BitLocker recovery in Microsoft Azure

Published Date: Jul 19, 2024

Objective

- BitLocker recovery in Microsoft Azure

Applies To

- Microsoft Azure
- Supported versions of the Falcon sensor for Windows
- Supported versions of Microsoft Windows
- Prerequisites:
    - **Azure AD:** Ensure your machines are joined to Azure AD
    - **Azure Automation:** Set up Azure Automation to manage your scripts
    - **BitLocker Recovery Key:** Ensure you have access to BitLocker recovery keys
- May be related to Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19

Procedure

1. Create an Azure Automation Account:

a. Sign in to the Azure portal
b. Navigate to "Automation Accounts" and click "**Add**" to create a new Azure Automation account

2. Develop a PowerShell Script – The script will handle booting into safe mode, changing the registry key, and rebooting into normal mode. However, since BitLocker is enabled, you'll need to ensure you have the recovery key.

```
# CrowdStrikeFix.ps1
# This script deletes the problematic CrowdStrike driver file causing
BSODs and reverts Safe Mode

$filePath = "C:\Windows\System32\drivers\CrowdStrike\C-00000291*.sys"
$files = Get-ChildItem -Path $filePath -ErrorAction SilentlyContinue

foreach ($file in $files) {
    try {
```

```
        Remove-Item -Path $file.FullName -Force
        Write-Output "Deleted: $($file.FullName)"
    } catch {
        Write-Output "Failed to delete: $($file.FullName)"
    }
}

# Revert Safe Mode Boot after Fix
bcdedit /deletevalue {current} safeboot
Restart-Computer -Force
```

3. Retrieve BitLocker Recovery Keys:

a. Use Azure AD to retrieve BitLocker recovery keys
b. Navigate to **Azure AD > Devices > All Devices**
c. Click on the specific device and select **"Show Recovery Key"**
d.

```
# Example of retrieving BitLocker recovery key
$bitLockerKey = Get-BitLockerVolume | Select-Object -ExpandProperty
KeyProtector | Where-Object { $_.KeyProtectorType -eq 'RecoveryPassword'
} | Select-Object -ExpandProperty RecoveryPassword
```

4. Deploy the Script with Azure Automation:

a. Upload the PowerShell script to Azure Automation
b. Create a Runbook and link it to your script
c. Test the Runbook on a single machine to ensure it works correctly

5. Automate Deployment:

a. Use Azure Automation to run the script on all impacted machines
b. Ensure the script includes error handling and logging

6. Monitor and Validate:

a. Monitor the deployment process
b. Validate that the machines are booting correctly into normal mode after the script runs

Additional Information

- **Azure Update Management:** Consider using Azure Update Management to push updates and scripts
- **Windows Admin Center:** Use Windows Admin Center for easier management and monitoring of your devices
- **Backup:** Ensure you have backups of important data before making changes to registry and system files

Example Use Case with Azure Automation

1. **Create a Runbook in Azure Automation:**
    a. Go to your Azure Automation account
    b. Click on "Runbooks" and create a new Runbook
    c. Paste your PowerShell script into the Runbook editor
2. **Schedule the Runbook:** Schedule the Runbook to run at a specific time or trigger it manually
3. **Monitor Runbook Execution:** Use the job output to monitor the success and any errors

Options if you lost or have difficulties to find your recovery key

If you have lost the BitLocker recovery key, the options for recovery are limited. However, you can try the following steps:

1. **Check for Stored Recovery Keys**
    - **Azure Active Directory (Azure AD):**
        a. Go to the Azure portal
        b. Navigate to Azure AD > Devices > All Devices
        c. Select the device and check if the BitLocker recovery key is listed
    - **Active Directory (AD):**
        a. Open the Active Directory Users and Computers snap-in
        b. Right-click on the computer object and select "Properties."
        c. Go to the "BitLocker Recovery" tab to see if the key is stored
    - **Microsoft Account:**
        a. Go to the Microsoft account website
        b. Log in with the associated Microsoft account
        c. Check for recovery keys under the "Devices" section
2. **Use Microsoft Support** – Contact Microsoft Support for assistance. They may have additional methods to help retrieve the recovery key, especially if the devices are managed through enterprise solutions.

3. **Prevent Future Loss**
    - **Backup Recovery Keys:** Ensure that recovery keys are backed up in multiple secure locations
    - **Document Management:** Implement a policy for documenting and storing recovery keys securely

Example: Checking Azure AD for Recovery Keys

1. Log in to the Azure Portal
2. Navigate to "Azure Active Directory" in the left-hand menu
3. Under "Manage," select "Devices."
4. Locate and select the device in question
5. View the recovery key in the "BitLocker Keys" section

Example: Checking Microsoft Account for Recovery Keys

1. Log in to the Microsoft Account
2. Sign in with the Microsoft account associated with the device
3. View the list of recovery keys saved to your account and locate the key for the device in question

See also

- BitLocker recovery in Microsoft environments using SCCM
- BitLocker recovery in Microsoft environments using Active Directory and GPOs
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager
- BitLocker recovery in Microsoft environments using ManageEngine Desktop Central
- BitLocker recovery in Microsoft environments using BigFix