QA Checks
User Guide

Informational Documentation

This document is intended for engineers who build and maintain servers.
End users should not be running the QA scripts.

Note: This document refers to version 3.0 and above.

Contents

Overview

The QA Checks (aka scripts) came about as a need to verify the build of new servers into our corporate environments. All servers should be built from a standard gold build image; however this image still lacks many of the additional tools and configuration settings that are needed before a server can be taken in to support.

Technical Details

The scripts are written using the Microsoft PowerShell scripting language, with a minimum version of 2.0. This is due to Windows Server 2008 R2 (the lowest supported operating system) having this version installed by default.

The scripts can be run on any Windows operating system as long as PowerShell version 2 or greater is installed, and the PowerShell command window is run with administrative privileges. The supported operating systems are listed below...

Supported Operating Systems

Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2

Unsupported Operating Systems (but still work)

Windows 2003 Server	
Windows Server 2016 Technical Preview	- No known issues

While the scripts will work on desktop operating systems, they were designed with servers OSes in mind.

How To Use

Quick Start

The following steps will run a QA check against the local server you are currently on:

1. Open a PowerShell console with elevated administrative privileges
2. Change to the correct folder for where the scripts are held
3. If required, enter: `Set-ExecutionPolicy Unrestricted –Force`
4. Enter: `.\QA.PS1 .` (*note the full stop at the end of the command*)

Detailed Instructions

To Start

You will need to open a PowerShell console with elevated administrative privileges. To do this, right click the PowerShell icon on the toolbar or start menu, and choose **Run as administrator**.

You may need to run a command before scripts can be run on the server, it will depend on the group policy settings for the environment. If you get the following error message when running the QA scripts, then run the command below.

```
.\qa.ps1 : File c:\qa\qa.ps1 cannot be loaded. The file c:\qa\qa.ps1 is not digitally
signed. You cannot run this script on the current system. For more information about
running scripts and setting execution policy, see about_Execution_Policies at
http://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\qa.ps1
+ ~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

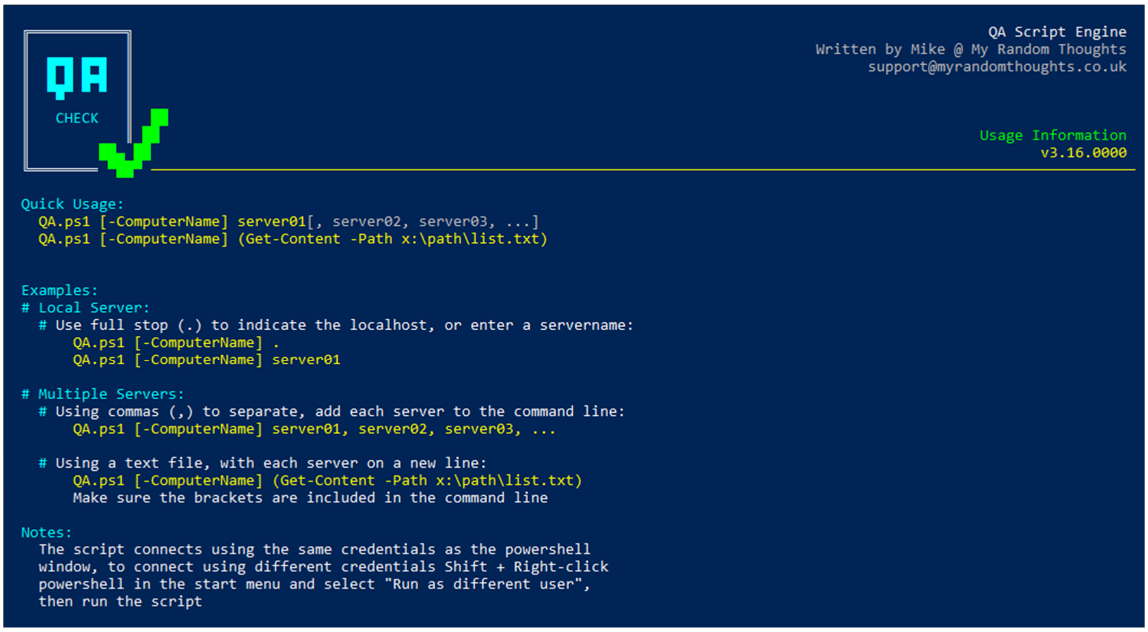
Type the following command in the PowerShell window:

```
Set-ExecutionPolicy -ExecutionPolicy Bypass –Force
```

See the Microsoft TechNet page https://technet.microsoft.com/library/hh847748.aspx for more information.

Help Screen

To get the help screen, simply run `.\QA.PS1`. This details all the ways that the tool can be used.



```
                                                             QA Script Engine
                                             Written by Mike @ My Random Thoughts
                                                  support@myrandomthoughts.co.uk

                                                            Usage Information
                                                                  v3.16.0000

Quick Usage:
  QA.ps1 [-ComputerName] server01[, server02, server03, ...]
  QA.ps1 [-ComputerName] (Get-Content -Path x:\path\list.txt)


Examples:
# Local Server:
  # Use full stop (.) to indicate the localhost, or enter a servername:
      QA.ps1 [-ComputerName] .
      QA.ps1 [-ComputerName] server01

# Multiple Servers:
  # Using commas (,) to separate, add each server to the command line:
      QA.ps1 [-ComputerName] server01, server02, server03, ...

  # Using a text file, with each server on a new line:
      QA.ps1 [-ComputerName] (Get-Content -Path x:\path\list.txt)
      Make sure the brackets are included in the command line

Notes:
  The script connects using the same credentials as the powershell
  window, to connect using different credentials Shift + Right-click
  powershell in the start menu and select "Run as different user",
  then run the script
```

To Run against current server only

Execute the following command to run the QA checks against the current server:

```
.\QA.PS1 .
```

The full stop at the end is a shortcut that means the localhost.

To Run against multiple servers

There are two ways to run the checks against more than one server. You can either type in each of the servers on the command line, or put them all into a text file, one server per line:

```
.\QA.PS1 -ComputerName server01, server02, server03, ...
.\QA.PS1 -ComputerName (Get-Content –Path c:\path\list.txt)
```

The second line above shows the use of a PowerShell command that opens the listed file (c:\qa\serverlist.txt) and puts the contents of that file on the command line. Note: the open and close brackets are important.

Checks

Introduction

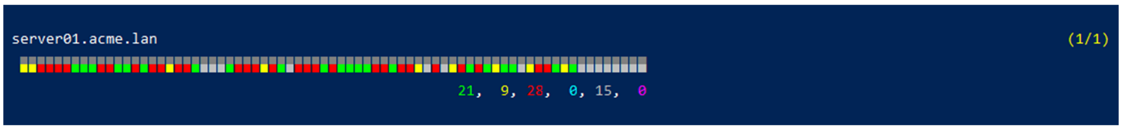
For a full list of sections, checks, including their descriptions, see **Appendix A**.

There are currently over 70 checks split into 9 sections, which are performed whenever the QA Check script is executed. These can take anywhere from 30 seconds to a couple of minutes to run, depending on the server running the script. If you are checking against more than one server, each server is checked one at a time; however the checks are performed concurrently, up to 5 at a time.

Each check is written to be as efficient as possible; however there are factors outside of its control. Networking could be taking a big hit at the time; the remote server (if running against multiple servers) may be busy with some task. With this in mind each check is set with a timeout value of about 60 seconds. This gives the checks time to try to complete their task.

Script Output

When running the checks, a coloured bar will appear to show you the current progress of the checks and the results so far. As some checks will complete faster than others, the progress bar will appear to stop and start in spurts – this is normal.



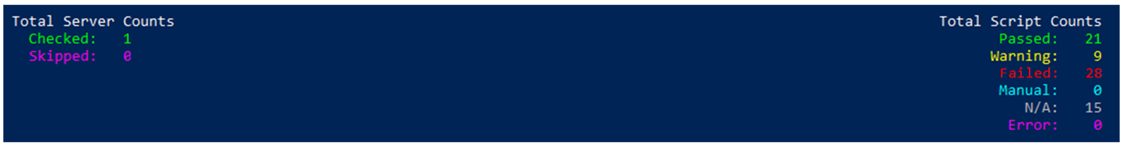
```
server01.acme.lan                                                                      (1/1)

                                         21,  9, 28,  0, 15,  0
```

The screen shot above shows a completed servers progress bar. As you can see there are quite a lot of passes (**green**), a couple of warnings (**yellow**) and a few failed checks (**red**). The other colours shown are for manual checks (**blue**) and not applicable (**grey**). There is one other colour that is not shown; it is for when a check may fail for some reason. This is shown as a **purple** bar.

Once each server has been checked, the results are saved as a HTML report file in **X:\QA\Reports\** (*Where **X:** is the system drive*). This file has detailed information about the check performed and the results.

Shown below, is a full analysis of the results which is also given, as well as HTML and CSV files that have been created containing the full results breakdown.



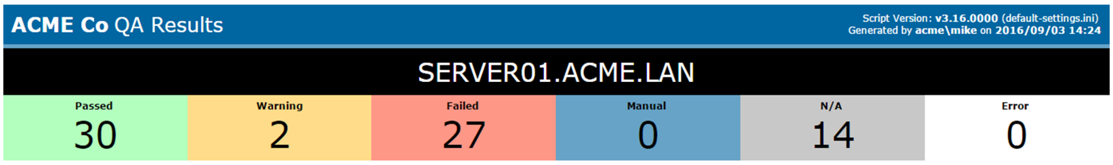
```
Total Server Counts                                                        Total Script Counts
  Checked:    1                                                               Passed:   21
  Skipped:    0                                                              Warning:    9
                                                                              Failed:   28
                                                                              Manual:    0
                                                                                 N/A:   15
                                                                               Error:    0
```

HTML Report

The HTML report gives a good visual overview of the results, as well as any details about why a particular check passed or failed. There is also hover help for each of the checks detailing more information about the particular check, if the command line argument for adding help was specified (see below).

Locate the HTML report folder, usually C:\QA\Reports, and look for the servers' report you want to view. Each server checked will have their own individual report file. Open the report in your browser of choice.

The top header row shows the same detail as the analysis totals in the PowerShell command window, giving additional detail on who ran the report and when. It also shows the version of the script used, so that you can check to see if the latest (or close to it) script was used. Newer scripts will have bug fixes and maybe even additional checks.



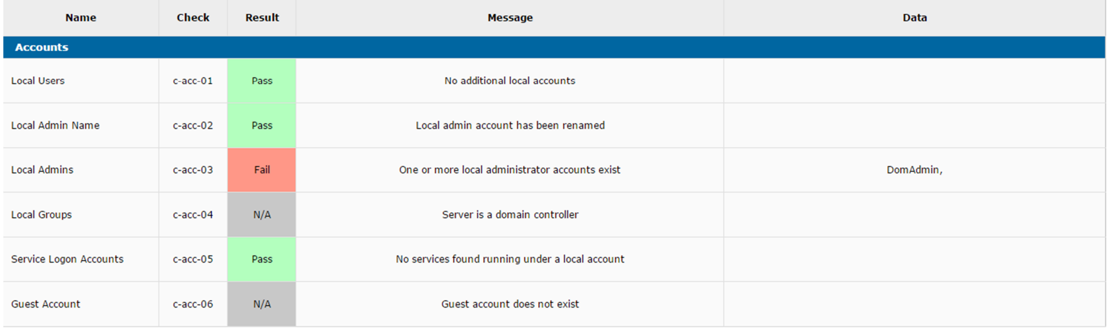
ACME Co QA Results

Script Version: **v3.16.0000** (default-settings.ini)
Generated by **acme\mike** on **2016/09/03 14:24**

SERVER01.ACME.LAN

Passed	Warning	Failed	Manual	N/A	Error
30	2	27	0	14	0

Below this are all the checks in a table format. The image below shows the first 5 checks of an example server

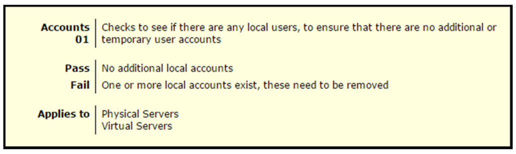


Name	Check	Result	Message	Data
Accounts				
Local Users	c-acc-01	Pass	No additional local accounts	
Local Admin Name	c-acc-02	Pass	Local admin account has been renamed	
Local Admins	c-acc-03	Fail	One or more local administrator accounts exist	DomAdmin,
Local Groups	c-acc-04	N/A	Server is a domain controller	
Service Logon Accounts	c-acc-05	Pass	No services found running under a local account	
Guest Account	c-acc-06	N/A	Guest account does not exist	

The columns in the table are:

Name	The friendly name of the check that was executed
Check	The function name
Result	The result of the check
Message	A short message detailing the result reason
Data	Specific data on the check result

When you hover over the result box, a small window will appear that gives more information on the check and shows what the possible values are for that check. This hover help is still being added and may lack some detail.



Accounts 01	Checks to see if there are any local users, to ensure that there are no additional or temporary user accounts
Pass	No additional local accounts
Fail	One or more local accounts exist, these need to be removed
Applies to	Physical Servers Virtual Servers

An optional command line parameter will remove this help popup; simply add the following to the end of your QA command line.

```
-SkipHTMLHelp
```

This will reduce the report file size from about 51KB to about 18KB.

CSV Report

There is also an option to generate a CSV report. Tools and applications that can read and parse the CSV format can be applied to this output file for running automated checks and reports against. It will be called results.csv.

Unlike the HTML file, only one CSV file is generated which holds the data for all the servers that are checked. The CSV file has the following columns:

Server	The name of the server this row is for
Name	The friendly name of the check that was executed
Check	The function name
Datetime	The date and time the check was started
Result	The result of the check
Message	A short message detailing the result reason
Data	Specific data on the check result

In order to generate this CSV file, add the following to the end of the command line...

```
-GenerateCSV
```

Appendix A – List Of Checks

There are currently over 70 checks split into 9 sections, which are detailed below.
Column headers are as follows:

C: Check number
A: Server type that the check applies to:
P: Physical servers
V/H: Virtual servers (VMware/Hyper-V)
D/T: Domain Controllers or Terminal Servers
Blank: All servers

Accounts

C	Check	Description	A
01	Local Users	Checks if any local user accounts exist	
02	Local Admin Name	Checks that the local admin account has been renamed	
03	Local Admins	Checks if any non-standard accounts are local admins	
04	Local Groups	Checks if any non-standard groups exist	
05	Service Logon Accounts	Checks if any services are running under non-standard accounts	
06	Guest Account Status	Checks if the guest account is disabled	

Compliance

C	Check	Description	A
01	McAfee Antivirus Installed	Check if McAfee is installed	
02	SCOM Monitoring Installed	Check if SCOM monitoring is installed	
03	SCCM Agent Installed	Check if the SCCM process is running (CcmExec.exe)	
04	NetBackup Client Installed	Check if NetBackup is installed, or VADP is used	
05	Last Windows Update Patch Date	Check when windows was last patched	
06	WSUS Server	Check if a WSUS server is configured	
07	Sentinel Agent Installed	Check if the Sentinel agent is installed	

Drives

C	Check	Description	A
01	System Drive Size	Checks the system drive is 50gb or larger	
02	Minimum Drive Free Space	Checks all drives have at least 17% free space	
03	Page file size and location	Checks the size and location of the page file	
04	CD/DVD Drive Letter	Checks the drive letter of the CD/DVD drive	
05	Shared Folders	Checks if any shared folders are available	
06	SAN Storage Agent	Checks if SAN storage agent software is installed	P
07	Disk Management Agent	Checks if any disk management software is installed	P
08	Drive NTFS Format	Checks all drives are formatted as NTFS	

Hyper-V Host

C	Check	Description	A
01	Not Server Core	Checks if server is Core edition or not	
02	No Other Server Roles	Checks that no other server roles exist	
03	VM Location	Checks that all VMs are not stored on the system drive	

Network

C	Check	Description	A
01	IPv6 Disabled	Checks if IPv6 is disabled globally or per NIC	
02	Unused Network Interfaces	Checks if all DHCP NICs are disabled	
03	Network Adapter Labels	Checks if “Production” or “Management” NIC labels exist	
04	Binding Order	Check the binding order of all NICs	
05	Network Speed / Duplex	Checks if the speed and duplex are set correctly	
06	Network Agent	Checks if network management software is installed	P
07	Network Teaming	Checks if teaming software is installed	
08	Management Adapter	Checks if a management adapter is configured	
09	Static Routes	Checks to make sure static routes are configured correctly	

Regional

C	Check	Description	A
01	Local Time	Checks if a time source is set and the time is correct	
02	Time Zone Setting	Checks if the time zone is correct	
03	Location Setting	Checks if the location is set correctly	
04	Language Setting	Checks if the language is set correctly	

Security

C	Check	Description	A
01	SSL Ciphers	Checks if the SSL ciphers are set correctly	
02	SSL Hashes	Checks if the SSL hashes are set correctly	
03	SSL Key Exchange Algorithm	Checks if the SSL KEAs are set correctly	
04	SSL Protocols	Checks if the SSL protocols are set correctly	
05	SSL Cipher Order	Checks if the SSL cipher order is set correctly	
06	Reject Enumerate Accounts	Checks if anonymous enumeration of accounts is disabled	
07	Reject Enumerate Shares	Checks if anonymous enumeration of shares is disabled	
08	Domain Credential Caching	Checks if domain caching is disabled	
09	Elevated Admin Request	Checks if “Prompt for credentials” is set for elevated requests	
10	Restrict Named Pipes Access	Checks if anonymous enumeration of named pipes is disabled	
11	IIS Default Page	Checks if the default IIS page is disabled	
12	SMB Signing	Checks if SMB signing is turned on	
13	RSA Authentication	Checks if the RSA authentication software is installed	D
14	Windows Firewall Rules	Checks if there are no additional rules in the Windows firewall	
15	Windows Firewall State	Checks the state of the Windows firewall	

System

C	Check	Description	A
01	Pending Reboot	Checks if the server is waiting for a reboot operation	
02	Windows License Status	Checks if windows is licenced	
03	Services Not Started	Checks if any automatic services that are not started	
04	Services Not Stopped	Checks if specific services are correctly stopped and disabled	
05	System Event Log	Checks if any errors are in the system event log	
06	Application Event Log	Checks if any errors are in the application event log	
07	System Devices Status	Checks if any devices are “unknown”	
09	Scheduled Tasks	Checks if any non-standard scheduled tasks exists	
10	Print Spooler	Checks if the printer spooler folder has been moved	
11	Auto Run Status	Checks if AutoRun is disabled	
12	SNMP Configuration	Checks if SNMP is installed and configured	
13	Domain User Logon	Checks that current user is logged with a domain account	
14	Power Plan	Checks if the power plan is set to “High Performance”	
15	Hibernation	Checks if hibernation is disabled	
16	Remote Desktop Enabled	Checks if RDP is enabled with secure connections	
17	Terminal Services Licensed	Checks if a terminal server has a licence server configured	T

VMs – Hyper-V

C	Check	Description	A
	Currently No Checks Available		H

VMs - VMware

C	Check	Description	A
01	Tools Upgrade Status	Checks if the VMware tools can be upgraded	V
02	Time Sync Disabled	Checks if the server is getting time updates from its host	V
03	NIC Type	Checks that all NICs are set as VMXNET3	V
04	LSI SAS Controller	Checks that all controllers are set as LSI SAS	V
05	SCSI Drive / Controller Count	Checks there are no more than 7 drives per controller	V
06	Total VM Size	Checks if the VM is larger than 1Tb	V
07	CD/DVD Or Floppy Mounted	Checks if any CD/DVD or floppy images are mounted	V

Appendix B – Command Line Options

Listed below are all the command line options available for the QA scripts. Some of them you will not need, they are for advanced testing or a specific set of users.

`QA.ps1`

`-ComputerName`	Allows you to add one or more servers to scan.
`-SkipHTMLHelp`	Removes hover-help from the resulting HTML output file.
- GenerateCSV	Also outputs a “results.csv” file with all the results.
`-Help`	Shows the help screen.
`-Verbose`	Performs one check at a time, for use when debugging checks.