# README.

> Le script permet d'automatiser les tâches nécessaires pour se conformer aux bonnes pratiques de configuration d'un serveur hébergeant **Veeam Backup & Réplication version 12.1 et ultérieures.**

Le script peut être utilisé en production après une mise à jour vers la version 12.1, mais il peut également être employé dans le cadre de la préparation d'un serveur Veeam.

!! Ne pas lancer le script en utilisant le service de bureau à distance (RDP). Le service RDP sera inaccessible après l'exécution du script.

*Veuillez utiliser un accès distant via TeamViewer ou une alternative, ou connectez-vous directement depuis l'hyperviseur.*

## Contenu du script.

Voici la liste des points présents dans la fonctionnalité - **Security & Compliance Analyser**

- Remote Desktop Service (TermService) should be disabled
- Remote Registry service (RemoteRegistry) should be disabled
- Windows Remote Management (WinRM) service should be disabled
- Windows Firewall should be enabled

- MFA for the backup console should be enabled
- Immutable or offline (air gapped) media should be used
- Password loss protection should be enabled
- Email notifications should be enabled
- Configuration backup should be enabled and use encryption
- Backup server should not be a part of the production domain
- All backups should have at least one copy (the 3-2-1 backup rule)
- Reverse incremental backup mode is deprecated and should be avoided
- Backup jobs to cloud repositories should use encryption
- Unknown Linux servers should not be trusted automatically
- The configuration backup must not be stored on the backup server
- Host to proxy traffic encryption should be enabled for the Network transport mode
- SMBv3 signing and encryption should be enabled
- WDigest credentials caching should be disabled
- Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled
- Hardened repositories should not be hosted in virtual machines
- Deprecated versions of SSL and TLS should be disabled
- Network traffic encryption should be enabled in the backup network
- Linux servers should have password-based authentication disabled
- Windows Script Host should be disabled
- SMBv1 protocol should be disabled
- Link-Local Multicast Name Resolution (LLMNR) should be disabled
- Backup services should be running under the LocalSystem account
- Credentials and encryption passwords should be rotated at least annually
- Hardened repositories should have the SSH Server disabled

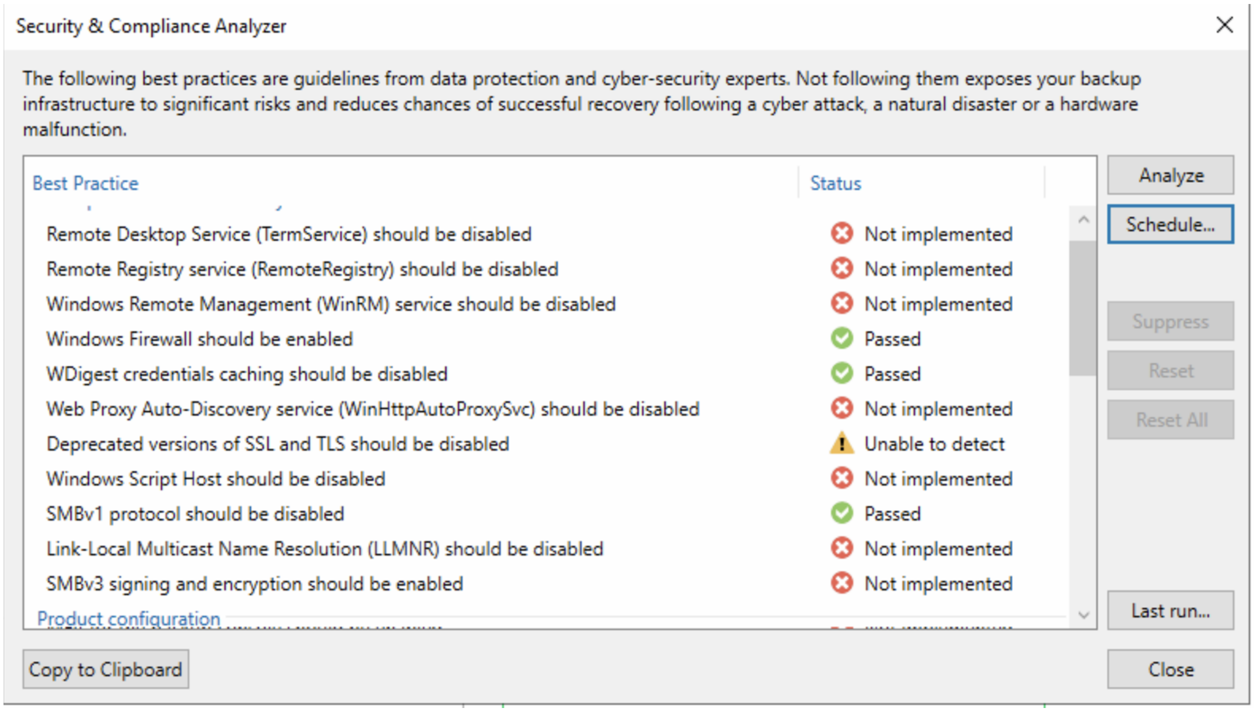
- S3 Object Lock in the Governance mode does not provide true immutability
- Latest product updates should be installed

---

Voici la **liste des points traités/corrigés** par le script :

- Remote Desktop Service (TermService) should be disabled
- Remote Registry service (RemoteRegistry) should be disabled
- Windows Remote Management (WinRM) service should be disabled
- Windows Firewall should be enabled
- Unknown Linux servers should not be trusted automatically
- SMBv3 signing and encryption should be enabled
- WDigest credentials caching should be disabled
- Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled
- Deprecated versions of SSL and TLS should be disabled
- Windows Script Host should be disabled
- SMBv1 protocol should be disabled

Analyse - Avant le script. 👇

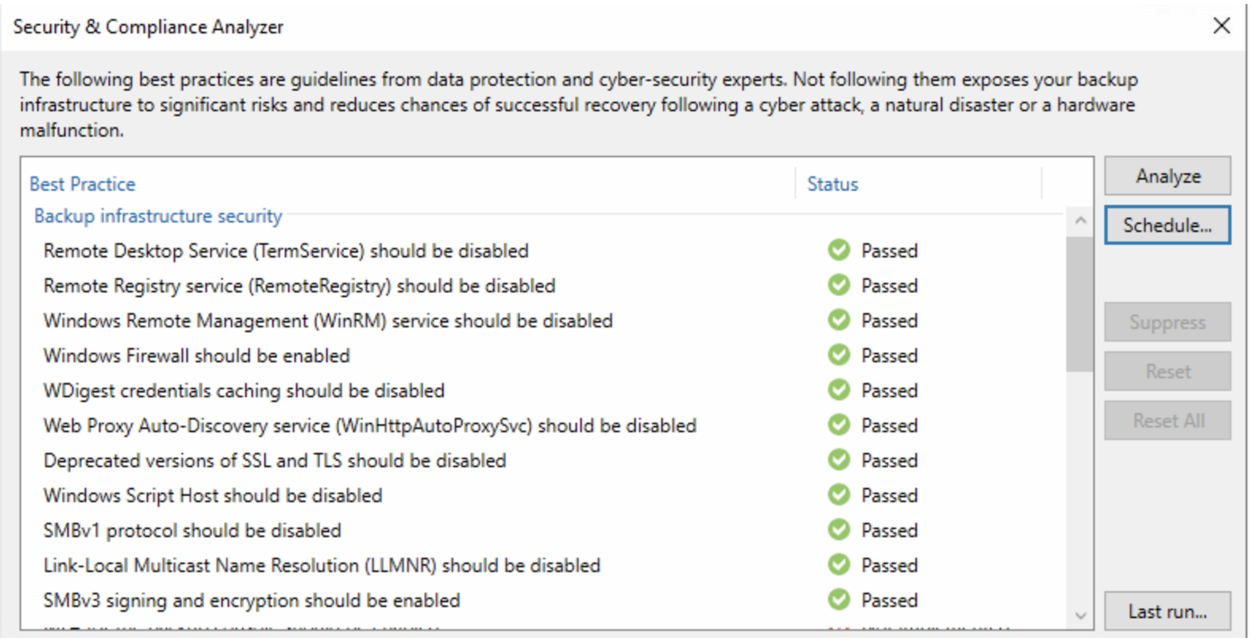


Security & Compliance Analyzer

The following best practices are guidelines from data protection and cyber-security experts. Not following them exposes your backup infrastructure to significant risks and reduces chances of successful recovery following a cyber attack, a natural disaster or a hardware malfunction.

| Best Practice | Status |
|---|---|
| Remote Desktop Service (TermService) should be disabled | ✗ Not implemented |
| Remote Registry service (RemoteRegistry) should be disabled | ✗ Not implemented |
| Windows Remote Management (WinRM) service should be disabled | ✗ Not implemented |
| Windows Firewall should be enabled | ✓ Passed |
| WDigest credentials caching should be disabled | ✓ Passed |
| Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled | ✗ Not implemented |
| Deprecated versions of SSL and TLS should be disabled | ⚠ Unable to detect |
| Windows Script Host should be disabled | ✗ Not implemented |
| SMBv1 protocol should be disabled | ✓ Passed |
| Link-Local Multicast Name Resolution (LLMNR) should be disabled | ✗ Not implemented |
| SMBv3 signing and encryption should be enabled | ✗ Not implemented |
| Product configuration | |

## Analyse - Après le script. 👇



Security & Compliance Analyzer

The following best practices are guidelines from data protection and cyber-security experts. Not following them exposes your backup infrastructure to significant risks and reduces chances of successful recovery following a cyber attack, a natural disaster or a hardware malfunction.

| Best Practice | Status |
|---|---|
| Backup infrastructure security | |
| Remote Desktop Service (TermService) should be disabled | ✓ Passed |
| Remote Registry service (RemoteRegistry) should be disabled | ✓ Passed |
| Windows Remote Management (WinRM) service should be disabled | ✓ Passed |
| Windows Firewall should be enabled | ✓ Passed |
| WDigest credentials caching should be disabled | ✓ Passed |
| Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled | ✓ Passed |
| Deprecated versions of SSL and TLS should be disabled | ✓ Passed |
| Windows Script Host should be disabled | ✓ Passed |
| SMBv1 protocol should be disabled | ✓ Passed |
| Link-Local Multicast Name Resolution (LLMNR) should be disabled | ✓ Passed |
| SMBv3 signing and encryption should be enabled | ✓ Passed |

Les points suivants **restent donc en attente** dans le cas où ils ne sont pas automatiquement validés par défaut :

- MFA for the backup console should be enabled
- Immutable or offline (air gapped) media should be used
- Password loss protection should be enabled
- Email notifications should be enabled
- Configuration backup should be enabled and use encryption
- All backups should have at least one copy (the 3-2-1 backup rule)
- Backup server should not be a part of the production domain
- Reverse incremental backup mode is deprecated and should be avoided
- Host to proxy traffic encryption should be enabled for the Network transport mode
- Backup jobs to cloud repositories should use encryption
- Hardened repositories should not be hosted in virtual machines
- The configuration backup must not be stored on the backup server
- Network traffic encryption should be enabled in the backup network
- Linux servers should have password-based authentication disabled
- Backup services should be running under the LocalSystem account
- S3 Object Lock in the Governance mode does not provide true immutability
- Hardened repositories should have the SSH Server disabled
- Credentials and encryption passwords should be rotated at least annually
- Latest product updates should be installed
- Link-Local Multicast Name Resolution (LLMNR) should be disabled

⚠ Pour valider les points ci-dessus, veuillez vous référer à la documentation VEEAM.

https://helpcenter.veeam.com/docs/backup/vsphere/best_practices_analyzer.html?ver=120