RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SECURING A VMWARE INFRASTRUCTURE

FUNDAMENTALS

ANSSI-BP-103-EN
02/04/2024

TARGETED AUDIENCE:

Developers **Administrators** **IT security managers** **IT managers** Users

Information

Warning

This document, written by ANSSI, the French National Cybersecurity Agency, is titled **"Securing a VMware infrastructure"**. It is freely available at `cyber.gouv.fr/en`.
It is an original creation from ANSSI and it is placed under the "Open Licence v2.0" published by the Etalab mission.
According to the Open Licence v2.0, this document can be freely reused, subject to mentionning its paternity (source and date of last update). Reuse means the right to communicate, distribute, redistribute, publish, transmit, reproduce, copy, adapt, modify, extract, transform and use, including for commercial purposes
The recommendations are provided as is and are related to threats known at the publication time. Considering the information systems diversity, ANSSI cannot guarantee direct application of these recommendations on targeted information systems. Applying the following recommendations shall be, at first, validated by IT administrators and/or IT security managers.
This document is a courtesy translation of the initial French document **"Titre non défini"**, available at `cyber.gouv.fr`. In case of conflicts between these two documents, the latter is considered as the only reference.

Document changelog:

VERSION	DATE	CHANGELOG
1.0	02/04/2024	Initial version

Contents

1
Preamble

Virtualisation technologies form the foundational layer of cloud computing infrastructures. Technical components, commonly referred to as 'hypervisors', enable the administration and pooling of compute,network, and storage resources.

As such, hypervisors are prime targets for attackers. Their compromise can provide access to all hosted data and workloads. Therefore, both state-sponsored and cybercriminal threats must be carefully considered when deploying virtualisation infrastructure. Depending on the nature of the threat, motivations may vary: espionage or disruption in the case of state actors; financial gain and sometimes destruction in the case of cybercriminals.

This document aims to provide guidance on how to secure virtualised infrastructures based on VMware technology. VMware is one of the most widely used platforms in this domain. These recommendations should be considered and adapted on a case-by-case basis, depending on the operational context of the infrastructure, the nature of the services it supports, and their criticality. This document focuses on the most important recommendations, and does not seek to be exhaustive or provide a high level of detail.

2
General principles

The purpose of this chapter is to define certain general VMware operational principles necessary to understanding the recommendations provided in chapter 3.

2.1 Architecture

When setting up virtualisation infrastructure, it is important to consider the virtualisation layer as a foundational component that must remain independent from the virtual machines it hosts.

The virtualisation infrastructure can be divided into two parts:

- the control plane, responsible for managing the virtual infrastructure;
- the data plane, which hosts the virtual machines.

This separation is a fundamental security measure, designed to protect the virtualisation infrastructure from the virtual machines it hosts.

In VMware terminology, used in the validated designs [1], this separation is referred to as:

- management domain for the administration cluster;
- workload domain for the production cluster.

2.2 Privilege management

Privilege management is critical in virtualisation infrastructure. It is therefore essential to understand the mechanisms used to control access and permissions. In vSphere, this is done through the use of roles [2]. A role is a collection of privileges which define authorised actions and read/write rights on the properties of a VMware object. VMware enables the definition of access control policies by associating a user, a role, and a VMware object (e.g., virtual machine, datastore, vSwitch, port group, etc.).

1. Vendor documentation on vSphere VCF architecture designs: https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/5-1/vcf-design-5-1/vmware-cloud-foundation-concepts/vmware-cloud-foundation-architecture-models.html

2. Vendor documentation onroles, https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vsphere-security/vsphere-permissions-and-user-management-tasks/using-roles-to-assign-privileges.html

2.3 Network segmentation

To enable communication between virtual machines (VMs), or between VMs and external systems or devices, the hypervisor creates a set of virtual devices (virtual switches, virtual network interface cards).

In a vSphere infrastructure, these devices include vSwitches or dvSwitches (virtual layer 2 switches), and vNICs (virtual network interface cards).

DvSwitches offer not only centralised management, but also advanced features such as PVLAN, traffic mirroring, and more.

The ability to easily segment networks within virtualised infrastructure allows for the isolation of VMs based on their use cases, exposure levels, or sensitivity.

To ensure connectivity between ESXi hypervisors and the various components of the virtual infrastructure (other ESXi hosts, vCenter, NSX, storage arrays, backup systems, monitoring tools, etc.), VMkernel adapters are used [3].

These adapters are assigned IP addresses and handle network traffic bound for specific infrastructure components. Multiple VMkernel adapters can exist on a single ESXi host.

2.4 Micro-segmentation

Micro-segmentation is a network security technique which allows the restriction of traffic between each VM—or group of VMs— through granular, stackable filtering rules. These filtering rules are managed centrally and independently of the virtual machine's operating system.

Micro-segmentation is a defence-in-depth measure which, when implemented effectively, makes it possible to:

- limit lateral movement in the event of a virtual machine compromise;
- limit north-south and east-west traffic [4];
- ensure the accuracy of filtering (e.g., using specific tags on VMs).

3. Vendor documentation on ESXi networking: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/9-0/vsphere-networking.html

4. "North-south" and "east-west" respectively refer to traffic flows which are external to the zone (e.g. to another zone or an Internet gateway), and to internal flows within the zone (e.g. between servers with similar sensitivity or purpose).

Warning

Any micro-segmentation solutions which rely on in-guest agents to perform filtering actions provides a lower level of security compared to solutions which operate at the hypervisor level (e.g., hypervisor kernel modules, openvswitch.).

Micro-segmentation solutions in virtualised environments each have their own specificities, along with their strengths and weaknesses. Within the VMware vSphere ecosystem, micro-segmentation is provided by the NSX solution. It should be noted that NSX offers additional security features and is not solely dedicated to micro-segmentation. The use of NSX is subject to licensing.

The NSX solution is mainly composed of four components:

- NSX manager, which provides the centralised creation and management of filtering rules;
- NSX controllers, which are part of the solution's control plane and ensure the consistency of rules created by the NSX manager across the infrastructure;
- a kernel module deployed on ESXi, enabling the creation of local firewalls on each virtual machine's network interface;
- NSX edges, which act as gateways between the virtual infrastructure and the outside world (e.g., another virtual infrastructure or a physical environment). This component is optional and can be replaced with physical firewalls for enhanced network isolation.

Micro-segmentation is a defence-in-depth mechanism which provides an additional layer of protection against cyberattacks, but which is not sufficient on its own.

2.5 Attack vectors

Virtualisation infrastructure is frequently targeted by ransomware attacks. Given the concentration of virtual machines, these environments are particularly attractive targets.

Common sources and causes of compromise include:

- compromise of the office IT environment (e.g. through phishing), followed by lateral movement towards the virtualisation infrastructure;
- lateral movement resulting from the compromise of a third-party service provider;
- exploitation of a vulnerability within the virtualisation infrastructure;
- use of compromised binaries;
- lack of security maintenance;
- failure to secure the virtualisation infrastructure in the first place;
- deployment of a malicious implant on the storage system used by the virtualisation infrastructure;
- exposure of hypervisors to the Internet.

3
Recommendations

3.1 General recommendations

R1 The virtualisation platform must be maintained by applying security updates as promptly as possible.

R2 It is advisable to subscribe to any security bulletins which pertain to the software and hardware components comprised in the virtualisation infrastructure.

3.2 Architecture-related recommendations

R3 For vSphere infrastructure, traffic flows should be segmented as follows:

- in the control plane, place the network traffic of vSphere infrastructure management components (administration vCenter, workload vCenter, NSX Manager, NSX Controller, ESXi administration interfaces);
- in the data plane, place the network traffic of hosted virtual machines (services, business storage, etc.).

Warning

Please note that a virtual machine's administration port should not be shared with the virtualisation platform's control plane.

R4 A virtual machine's administration port must be isolated from the virtualisation platform's control plane by, at the very least, using a dedicated VLAN.

R5 Management, storage, and backup network flows should be individually segregated through the use of dedicated VLANs and dedicated VMkernel adapters.

R6 Administrative flows should use a physical network port specifically intended for this purpose.

R7 To best secure the virtualisation infrastructure, **it is advisable to maintain a cluster dedicated to IT administration** (management domain), separate from the production clusters. This cluster hosts the control plane components — such as the vCenter(s) for the production cluster(s) (Workload Domain) — as well as the vCenter for the management cluster itself.

Information

To optimise costs, a management cluster may be used to establish an administration information system, as outlined in ANSSI's *"Recommandations relatives à l'administration sécurisée des systèmes d'information"* (i.e. Recommendations to secure the administration of IT systems) guide[4].

R8 Production clusters or servers (workload domains) should be dedicated according to their sensitivity and trust zones.

R9 Each sensitivity or trust zone must be managed by a dedicated vCenter, hosted within the management domain.

R10 Within the management cluster (management domain), VLAN segmentation should be implemented to isolate the different control planes associated with each production environment (workload domain).

R11 If the IT system administration is complex, the management environment must include an ESXi cluster acting as a management domain, and a workload domain containing the administration tools.

Figure 1 presents an example of architecture which has implemented this segmentation.

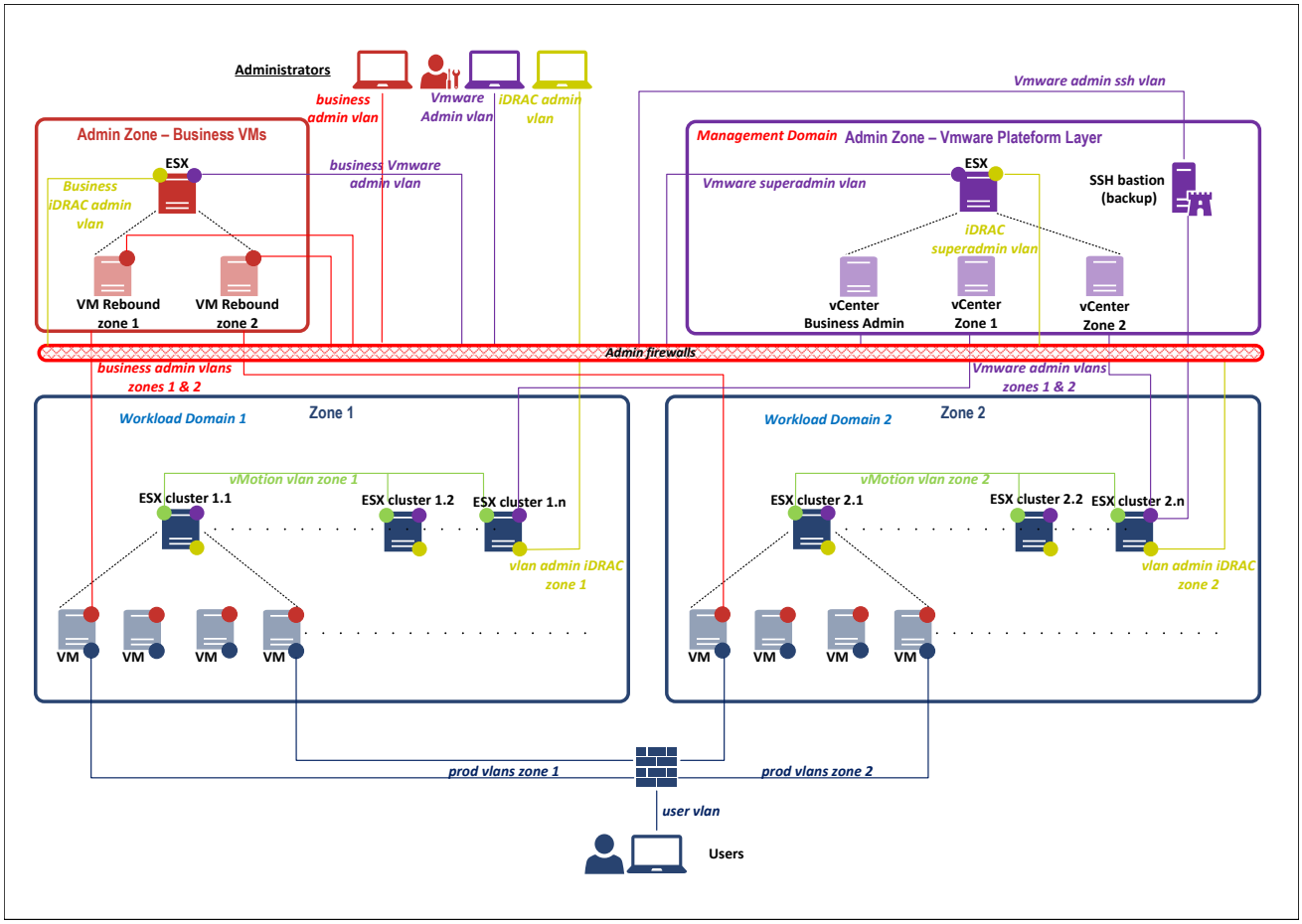

Figure 1 – VMware administration architecture

The following key principles must be respected:

R12 trust zones must be defined according to the sensitivity level of the resources (business values).

R13 the adminsitration of ESXi hypervisors (shown in purple in Figure1) must be segregated from the business administration of VMs (shown in red in Figure 1).

R14 the administration of these trust zones must be segregated by deploying one vCenter administration system per zone for platform layer administration (shown in purple in Figure 1) and a jump system for business VM administration (shown in red in Figure 1);

R15 out-of-band management (OOB; e.g., iDRac, shown in yellow in Figure 1) must be segregated from the rest of the administration.

R16 the vMotion transfer flows (shown in green in Figure 1) must be segregated for each trust zone.

VMware infrastructure administration authorised flows are shown in blue on Figure 2.

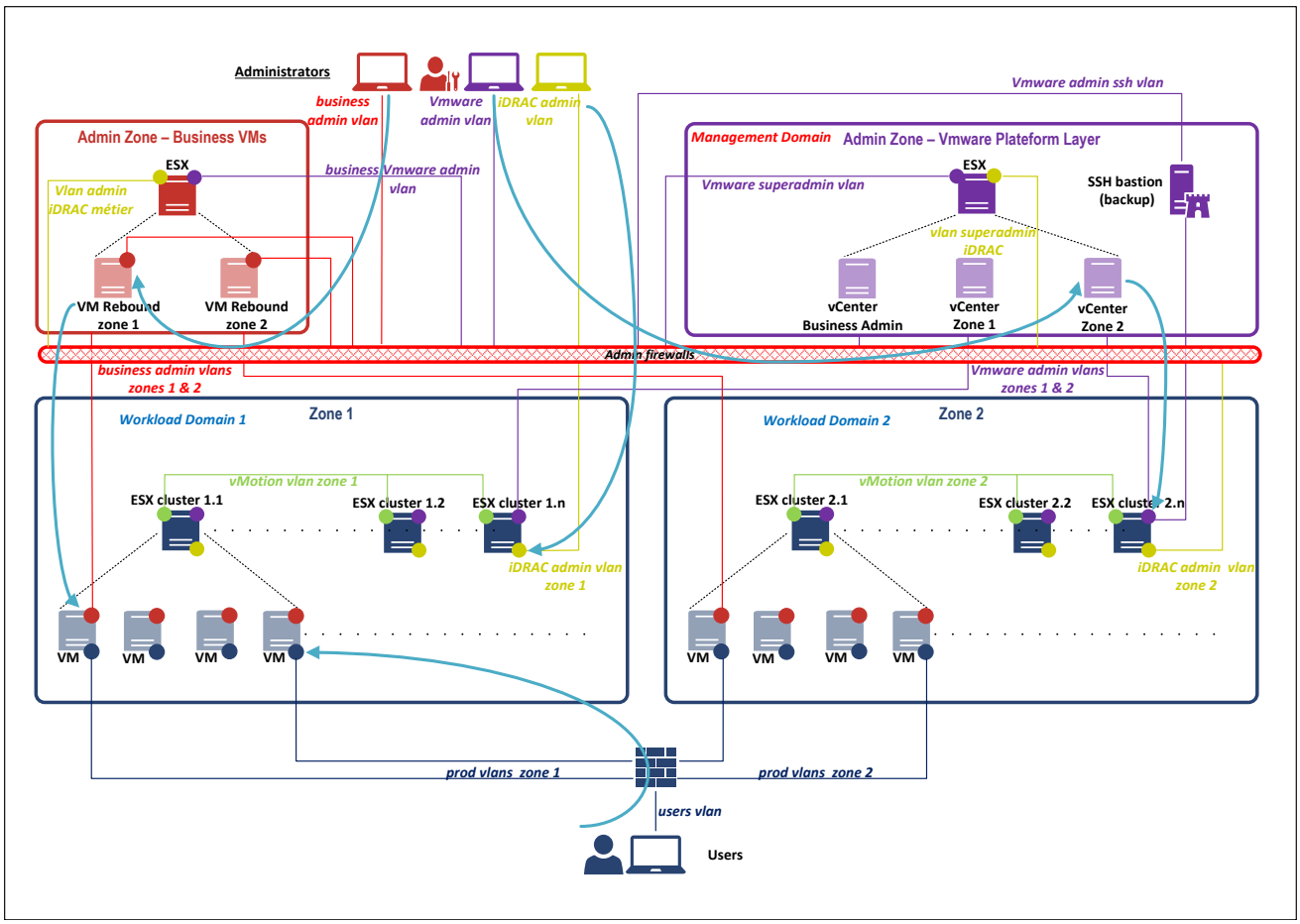

Figure 2 – VMware management architecture – network flows

R17 Filtering rules should be created to correspond to the flows[5] defined in Figure 2.

R18 The VMware virtualisation platform must be considered to be critical infrastructure for the information system. This virtualisation platform must benefit from the appropriate protection measures and be integrated into the entity's administration information system.

5. Vendor documentation on ports needed by VMware products and solutions : `https://ports.esp.vmware.com/`

R19 All hardware related to the VMware infrastructure must be securely managed as described above. Beyond servers, this includes iLO/iDRAC interfaces, storage arrays, etc.

R20 A dedicated network interface must be assigned for the administration and management of ESXi hosts (SSH access and vCenter management flows). This interface must be connected to the entity's administration network and must not under any circumstances be accessible from a production network.

R21 The administration directory for VMware infrastructure must be separate from the directories used in production (e.g., Active Directory). Control paths must be regularly verified [1], to make sure that there is no possibility of privilege escalation from the VMware infrastructure to production directories and vice versa.

R22 ESXi clusters and datastores should be dedicated according to the sensitivity level of the applications and/or of the data hosted.

R23 Regular checks of ESXi configurations should be implemented by comparing the current configuration with the configuration at the time of deployment, by using the host profile feature or through Network segmentation *via* vSphere APIs.

R24 Private VLANs (PVLANs) should be implemented on VMs whenever possible.

R25 VM time synchronisation must be carefully configured. For example, for Active Directory domain controllers, it is preferable not to configure the hypervisor as the time source to avoid time desynchronisation during VM reboot or snapshot operations, which could impact Active Directory replication [6].

R26 A proxy must be dedicated to the administration information system for the retrieval of updates from the Internet. This proxy should filter VMware URLs using an allowlist [7].

3.3 Administrative actions

Depending on the size of the administration teams, two different models may be implemented for the management of virtualisation infrastructure:

- a team specifically dedicated to the virtualisation infrastructure;
- or a shared team managing both the virtualisation infrastructure and the administration of the information system.

R27 A coherent Role-Based Access Control (RBAC) policy must be established for administration accounts, in line with the entity's delegation model (team size).

R28 The principle of least privilege [8] must be applied to all VMware administration accounts [9] and service accounts (e.g., monitoring).

6. Disabling time synchronisation *via* the host for a virtual machine: https://kb.vmware.com/s/article/1189
7. Allow list of VMware update servers https://kb.vmware.com/s/article/82205
8. Vendor documentation for identifying the minimal set of privileges: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere-supervisor/8-0/required-privileges-for-common-tasks.html
9. Vendor documentation on user and authorisation management in vSphere: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vsphere-authentication.html

R29 Multi-factor authentication [5] [10] should be implemented for administrator login on the vSphere/vCenter interface.

R30 At least one account must be dedicated to automated administration actions using the vSphere APIs.

R31 API connections must be monitored to identify legitimate connection sources (e.g., orchestration servers).

R32 All components must be included in the security maintenance process: ESXi, VMware Tools, vCenter, additional VMware vendor tools, and third-party tools, etc.

R33 Additional tools must be limited to strict operational needs. Those which are no longer in use should be uninstalled.

3.4 ESXi hardening

R34 SSH access on ESXi hosts should be disabled and the lockdown function [11] should be set to "normal mode" with an emergency access account configured (a "break-glass" account).

R35 Secure Boot must always be enabled, and the signature of VIBs for ESXi must always be verified [12].

R36 ANSSI's Security recommendations for TLS [3] must be applied to configure HTTPS access for vSphere (Web interface, API) [13] (e.g., minimum TLS version 1.2).

R37 For vMotion functionality, TLS must always be enabled.

R38 VM VLAN tagging must not be configured inside the VM but at the ESX hypervisor level.

R39 The local firewall on ESXi must be configured.

R40 Access to virtual machine administration interfaces and access to the virtualisation platform's administration interfaces must be strictly separated.

10. Vendor documentation on two-factor authentication: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vsphere-authentication/vsphere-authentication-with-vcenter-single-sign-on-authentication/understanding-vcenter-server-two-factor-authentication-authentication.html

11. Vendor documentation on implementing lockdown mode: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/9-0/vsphere-security/securing-esxi-hosts/customizing-hosts-with-the-security-profile/lockdown-mode.html

12. Vendor documentation on ESXi Secure Boot: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/9-0/vsphere-security/securing-esxi-hosts/uefi-secure-boot-for-esxi-hosts.html

13. Vendor documentation on TLS configuration: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/9-0/vsphere-security/managing-tls-protocol-configuration-with-the-tls-reconfiguration-utility.html

3.5 Security monitoring

R41 The following security events related to ESXi and vCenter must be logged and monitored:

- access to ESXi hosts (“auth.log”);
- changes to ESXi and VMs configurations (parameters, services);
- ESXi reboots;
- connections to vSphere/vCenter;
- network traffic on interfaces (administration interfaces should have low network traffic; for example, high traffic could indicate data exfiltration);
- VM suspensions suspended state, suspicion of memory dump);
- the mass shutdown of VMs (possible indication of VMDK encryption);
- any events indicating the use of internal technical accounts in vSphere or ESXi such as vpx-user and dcui (root privileges);
- the history of interactive commands “shell.log”;
- guest operations;
- the upload and download of files on datastores.

3.6 Micro-segmentation

When using micro-segmentation with the NSX solution, the following recommendations apply:

R42 The NSX Manager and NSX Controllers must be deployed on an administration cluster only — never on a production cluster.

R43 The security and effectiveness of micro-segmentation are contingent on the non-compromise of NSX Manager and NSX Controller components. Therefore, their access should be secured, their usage should be limited, and an access control policy should be enforced based on the principle of least privilege.

R44 Filtering rules must not rely on criteria which can be modified or altered by the virtual machine (e.g., hostname, MAC address).

R45 All traffic flows which are not explicitly authorised must be blocked.

R46 Generic rules should be used in addition to more specific rules for more flexible management which can be maintained over time.

R47 The infrastructure should be properly segmented by isolating zones of different sensitivity levels using physical firewalls.

R48 In dynamic infrastructure where virtual machines can be created and deleted very frequently, the following security approach may be appropriate:

- Physical firewalls to filter north-south traffic (traffic between security zones) in a more traditional manner: source IP, destination IP, source port, destination port;
- Micro-segmentation for east-west traffic (traffic within a security zone) with more granular controls: source IP, destination IP, source port, destination port, VM type, tag, operating system, TLS filtering, time of day, etc.

3.7 Backup

R49 A backup strategy for the virtualisation infrastructure must be set. At the very least, it should include: binaries to install a minimal infrastructure (operating systems, software and their patches, hardware firmware), procedures to import configurations, or configuration scripts. Virtual machine restoration procedures must be regularly tested.

R50 A backup of the environments hosted on the virtualisation infrastructure must be established in accordance with the recommendations provided in ANSSI's Information System Backup Fundamental [2].

4
Going further

With these recommendations in place, you will have adopted the key best practices necessary to the establishment of secure virtualisation infrastructure. To go a step further and enhance the security of your VMware-based virtualisation infrastructure, we recommend implementing the various guides published by ANSSI and conducting a thorough risk analysis.

VMware also provides a hardening guide [14] which may prove useful when refining your security project.

14. Hardening Guide (in French): https://www.vmware.com/security/hardening-guides.html

Bibliography

[1] *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory (Recommendations for secure administration of information systems based on Microsoft Active Directory)*.
Guide ANSSI-BP-099 v1.0, ANSSI, October 2023.
https://cyber.gouv.fr/guide-admin-si-ad.

[2] *IT Backup*.
Fondamantal ANSSI-BP-100-EN v1.1, ANSSI, October 2023.
https://messervices.cyber.gouv.fr/guides/en-fundamentals-it-backup.

[3] *Security recommendations for TLS*.
Guide SDE-NT-035-EN v1.1, ANSSI, January 2017.
https://cyber.gouv.fr/en/publications/security-recommendations-tls.

[4] *Recommandations relatives à l'administration sécurisée des systèmes d'information (Recommendations for securing the administation of information systems)*.
Guide ANSSI-PA-022 v3.0, ANSSI, May 2021.
https://cyber.gouv.fr/guide-admin-si.

[5] *Authentification multifacteurs et mots de passe (Multi-factor authentification and password)*.
Guide ANSSI-PG-078 v1.0, ANSSI, October 2021.
https://cyber.gouv.fr/guide-authentification.

Version 1.0 - 02/04/2024 - ANSSI-BP-103-EN

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité