



Ansible Meetup

April 2, 2019

Microsoft Windows BitLocker Management with Ansible

Simon Bärlocher & Pascal Mages

hello@itigo.ch, 044 552 0250

Who we are



- Established in May 2016
- Corporation (AG with 179'500 CHF shares)
- 4 founders + 3 employee

Our Partners



What we do



IT-Infrastruktur for SMEs

- Telephony
- Networking / Security / Site to Site
- Workplaces
- Cloud / Remote Backup
- Printers / Screens / Projectors
- Basic Software
- IT-Support

Why BitLocker Management? ITIGO

- Default Windows Drive Encryption
- Could be managed through AD/GPO
- Deployment with Ansible
 - TPM and Recovery Key
 - other modes possible
 - Store Recovery Key somewhere

Ansible Module



```
#!/powershell

# Copyright: (c) 2019, Simon Baerlocher <s.baerlocher@sbaerlocher.ch>
# Copyright: (c) 2019, ITIGO AG <opensource@itigo.ch>
# GNU General Public License v3.0+ (see COPYING or https://www.gnu.org/licenses/gpl-3.0.txt)

#Requires -Module Ansible.ModuleUtils.ArgvParser
#Requires -Module Ansible.ModuleUtils.CommandUtil
#Requires -Module Ansible.ModuleUtils.Legacy

$ErrorActionPreference = "Stop"
Set-StrictMode -Version 2.0

$params = Parse-Args -arguments $args -supports_check_mode $true
$check_mode = Get-AnsibleParam -obj $params -name "_ansible_check_mode" -type "bool" -default $false
$diff = Get-AnsibleParam -obj $params -name "_ansible_diff" -type "bool" -default $false

$mount = Get-AnsibleParam -obj $params -name "mount" -type "str" -failifempty $true
$state = Get-AnsibleParam -obj $params -name "state" -type "str" -default "enabled" -validateset "enabled", "disabled"
$keyprotector = Get-AnsibleParam -obj $params -name "keyprotector" -type "str" -validateset "RecoveryPasswordProtector", "TpmProtector"

# Create a new result object
$result = @{
    changed = $false
}

$protectionstatus = (Get-BitLockerVolume -MountPoint $mount).ProtectionStatus
```

Ansible Module



```
if ($state -eq "enabled") {  
    if ( $protectionstatus -eq "Off" ) {  
        if (-not $check_mode) {  
            if ( $keyprotector -eq "RecoveryPasswordProtector" ) {  
                $res = Enable-BitLocker -MountPoint $mount -RecoveryPasswordProtector  
            } elseif ( $keyprotector -eq "TpmProtector" ) {  
                $res = Enable-BitLocker -MountPoint $mount -TpmProtector  
            }  
            $result.res = $res  
        }  
        $result.changed = $true  
    }  
}  
  
if ($state -eq "disabled") {  
    if ( $protectionstatus -eq "On" ) {  
        if (-not $check_mode) {  
            Disable-BitLocker -MountPoint $mount  
        }  
        $result.changed = $true  
    }  
}  
  
# Return result  
Exit-Json -obj $result
```

How it works with Ansible



- Checks if TPM chip is available
- BitLocker Module encrypts drive

► DEMO

Next steps



- Modules will be upstreamed

Questions?



hello@itigo.ch

044 552 0250

www.itigo.ch



IT-Infrastructure | IT-Support | IT-Consulting