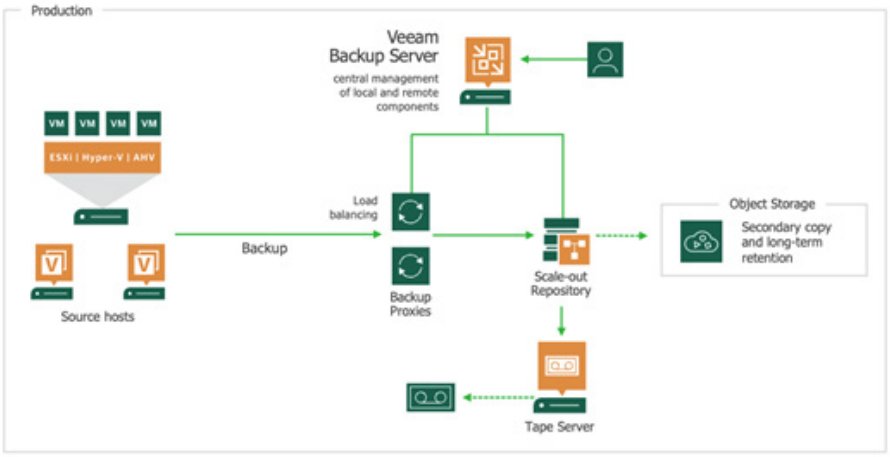
- **Veeam Backup Server:** is the central element that allows you to configure and manage the rest of the components of the solution.
- **Veeam Backup Proxy:** The main function of the proxy server is to read data from the production environment and process it in order to send it to the backup repository.
- **Veeam Repository Server:** The repositories are responsible for storing the backup images and metadata.

All metadata information is self-contained in the backup itself (in the local repository and also in the copy that overflows to the cloud), so no index, volume or deduplication database stored on the backup server is required. This provides advantages in case of recovery from a total or partial disaster in the local data centre.

It is important to mention that, depending on the needs or size of the infrastructure, these components can be installed in a single device (all-in-one installation) or decoupled in different devices.

1. Introduction

A possible high-level architecture of the solution could be the following:



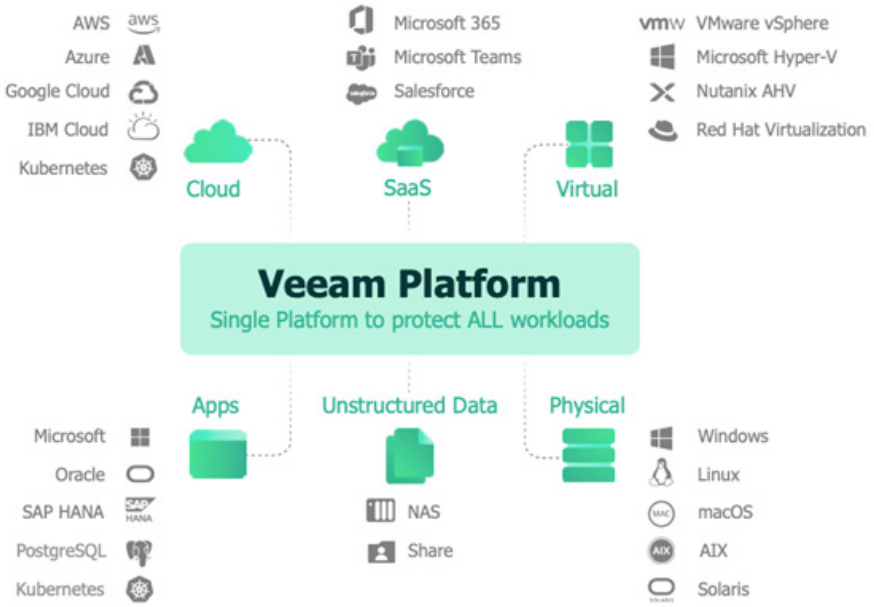
The diagram shows:

- The multiple data sources that Veeam supports. Virtualised environments, physical servers, NAS environments or file servers, among others.
- At the heart of the copying process are the backup proxies, which read and process the source data and send it to the backup repository, compressed and deduplicated.
- On the right side of the image is the backup repository. This will usually be local in order to provide the solution with high performance in both the backup generation and restore processes. It is possible to replicate or extend the repository, either locally or in the cloud, in order to follow the typical 3-2-1 rule that any backup solution should apply.
- Optionally, it is feasible to outsource the copies to tape, thus guaranteeing the availability of these offline and even in different facilities.
- All centrally managed by the Veeam Server through a protected console with multi-factor authentication mechanisms to help meet technical and regulatory requirements.

2. Ransomware, resilience and security

Veeam Data Platform is modular and extensible, which means it can offer virtual and physical protection in on-premises environments, cloud-native protection in AWS, Azure and Google Cloud environments, Kubernetes anywhere, as well as SaaS protection for Microsoft 365 and Salesforce environments.

Provides complete protection for virtual, physical, SaaS and Kubernetes environments, with agentless backup options and advanced anti-ransomware measures.



- **Virtual loads.** Veeam allows you to perform an image backup, both at virtual machine and application level, without the installation of any type of agent, neither for the copy nor for the restore.

  In the case of databases (Microsoft SQL Server, PostgreSQL or Oracle), Veeam also allows you to protect transaction logs on a regular basis, without installing agents.

- **Physical loads.** Veeam allows the protection of Windows, Linux, MAC, AIX and Solaris physical machines by means of Veeam Agents. To do this, a single agent must be installed on the system to protect the server as a whole (the operating system, folders and applications).

  Agents will be centrally managed from the Veeam server and data travels directly from the server to the backup repository and as with virtual loads, to protect the organisation's data, the entire backup process is encrypted end-to-end (source, network and destination).

- **NAS / File Server uploads.** The NAS Backup functionality is used for the protection of file environments (NAS or Windows/ Linux File Servers, physical or virtual).

  The backup of the NAS devices (SMB/CIFS and NFS) is done through the local network and the data is processed by the File Proxies which will process the data and send it directly to disk.

- **Kubernetes-based container loads.** Veeam's K10 is purpose-built for Kubernetes and provides operations teams with an easy-to-use, scalable and secure system for backup and restore, disaster recovery and Kubernetes application mobility.

  It natively integrates with Kubernetes to automatically discover all application components running on the cluster and treat the application as a unit. It also features Multi-Tenancy support with integrated security, multi-cluster management and ransomware protection by supporting immutable object storage.

- **Cloud-native workloads.** Another possible approach is to perform modular, cloud-native backup and recovery to protect specific AWS, Azure or Google Cloud workloads.

  Cloud-native backup can be deployed independently or integrated into more comprehensive deployments with the Veeam platform, unifying data protection capabilities in hybrid or multi-cloud environments and advanced data management in a single interface, enabling broad cross-platform data mobility.

2. Ransomware, resilience and security

Ransomware attacks are one of the most serious and frequent threats to organisations today. Having a solid defence, a robust data protection strategy and proven, agile recovery plans are the best way to protect against this type of threat.

Validated and verified backups are the last line of defence against cyber-attacks and can be the decisive factor in avoiding significant downtime, data loss and negative impact on the business and reputation of organisations.

It is recommended **when planning backups to follow the 3-2-1-1-0 rule.** This is an enhancement implemented by Veeam to the well-known 3-2-1 rule.

With the **3-2-1-1-0 rule**, the suggested practice is to have **(3) different copies** of the data, on (2) different **types of media, (1)** of which is located at an **offsite location, (1)** of which is **offline, isolated or immutable**, and which has **(0) backup errors**, as they have been previously tested and automatically verified as recoverable.

A **robust and comprehensive cyber defence strategy** always starts with backups and these must be reliable, verified and tested. Furthermore, immutability is a key step that will prevent cybercriminals from accessing, encrypting or deleting backup data.

Immutability provides the **protection of offline storage in** a WORM (Write Once, Read Many) fashion, making backup data impenetrable to attacks. Various immutability options are possible in the public cloud (AWS, Azure, Wasabi, etc.), as well as object lock-compatible S3 repositories for immutability in the local environment, not to mention tape backup options.

3. Veeam security best practices

3.1 Protect

3.1.1 Protecting backups - the 3 2 1 1 0 rule

A properly designed backup infrastructure must include a data protection mechanism. This can be provided by features such as:

- Deduplication appliances through proprietary mechanisms such as immutability or protected snapshots.
- Storage of objects, through Immutability.
- Tape devices, with physical air gapping.
- Through WORM (Write Once, Read Many) mechanisms.

It is recommended to **protect all retentions by air gap or immutability**. As the persistence time of attackers is approximately one month on average, it is essential to protect at least **four (4) weeks of restore points** to mitigate the attack.

Following the **3-2-1-1-0 rule** creates multiple layers of resilience and security. Data and workloads will be made immutable (protection against deletion and modification), stored off-line (protection against internal threats) and an air-gap (protection against internal and external threats and other business continuity disasters, such as fire, flood, earthquakes, etc.) will be available.

Additionally, it is possible to add what is called a **protocol break**, to make it more difficult for attackers to destroy data. It consists of using different types of repositories, based on different technologies (disk block, CIFS, NFS, S3, proprietary deduplication device protocols, etc.), thus making it more difficult for attack tools to target the data.

3.1.2 Protecting the backup infrastructure

It is recommended to protect the Veeam infrastructure by applying **countermeasures such as bastioning or hardening** of components. At least the protection should take into consideration the following:

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

The backup solution must be considered a **prime target for attacks on an infrastructure.** Its access must be highly restricted, and both its access and its deployment must be controlled at all times.

Backup proxies should be considered as a **target for data compromise**. During the backup generation process, proxies obtain from the backup server the credentials needed to access the virtual infrastructure servers. A user with administrator privileges on a backup proxy can intercept the credentials and use them to access the virtual infrastructure.

3.1.3 Staff training

Through awareness-raising actions and training, employees' ability to **detect strange behaviour** and their awareness of their fundamental role in the protection of the organisation's services and data is significantly increased.

This applies not only to the IT department, but to all users in an organisation, as they can all **witness suspicious behaviour, or be socially engineered and potentially open a security breach** if they do not have the proper security training and awareness.

3.2 Threat detection

3.2.1 Surveillance

To know when you are under attack or have suffered a security breach, it is vital to have **visibility of the entire data flow path**. You must be able to differentiate between abnormal behaviour and non-abnormal behaviour. To do this, it is recommended to monitor your Veeam accounts and infrastructure for suspicious activity.

One of the most effective measures is the setting of **virtual traps**, such as the creation of an unused administrator account with alarms linked to it (e.g. Honeypot users). When any activity is observed on that account, an alert will be triggered instantly.

It is important to be alerted as early as possible to defend against other attacks such as viruses, malware and ransomware. The greatest danger of these is the ability to spread quickly to other systems. **Being vigilant about, for example, possible ransomware activity is critical.**

3.2.2 Honeypot servers

Honeypot servers or decoy servers with authentication monitoring can help detect attacks targeting the Veeam infrastructure. These decoys should be visible, and their DNS entries should be understandable, such as vbrsrv01 or vbrrepo, thus appearing as easy targets for the attacker.

A suitable decoy could include a fake repository, where changes to backup files are closely monitored.

3.2.3 Honeypot users

Honeypot users with authentication monitoring also help in the detection of attacks targeting the Veeam infrastructure. As in the case of decoy servers, these users must be visible and their names very understandable, such as VBRAdmin or BackupAdmin, in order for them to be considered by the attacker as potentially accessible targets.

Of course, **these users** must be **configured to render their exposure and possible malicious exploitation useless**, so that their compromise has no effect on the security of the organisation's infrastructure.

3.2.4 Alarms

Veeam One offers the possibility to monitor possible ransomware activity through a set of **predefined alarms such as immutability status, possible ransomware activity or immutability change tracking.**

These alarms must be triggered on both the production server and the honeypot.

3.3 Recovery strategy

Having a recovery strategy and knowing how to act when an incident occurs is key to minimising the impact of an incident and the associated economic losses. Logically, among the fundamental recommendations is to **make backup copies of the data, ensuring that an attacker cannot access to delete or alter them.**

In this sense, external (air-gap) or read-only copies on any media are highly recommended. In addition, it is necessary to be aware that in case of a report to law enforcement agencies, it is very likely that the assets will be sealed by governmental entities for analysis or forensic analysis and therefore will not be available for recovery. It is therefore advisable to **have dedicated recovery hardware and to keep copies off-site.**

It is also very likely that the **internet connection will be disabled as a method of expelling the attacker** and/or preventing data leakage. Therefore, an alternative way of accessing external backups may be necessary.

Preparation is the key. In short, having tested the recovery taking into consideration that the reboot will have to be performed only from backup files and zero-based infrastructures.

Other recommendations to consider are: **having the response team prepared**, knowing which assets to **prioritise in the recovery,** as well as making appropriate use of testing and automation tools, such as Veeam SureBackup or Veeam Disaster Recovery Orchestrator.

3.4 Roles and users

Controlling access to management tools is crucial to maintaining good security practice. The **principle of least privilege** should be **used** in all cases.

An attacker gaining access with elevated privileges to the servers of the backup infrastructure can obtain user account credentials and compromise **other systems in your environment** or exploit recovery procedures.

It is therefore necessary to ensure that **all accounts have specific and controlled roles and permissions**. Some recommendations in this regard are:

- Do not use user accounts for access with administrative privileges.
- Provide each Veeam administrator with their own specific account with administrative privileges, to facilitate traceability, adding and deleting.
- Remove the default role Veeam Backup Administrator from the Local Administrators group.
- Grant only the access necessary for the work to be done for as long as it is necessary (JIT).
- Strictly limit the users that can log in via Veeam Console.
- Add two-factor authentication to high-value assets.
- Monitor accounts for suspicious activity.

3.4.1 Non-predictable accounts

Many companies and organisations follow good practice in using dedicated accounts for administrators to perform privileged tasks independent of their user account, which allows them to perform basic office tasks.

These accounts are often prefixed with adm_, which can be useful, but helps attackers to identify privileged accounts. **It is advisable to use adm_ accounts only for honeypot users and to choose another naming strategy for real admin accounts.**

Social media can also assist in the identification of a potential owner of a privileged account within a company or organisation. It is therefore recommended to avoid the use of the user's name, thus adding complexity to the identification of privileged accounts.

3.4.2 Password management policy

It is recommended to use a **functional but smart password management policy.** Enforcing the use of strong passwords throughout the infrastructure is a must, making it difficult for attackers to discover passwords or crack hashes to gain unauthorised access to critical systems.

It is also necessary to **verify that default accounts and passwords have been changed regularly** for all assets. For administrative accounts, it is imperative to **add two-factor authentication (2FA)** for additional infrastructure protection.

It is recommended to verify that the password tool and database are available at a **recovery site** so that they are available in the event of a disaster or critical incident. A recent backup of the password tool and database must reside on air-gap protected media, such as DVD, CD-ROM or tape. Most crucial is the Veeam Repository password that allows restoration from backup files.

Access to production systems from the backup infrastructure can be based on **Group Managed Service Accounts (gMSA)** to facilitate the achievement of a good level of security, as **complex passwords are** then **automatically set and rotated**. Group Managed Service Accounts can be used with Veeam Backup and Replication from version 12.

3.4.3 Blocking policy

The use of a **lockout policy** that complements a smart password management policy is recommended. Accounts will be locked after a limited number of incorrect attempts. This can **stop password guessing attacks.**

It is necessary to consider that this policy **may also block the backup and replication system** for a while. For service accounts, it is sometimes preferable to generate an alarm quickly rather than locking accounts. This provides visibility into suspicious behaviour towards data or infrastructure.

3.4.4 Permits required

As indicated above, it is recommended to follow the **principle of least privilege,** i.e. to provide the minimum permissions necessary for user or service accounts to function.

3.5 Authentication protocols

It is recommended to choose **strong encryption algorithms for SSH**. To communicate with Linux servers deployed as part of the backup infrastructure, Veeam Backup & Replication uses SSH. For the SSH tunnel it is recommended to use a **robust and tested encryption algorithm** with sufficient key length. It is necessary to ensure that the private keys are stored in a secure location and cannot be discovered by third parties.

Since Veeam Backup & Replication v12, a Kerberos-only architecture is possible, so **it is recommended to disable NTLM authentication whenever possible.**

3.6 Encryption

3.6.1 At rest

Veeam Backup & Replication's built-in encryption should be used to protect backup data. In addition, to set up such encryption, it is recommended to follow the best practices for encryption at rest:

- **Secure passwords** that are difficult to crack or guess.
- **Keep passwords** in a safe place.
- **Change passwords** for encrypted jobs regularly.

3.6.2 In transit

Backup and replication data can be intercepted in transit, when communicating from source to destination over a network. To protect the communication channel of backup traffic, it is necessary to take these guidelines into account:

- **Isolate backup traffic.** Use a segmented network to transport data between the components of the backup infrastructure: backup server, backup proxies, repositories, etc.
- **Encrypt network traffic.** By default, Veeam Backup & Replication encrypts network traffic travelling between public networks, but it is recommended to enable encryption of traffic on private networks to ensure secure communication of sensitive data within the boundaries of the same network.

3.7 Bastioning

Bastioning is about protecting the infrastructure against attacks by reducing the attack surface and minimising the risk as much as possible.

One of the main steps for hardening is the **removal of all non-essential software and utilities from** the deployed Veeam components. Although these components may provide useful functions for the administrator, if they provide additional access to the system they should be removed during the hardening process.

Setting up monitoring and event logging of what happens in the infrastructure is part of infrastructure hardening. It is recommended to verify that it is possible to detect when an attack may occur or has occurred and then confirm that the logs and traces are saved for use by law enforcement agencies and security specialists if needed.

Making it more difficult and therefore slower for attackers to operate is always an objective to consider. Thus, **naming backup infrastructure servers using** unrelated **names** is a good strategy. Avoiding names containing acronyms such as bkp, pxy, repo, vbr or any name that might make it easier to identify the backup infrastructure components is part of this strategy.

3.7.1 Segmentation

A good strategy is to design a **defence-in-depth framework that includes all layers**. To do this, the most valuable data must be identified and layers of defence built around it to protect its availability, integrity and confidentiality.

A zone is an area that has a particular characteristic, purpose, use and/or is subject to particular restrictions. Instead of blanket protection at the same level, systems and information are associated with specific zones and those systems that are subject to regulatory compliance can be grouped into sub-zones to limit the scope of compliance checking and thereby reduce the costs and time required to complete lengthy audit processes.

It is necessary to think about the importance of the data and systems in that particular zone and who should have access to them. **Only systems in adjacent zones should be allowed to communicate with each other.** A common data classification for a zone refers to the requirements of shared availability, confidentiality, integrity, access controls, auditing, logging and monitoring.

These common characteristics and requirements inherently lead to a certain level of isolation, but this isolation occurs not only between zones, but also within zones called sub-zones.

The attack surface of data and systems within an area can be **significantly reduced by exposing a limited number of services** across the perimeter of the area and implementing strict **access controls,** limiting access to specific groups of users. A potential attacker would have to access all outside zones before reaching the restricted zone where critical data is stored, reducing the likelihood of data theft or mutilation. In addition, the availability of these critical systems is increased.

It is possible to use a **zone model as a strategic defence model** that divides the different Veeam components into separate zones. It is recommended to take the **following rules into account during the design:**

- **Insurance by design.**
- **Identify what is important, add security and classification.**
- **Know the attack vectors and possible forms of protection.**
- **Use the principle of least privilege.**
- **Have a view of costs and benefits.**

There is no exact formula that solves all security needs at once. There are many ways to achieve the objective. One should not believe that an environment is secure because all good practices have been followed, then one would have a false sense of protection.

The organisation's needs must be analysed and the best way to meet them, taking into account budget, risks (attack vectors) and possible outcomes (what would be the damage).

3.7.2 Layers between zones

Each of the adjacent zones can be assessed through the **seven (7) layers of the cyber security model:**

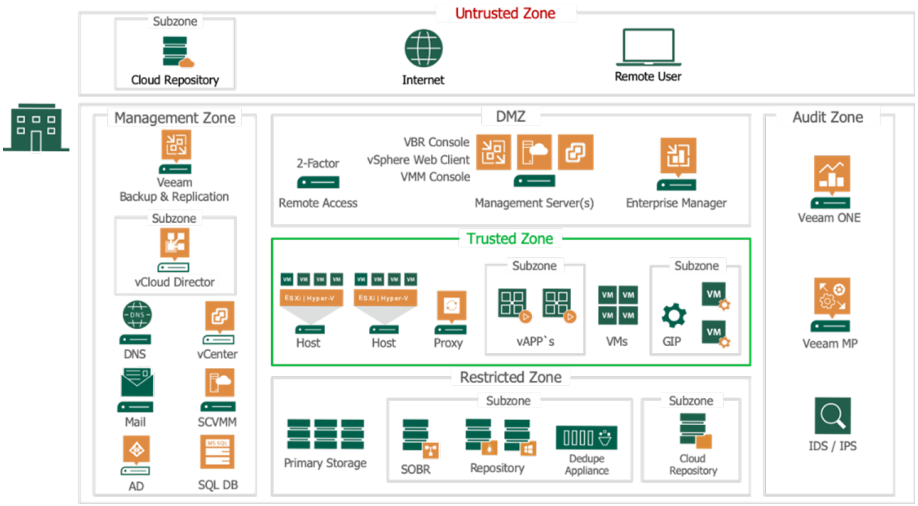
- **Human layer:** training, physical access...
- **Perimeter:** firewalls, spam filters, intrusion detection/prevention...
- **Network:** secure design and topology, VLANs, multilayer firewalls/ switches...
- **Endpoint:** antivirus, software firewalls, breach detection agents...
- **Applications:** patches, updates,...
- **Data:** encryption at rest and in transit.
- **Mission Critical:** backup, response and recovery plan.

3.7.3 Examples using zones

Nowadays most threats come from the inside, so it is recommended to divide the infrastructure into zones to provide better visibility of the most important parts. To strengthen the security of Veeam Availability infrastructure components, they are placed in several logical zones.

One of the most targeted attack vectors will be **gaining access to accounts and management components.** In Veeam Backup & Replication there are three (3) management components available.

- Veeam Backup & Replication Console, also referred to as Console.
- Veeam Backup & Replication Server is the central component that orchestrates all the different tasks and organises the movement of data across the infrastructure.
- Veeam Backup Enterprise Manager, which federates multiple backup servers into a single management console.



3.7.3.1 Untrusted Zone

To maintain a balance between security and operational efficiency, **it is not desirable to install Veeam Backup & Replication Console on any system outside the organisation's infrastructure.**

It is recommended to **deploy a firewall at the perimeter** between the untrusted zone and the DMZ. On the firewall and/or on the dedicated RDS gateway server, add **two-factor authentication to** allow remote administrators to access the RDS gateway.

The mapping of drives, printers, clipboards, etc. on the RDS gateway must be **restricted and denied to** protect the infrastructure against downloading of content or files from any remote machine.

3.7.3.2 DMZ

The DMZ hosts **systems that require exposure to the untrusted zone.** This zone allows access between systems in the DMZ and the Management Zone.

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. The console allows multiple backup operators and administrators to log in to Veeam Backup & Replication simultaneously and perform all types of data protection and disaster recovery operations as if they were working on the backup server.

The Veeam Backup & Replication console can be installed on a **central management server that is located in the DMZ zone,** protecting it with **two-factor authentication (2FA).** It is also possible to install other infrastructure tools on this management server, such as Microsoft VMM Console and/or VMware vSphere Client to manage the hypervisor deployment.

If required, Veeam Enterprise Manager can also be installed in the DMZ zone, as it serves as a **self-service portal for specific user groups** in the organisation.

3.7.3.3 Management Zone

In the management zone, **infrastructure services such as DNS, Active Directory and SMTP** are placed. But also the VMware vCenter server and/or Microsoft System Center Virtual Machine Manager (SCVMM).

Of 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,** required to host the Veeam backup database and the Veeam Enterprise backup database, **should be placed in this zone if it is dedicated to Veeam only.** It is a good practice to **use a dedicated SQL server that hosts the different SQL instances for the infrastructure components and a different SQL server for the SQL instances of the business processes.**

The Veeam Backup & Replication server is a heavy user of SQL Server, so placing the SQL database server nearby increases operational efficiency. VMware vCloud Director is part of a sub-zone within the management zone and controls the vAPPs running in sub-zones within the trust zone.

The management zone r**equires secure and controlled access to the Internet to download licenses and updates** for the various infrastructure components. It is strongly recommended to use an **Internet proxy or a reverse proxy located** in the DMZ as a controlled gateway to the Internet.

All types of cloud repositories should be placed in **sub-zones within the Untrusted zone.** The organisation's data is going outside the security boundaries, so it is necessary to ensure that, **as an additional precaution, data to 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 to transport the data to the Cloud Provider, Azure Proxy or AWS deployment.

3.7.3.4 Trusted Zone

The trusted zone will be populated by **hypervisor hosts** such as VMware ESXi and/or Microsoft Hyper-V hosts. All components of the trusted zone will need access to different services in the management zone. The Veeam Proxy servers, which are the ones that move the data, are part of the zone of trust.

Veeam Proxies can back up virtual machines without having access to the guest operating systems themselves. If you are backing up or replicating running virtual machines, you can enable the guest processing options.

Guest processing options are advanced tasks that require Veeam Backup & Replication to communicate with the guest operating system of the virtual machine. When virtual machines are separated into sub-zones, they can be deployed and take advantage of the Veeam Guest Interaction Proxy (GIP), in the trusted sub-zone, which will have secure access and deploy the necessary runtime to the virtual machine for guest processing tasks.

In the case where different business units or customers run in the trusted zone, consideration should be given to running them in sub-zones of the trusted zone. But bear in mind that **overly complex designs can be counterproductive** and provide an erroneous sense of security.

VMware vCloud Director vAPPs are also part of the Trusted Zone and would normally be divided into sub-zones per business unit or tenant. Veeam can capture entire vApps and vCloud Director configurations within backup jobs.

3.7.3.5 Restricted Zone

Primary storage, where production data and virtual machines reside, must be located in this restricted area, but so must other components that store data.

This area must never be accessible by any user directly. It is only available to virtual infrastructure components and application servers and administrators with strict rights.

In addition, the Veeam Scale Out Backup Repository (SOBR), Simple Repository, Deduplication Appliances or Cloud Repository when used in combination with Veeam Cloud Connect for Enterprise (VCC-E) must be part of this zone. For organisations using VCC-E it is possible to define cloud repositories on top of the SOBR or as separately defined cloud repositories in a Restricted Zone sub-zone.

3.7.3.6 Audit Zone

Visibility is key to protect, detect and contain threats at an early stage. Monitoring solutions such as Veeam ONE and/or Veeam Management Pack in combination with Microsoft System Center are placed in this zone. IDS and IPS systems should also be placed in this audit zone.

3.7.4 Reduction of the attack surface

3.7.4.1 Access to the console

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. The console allows multiple backup operators and administrators to log in to Veeam Backup & Replication simultaneously and perform all types of data protection and disaster recovery operations as if they were working on the backup server.

It is preferable to **install Veeam Backup & Replication Console on a central management server located in a secure network area and protected with two-factor authentication (2FA)** instead of multiple installations of the console on local desktops of backup and recovery administrators. It is recommended to **always apply MFA** when authenticating to the VBCR itself (supported as of v12).

Access to the Veeam Backup & Replication Server must be limited to the Veeam Backup & Replication console, any remote access protocol must be disabled.

3.7.4.2 Uninstall the Backup server console

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

The Console cannot be removed through the installer or using Add/Remove in Microsoft Windows. It is necessary to open a cmd command prompt with administrative access. At 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.

To uninstall Veeam Backup & Replication Console, it is required to uninstall all Veeam Explorers first:

- **"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".**

These components can be uninstalled using: *msiexec /x {ProductCode}*

Example to uninstall Veeam Backup & Replication console: msiexec /x {D0BCF408-A05D-45AA-A982-5ACC74ADFD8A}

NOTE: Uninstalling the Veeam Backup and Replication console removes the PowerShell module and makes it impossible to use the Veeam Backup PowerShell cmdlets on the backup server. This may affect automation scripts or products that rely on PowerShell to interact with Veeam Backup and Replication, for example Veeam Recovery Orchestrator (formerly Veeam Disaster Recovery Orchestrator).

3.7.4.3 Veeam Backup & Replication Database Protection

The backup and replication configuration database stores credentials for connecting to virtual servers and other systems in the backup and 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 is a potential threat.

To protect the Backup & Replication configuration database, these guidelines are followed:

- **Restrict user access to the database.** Ensure that only authorised users can access the backup server and the server hosting of Veeam Backup & Replication configuration database (if the database is running on a remote server).

- **Encrypt data in configuration backups.** It is recommended to enable data encryption in the configuration backups to protect the data stored in the configuration database. Note that user accounts and passwords are not stored in the configuration backups when encryption is not enabled.

3.7.4.4 Disposal of unused components

Remove all unnecessary software and applications from the deployed Veeam components. While these programs may provide useful functions for the administrator, they also **provide unwanted access** (backdoors) to the system and should be removed during the hardening process.

Additional software such as web browsers, Java, Adobe Reader and similar programs must be uninstalled. In general, it is recommended to **remove all functionality outside of the operating system** or active Veeam components. This will make maintaining an up-to-date patch level much more effective.

3.7.4.5 Elimination of unused services

Disable the Veeam vPower NFS service on each component where you do not plan to use the following Veeam features: SureBackup, Instant Recovery or file level recovery (FLR) operations from another OS.

Remove the default proxy and the default repository role from the VBR server if you do not plan to use them. Similarly, when Enterprise Manager is not used, it is also recommended to **uninstall and remove it from the environment.**

3.7.4.6 Patches and updates

Applying security patches to operating systems, software and firmware for Veeam components is critical. Most attacks succeed because there is already vulnerable software in use that is not aligned with current patch levels.

Therefore, it is very important to **verify that all software and hardware components running Veeam components are up to date.** One of the most common causes of credential theft is guest operating system updates and the use of outdated authentication protocols.

To mitigate risks, the following guidelines can be followed:

- Track Common Vulnerabilities and Exposures (CVE) of systems.
- Verify that the Operating Systems of the infrastructure servers are regularly updated.
- Install the latest updates and patches on backup infrastructure servers to minimise the risk of exploitation of operating system vulnerabilities by attackers.

You can choose to isolate the Veeam Backup and Replication server from the Internet. In this case, it is necessary to proceed with **offline updates**. To do this, the updates are downloaded from another computer, the binaries are copied to the VBR server and the downloaded updates are applied.

In cases where Veeam Backup and Replication Server can access the Internet, it is necessary to **strictly restrict access to the application and operating system update servers,** again removing any tools and browsers, thereby preventing the installation/downloading of potentially harmful pieces of code. Of course, **never expose Veeam Backup and Replication Server to the Internet.**

3.7.4.7 Ports

It is best not to **use dark ports or other mechanisms** to try to hide the ports and protocols in use by Veeam, although this may seem like a good option. In practice, this often makes it more difficult to manage the infrastructure, which opens up other possibilities for attackers. Hiding is not always synonymous with security.

Two (2) tools have been developed to facilitate the identification of ports between Veeam components:

- **"Veeam Network Port Mapping Tool".**
- **"Ports List Finder".**

It is recommended to **apply appropriate firewall rules** to restrict network communications to the minimum needs of the applications.

3.7.5 Working group or domain

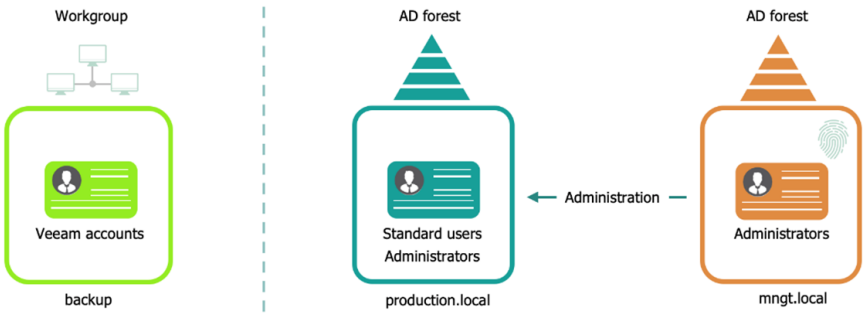
Microsoft Active Directory is at the heart of the IT infrastructure of almost every organisation. When configuring the Veeam Availability infrastructure, it is necessary to take into consideration the principle that **a data protection system should in no way be dependent on the environment it is supposed to protect.**

This is because when the production environment fails along with the domain controllers, it will affect the ability to perform actual restores due to the dependency of the backup server on those domain controllers for authentication of the backup console, DNS for name resolution, etc.

When it comes to securing the administrative accounts and installation of the Veeam infrastructure, **several options are available, from the most secure to the least secure:**

- Add Veeam components to a management domain residing in a separate Active Directory forest and secure administrative accounts with two-factor authentication (2FA) mechanisms.
- Add the Veeam components to a separate workgroup and place the components on a separate network where appropriate.

Add the Veeam components to the production domain, but verify that accounts with administrative privileges are protected with two-factor authentication (2FA).



3.7.5.1 Best practices

For the most secure deployment, **it is recommended to add the Veeam components to an administration domain** residing in a separate Active Directory forest and to protect administrative accounts with two-factor authentication (2FA) mechanisms.

In this way, Veeam's availability infrastructure does not depend on the environment it is supposed to protect.

3.7.5.2 Windows Working Group

When using a **workgroup, it is necessary to have everything carefully documented for management and compliance reasons.** Each system needs to be configured independently with a local security policy, as well as case-specific user management, permissions assignment, etc.

With multiple Veeam servers and multiple users, this could become **extremely difficult in large environments.** Kerberos authentication cannot be used with a workgroup server, instead **NLTM will be used, which in itself can be an added risk.**

A workgroup is more difficult to defend against insider threats, such as a disgruntled employee, as they may use local accounts on the workgroup's servers, and it is not possible to disable a single AD account by locking that specific employee out of the critical infrastructure. In

addition, **it is more difficult to demonstrate for compliance needs that the systems are secure** and used correctly. A workgroup configuration is a good solution for environments of a limited size.

Advantages

- Quick and easy to set up.
- It separates Veeam accounts from privileged domain accounts (helps against keyloggers and production domain violation).
- It does not depend on the environment it is meant to protect.
- No infrastructure servers such as Domain Controllers, NTP or DNS are required.

Inconvenientes

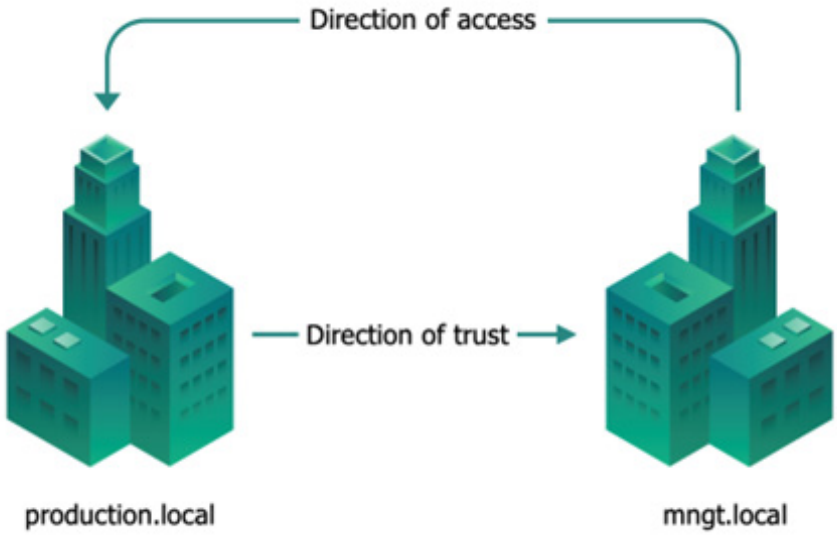
- High management overhead in large environments.
- No Kerberos communication when logging into a standalone server (workgroup), only NTLM.
- It is more difficult to comply with regulations, to carry out compliance checks and to demonstrate compliance with the adopted frameworks.
- It is not possible to use the gMSA authentication system for the interaction of guest OS backups.

3.7.5.3 Domain of management

While this approach adds a forest to an Active Directory environment, the cost and complexity is 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 easier. It also allows one-click deactivation of a single AD account when an insider threat such as the one mentioned above needs to be addressed.

Setting up a separate forest with a management domain is the best option for large environments. You can also add **multi-factor authentication** to the domain to further protect administrative accounts, blocking Man-in-the-Middle attacks and keyloggers.

Forest trusts help manage a segmented Active Directory Domain Services (AD DS) infrastructure and support access to resources and other objects across multiple forests. They are also useful for organisations seeking an administrative autonomy solution as two (2) different forests can be linked together to form a unidirectional or bidirectional transitive trust relationship. A forest trust allows administrators to connect two (2) AD DS forests with a single trust relationship to provide a seamless authentication and authorisation experience across forests.



If a one-way trust relationship is created between two forests, the members of the trusted forest use the resources located in the trusting forest and the trust operates only in one direction.

3.7.6 Worm Storage with Veeam Hardened Repository

Veeam Hardened Repository is a WORM storage solution that protects against unwanted changes to backup files. It is available from version 11 and supports the following features:

- **Immutability:** When you add a hardened repository, you specify the period of time for which the backup files must be immutable. During this period, the files stored in this repository cannot be modified or deleted.
- **One-time credentials:** credentials that are used on a one-time basis to deploy Veeam Data Mover, or the transport service, while adding the Linux server to the backup infrastructure. These credentials are not stored in the backup infrastructure. Even if the Veeam Backup & Replication server is compromised, the attacker cannot obtain the credentials and connect to the hardened repository.

As a reminder or complement to the user guide, the following actions are recommended for creating a hardened repository:

- **Deploy the Veeam repository using single-use credentials:** Veeam will not store the repository root account, keeping the backup files safe if the Veeam Backup server is compromised. Do not forget to remove the user from the sudoers group after installation.
- **Disable SSH after deployment:** SSH connection is only required for deployment or upgrade of Veeam Data Mover. Once Veeam is deployed, it is possible to disable SSH to improve security. If it is kept active, multi-factor authentication should be enabled for use.
- **IPMI:** any management tool such as ILO or DRAC can be used to access the repository, and even to erase hard disks. It is strongly recommended to disconnect these tools from the network when not in use.
- **NTP:** time management is crucial when talking about immutability. It is not advisable to use public NTP servers, as this would mean exposing the repository server on the Internet. Using your own NTP server is an option, but may pose a security risk in case an attacker takes control of it.

The use of the internal CMOS clock is an advisable option, but the trade-off is the need to regularly check and manually adjust the system time. In addition, a time difference between the repository and the backup server would make the forensic analysis of the logs more complex. A second advisable and interesting option is to use a DCF77 dongle (or local equivalent) with the XNTP package to synchronise the repository in longwave signal.

3.7.7 Application processing

Application Aware Processing requires the Veeam Backup and Replication infrastructure to log on to production servers to interact with operating systems and applications.

Although it allows applications and the file system to be consistent at backup time, it **can be considered a risk as any credentials provided will be stored in the** Veeam Backup and Replication **configuration database.**

Alternative solutions would be:

- Perform backups without application processing, i.e. perform fault tolerant backups.
- Use gMSA (Group Managed Service Accounts) in VBR v12 or later.
- Use agents to perform backups.

NOTE: Application items can still be restored in a granular way from a non-application-aware backup via browsers. To do this, a Guest file restore is initiated and, from the explorer, an Application Item restore is forced.

3.7.7.1 gMSA

Although not fully secure, if it is considered necessary to delegate password management to Microsoft gMSA, it should be taken into consideration that **the VBR server will then have to be part of the domain.**

3.7.7.2 Active Directory Backup

A consistent Active Directory backup requires Built-in Administrator credentials on the guest. To avoid storing these credentials in the Veeam database, **it is good practice to back up Active Directory servers using an unmanaged agent** against a Veeam repository.

In this way, the Administrator account will remain protected and restoring Active Directory items via the browser will prompt for the appropriate login at restore time.

3.7.7.3 Location of the Guest Interaction Proxy

Guest interaction proxies allow interaction with Microsoft Windows virtual machines in lower security zones without exposing the backup server in these zones.

Using the Guest interaction proxy with guests will drastically limit the exposure of the Veeam backup and replication server. The ports required for guest interaction processing are available in the user guide.

3.7.7.4 Location of the Console for Explorers

The deployment of the Veeam Console in isolated zones will be of great help when restoring guest items, as it will **allow operation without the need to open the Microsoft RPC dynamic port range** from the management zone to the isolated zone. The console can be deployed in the Guest interaction Proxy which should already be in that zone.

3.7.7.5 Credentials for restorations

At restore time, when using Veeam Explorers, authentication against the target server is performed using the guest interaction credentials configured in the backup task. If the credentials are changed in the job configuration, the account used at restore time will change.

Removal of guest interaction settings will incur the interactive credential entry at restore time.

4. Decalogue of recommendations

Below are ten security recommendations when using Veeam Data Platform.

Decalogue of recommendations for Veeam Data Platform

1. It is recommended that **security** be implemented **from the beginning of the design of** the environment. As well as a properly designed backup infrastructure.

2. It is recommended to **protect backups**, infrastructure, as well as to train the organisation's staff.

3. It is recommended that a strategy be drawn up to **monitor alerts, users, servers and other critical elements** that are part of the system.

4. It is recommended to have a **recovery plan** in place, as well as to train the necessary personnel to carry it out, which will reduce the response time in the event of an incident.

5. It is recommended to deploy an **Access Control policy** to management components using the principle of least privilege. Enforce containment to prevent attackers from moving too easily (change the rules of the game to the attacker).

6. It is recommended to create a **strong password policy** and implement a **policy of blocking** failed login attempts to prevent brute force attacks.

7. It is recommended to choose **strong encryption algorithms** for remote access to the backup infrastructure.

8. It is recommended for data encryption to **enable encryption both in transit and at rest to** avoid breaches and unwanted reads.

9. It is recommended to **reduce the attack surface** by removing all non-essential software and utilities from the deployed Veeam components.

10. **Segmentation into different areas,** reducing the exposure area by removing unnecessary add-ons or functionality, having immutable backups, as well as properly managing other products or solutions used in conjunction with Veeam are recommended.

Centro Criptológico Nacional 20 ANIVERSARIO

CCN-CERT centro criptológico nacional

Annex A. National security framework (ENS) security measures and security controls

The following table links different security measures of Royal Decree 311/2022, of 3 May, which regulates the National Security Framework with Veeam Backup solutions, highlighting their applicability, as well as a reference to the corresponding section of this guide, where it is justified:

ENS measure	Justification of applicability	Section in this guide
Backup copies [mp. info.6].	The aim of Veeam Backup solutions is precisely to make backups that enable the recovery of accidentally or intentionally lost data **[mp.info.6.1**]. They also make it possible to determine the frequency of backups, to store backups on-site and/or off-site, and to establish controls to limit authorised access to backups **[mp. info.6.2].** These solutions also allow for recovery tests **[mp. info.6.r1.1]** and the storage of one of the copies separately in a different location, so that a potential incident cannot affect both the original information and the copy simultaneously **[mp.info.6.r2].**	Introduction. 3.3 Recovery strategy.
Identification [op.acc.1]. Access requirements [op.acc.2].	Account management will be supported by the account management of the domain where the Veeam backup solution is deployed. Single-use credentials provided by the user are used interactively at the time of initial installation and when installing product updates. They are never stored in the configuration database.	3.4 Roles and users. 3.7.6 Worm Storage with Veeam Hardened Repository.

Annex A. National security framework (ENS) security measures and security controls

ENS measure	Justification of applicability	Section in this guide
Authentication mechanism [op.acc.5], [op.acc.6].	All use of the SSH protocol has been encapsulated in an extended transport protocol. As a result, SSH connectivity is only required at the time of initial deployment and when installing product updates. This allows customers to protect SSH with interactive multi-factor authentication (MFA) or even disable the SSH server entirely to protect their repository, even from future zero-day vulnerabilities. Since Veeam Backup & Replication v12, a Kerberos-only architecture is possible, and it is recommended to disable NTLM authentication whenever possible.	3.5 Authentication Protocols.
Continuity plan [op.cont.2].	It is recommended that image-level backups be immutable for the time specified in the retention policy, at least four (4) weeks, following a GFS (Grand father, Father, Son) framework. This functionality uses the native Linux file immutability feature.	3.1.1 Protection of backups.
Cryptography [mp.si.2].	Integrated 'Veeam Backup & Replication' encryption is available to protect data at rest from backups **[mp.si.2.r2.1].** The encryption modules are based on FIPS.	3.6.1 Encryption at rest.
Separation of information flows in the network [mp.com.4].	To isolate the backup traffic, it is recommended to use a segmented network between the main components of the backup infrastructure: backup server, backup proxies, backup repositories, etc. **[mp.com.4.1]** By default, Veeam Backup & Replication encrypts network traffic travelling between public networks, but it is recommended to enable traffic encryption also on private networks to ensure secure communication in the internal network. **[mp.com.2.r5.1]**	3.6.2 Encryption in transit.
Registration of the activity [op.exp.8].	Veeam backup solutions can add entries in the system event log for better visibility for users performing log-based monitoring **[op.ep.8.1].**	3.7 bastioning. 3.7.1 segmentation.
Dimensioning / capacity management [op.pl.4].	The use of scalable backup repositories using Scale-Out Backup Repositories (SOBR) makes it easier to manage the available capacity for backups. **op.pl.4.2], [op.pl.4.r1.2], [op.pl.4.r1.2].**	

Annex B. Checklist

Element	Check	Result
RULE 3-2-1-1-0		
3 copies	Are there 3 different copies of the data?	Yes/No/Partially/Doesn't Know
2 media	Are the copies hosted on two different media?	Yes/No/Partially/Doesn't Know
1 offsite	Is there a copy outside the main site?	Yes/No/Partially/Doesn't Know
1 immutable / separate	Is a copy immutable or separate?	Yes/No/Partially/Doesn't Know
0 errors	Are backups regularly tested to ensure that they can be restored?	Yes/No/Partially/Doesn't Know
THREAT DETECTION		
EDR-XDR	Is an EDR or XDR implemented to detect threats?	Yes/No/Partially/Doesn't Know
Honeypots	Have decoys been implemented?	Yes/No/Partially/Doesn't Know
VeeamOne	Is Veeam One implemented and monitoring threats?	Yes/No/Partially/Doesn't Know
RECOVERY STRATEGY		
Existence of recovery strategy	Is there a recovery strategy?	Yes/No/Partially/Doesn't Know
Recovery strategy test	Is the recovery strategy regularly tested?	Yes/No/Partially/Doesn't Know
Dedicated recovery infrastructure	Is there a dedicated recovery infrastructure?	Yes/No/Partially/Doesn't Know
ROLES AND USERS		
Anonymous accounts	Do the names of the accounts contain references to their functions?	Yes/No/Partially/Doesn't Know
Password change policy	Are passwords changed regularly?	Yes/No/Partially/Doesn't Know

Annex B. Checklist

Element	Check	Result
Blocking policy	Do users log off after a certain period of inactivity?	Yes/No/Partially/Doesn't Know
Role-based access control	Can the backup infrastructure only be accessed via backup accounts?	Yes/No/Partially/Doesn't Know
Decoy accounts	Are there visible decoy accounts that are monitored?	Yes/No/Partially/Doesn't Know
Multi Factor authentication	Are there visible decoy accounts that are monitored?	Yes/No/Partially/Doesn't Know
ENCRYPTION		
At rest	Is the data encrypted in the repositories?	Yes/No/Partially/Doesn't Know
In transit	Is the data encrypted in transit?	Yes/No/Partially/Doesn't Know
FORTIFICATION		
Targeted segmentation	Is the back-up infrastructure in specific segments?	Yes/No/Partially/Doesn't Know
MFA	Is MFA enabled in the backup infrastructure segment?	Yes/No/Partially/Doesn't Know
Veeam DB	Is access to the Veeam database restricted?	Yes/No/Partially/Doesn't Know
Console	Is the VBR server console uninstalled?	Yes/No/Partially/Doesn't Know
Cleaning of backup infrastructure servers	Have the servers been cleaned of all unnecessary functions/components?	Yes/No/Partially/Doesn't Know
Patches and updates	Are the servers regularly patched/updated?	Yes/No/Partially/Doesn't Know
Remote management	Are remote administration tools disabled/uninstalled?	Yes/No/Partially/Doesn't Know
Immutability	Is the repository immutable?	Yes/No/Partially/Doesn't Know
Fortification	Is the repository hardened?	Yes/No/Partially/Doesn't Know
APPLICATION PROCESSING		
Domain controller credentials	Is the domain administrator account stored in Veeam?	Yes/No/Partially/Doesn't Know
gMSA	Is gMSA used for interaction with guests?	Yes/No/Partially/Doesn't Know

Annex C. Glossary

Term	Description
AES-256	Encryption algorithm
Air gap	Safety measure to isolate an object from the network
API	Application Programming Interface
Appliance	Software or hardware element that has been designed to provide a specific computing resource
Backup	Security copy of any asset.
Baremetal	Dedicated physical server
Bastionado	Hardening or bastioning is about protecting the infrastructure against attacks by reducing the attack surface and thus eliminating as many risks as possible.
CCTV	Closed Circuit Television
CIFS	File transfer protocol
Cloud	A set of remote servers connected to the internet that provide a service or purpose.
Cluster	Set of nodes of a kubernetes infrastructure
CMOS	Complementary Metal Oxide Semiconductor, also called a button-type battery, on the motherboard helps the BIOS or UEFI to store hardware configuration settings.
Configmaps	Key-value data file
CPU (Central Processing Unit)	Central processing unit
Cryptoprocessors	Microprocessor optimised to perform cryptographic operations
Deduplicate	Computerised de-duplication process
DMZ	Demilitarised Zone or DMZ is an area of infrastructure where services are exposed to insecure networks such as the internet.

Annex C. Glossary

Term	Description
DNS (Domain Name System)	Service that translates domain names into IP addresses or vice versa
Dongle	A dongle is a small device, which connects to another device to provide an additional function.
DR (Disaster Recovery)	Defined process for recovering data from a system outage.
Failback	Ability to transfer from the repaired environment to the original environment after the failure
Failover	Ability of a system to continue to function in the event of failure
Forest	Microsoft Windows domain set
GDPR (General Data Protection Regulation)	General Data Protection Regulation
GPO (Group Policy Object)	Group policy, active directory object that assigns a policy or configuration value
Honeypot	Lure used to visualise possible attacks
IDS	Intrusion detection system
IPS	Intrusion prevention system
Kerberos	Authentication protocol
keyloggers	Malicious software that records what is typed on the keyboard
Kubernetes	Open source container platform
LAN	Local Area Network
Multi-Tenant	Software architecture that allows a single instance to serve multiple clients
Namespace	Workspace / namespace
NAS (Network Attached Storage)	Network-attached storage technology
NDMP	Network Data Management Protocol
NFS	Network file system protocol

Annex C. Glossary

Term	Description
NTLM	Microsoft Authentication Protocol Set
NTP	Clock synchronisation protocol
Object Storage	Object-based storage
IODC	Authentication protocol
RBAC (Role-Based Access Control)	Role-based access control
RPC	Remote procedure call programme
RPO	Recovery point target
RTO	Recovery time target
SaaS	Software as a service
UPS	Uninterruptible Power Supply
Secret	Confidential data file
SMB	Server Message Block. It is a file transfer protocol.
SSH	Secure Shell is a remote administration protocol.
Token	Validation identifier
WAN	Wide Area Network
Workgroup	Microsoft Windows Working Group
WORM (Write Once, Read Many)	Write-once, read-many backup method

Centro Criptológico Nacional

20 ANIVERSARIO

CCN-CERT
centro criptológico nacional

VEEAM

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es