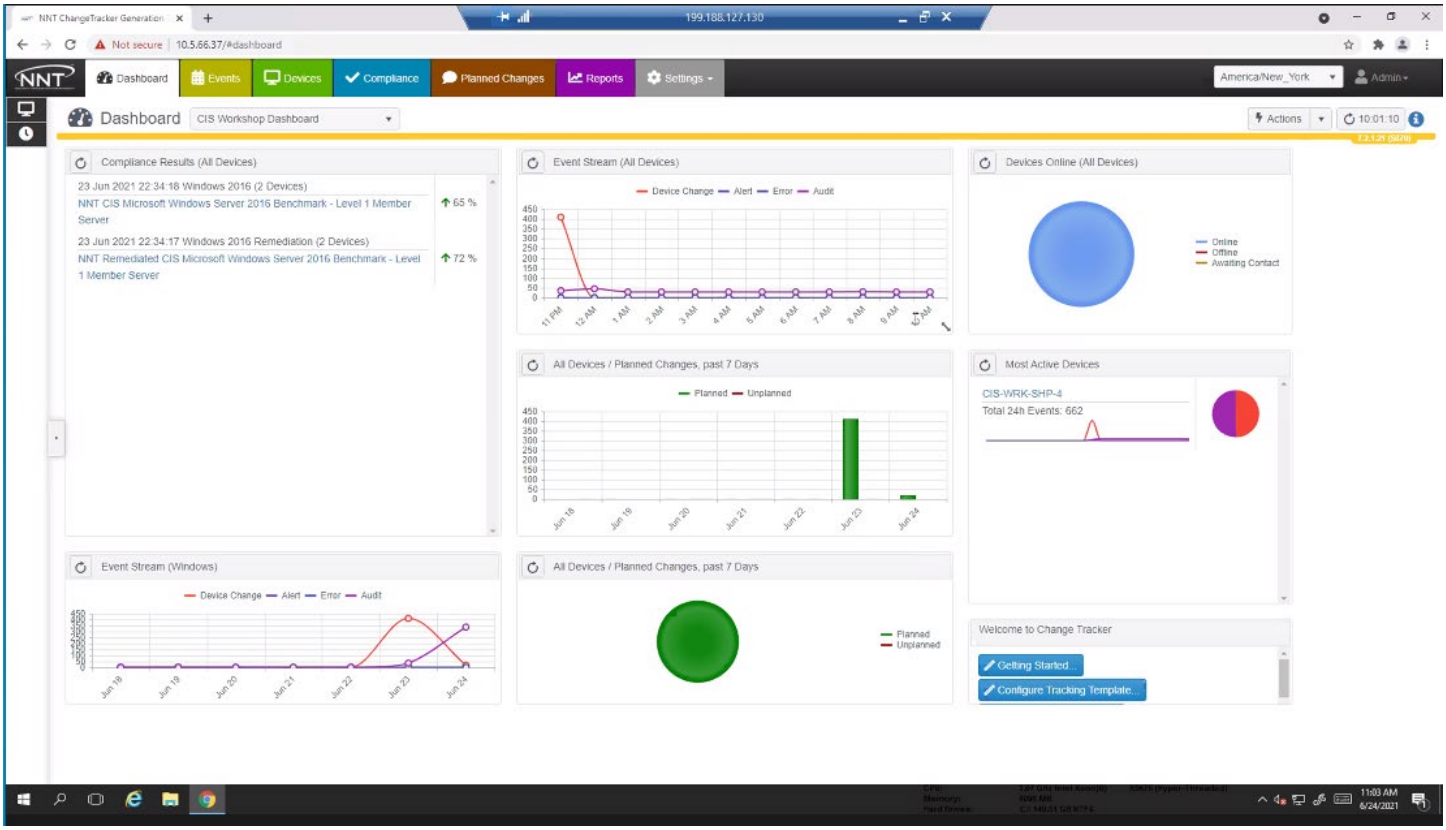
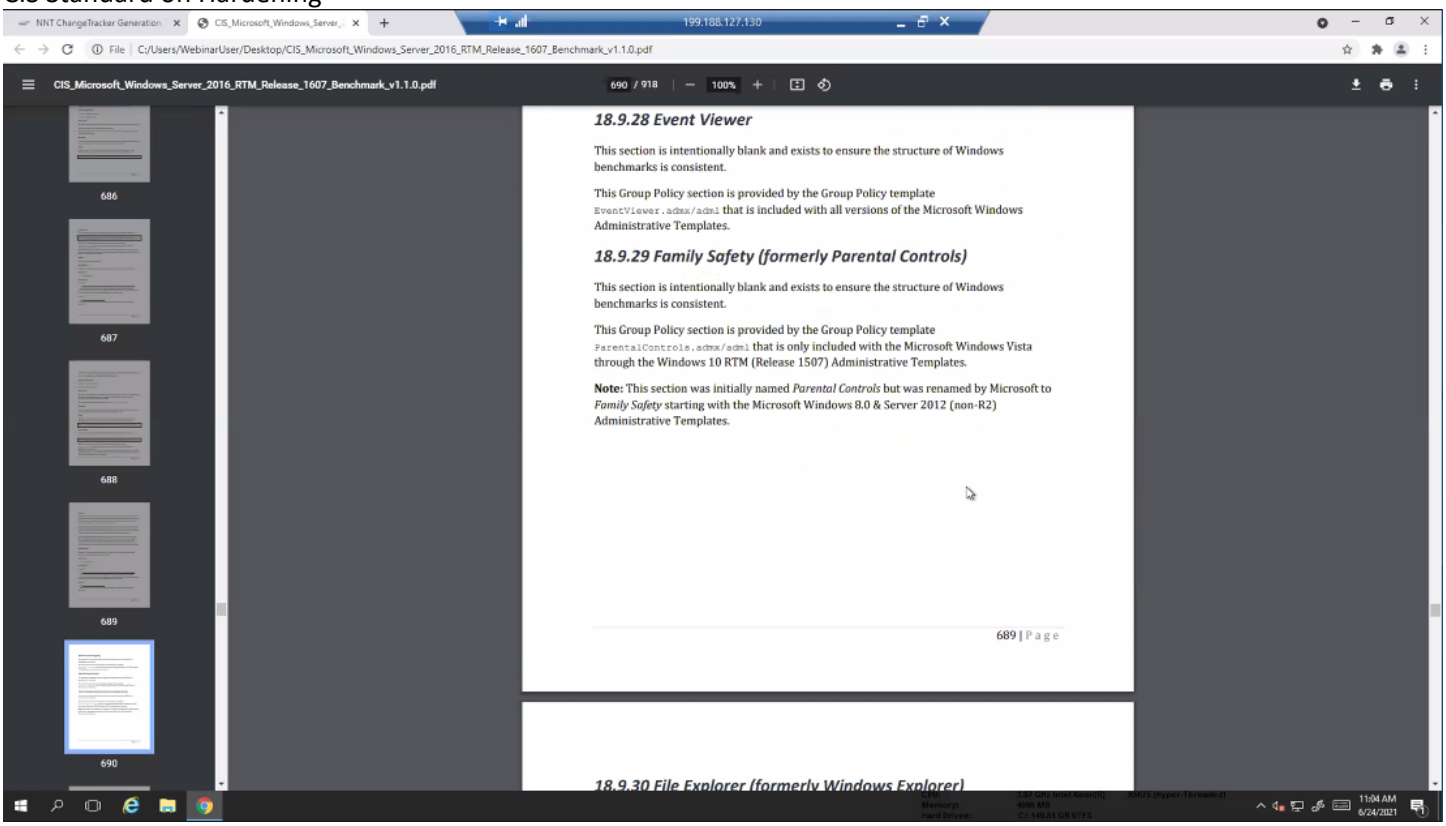


CIS Standard on Hardening



18.9.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 32,768 or greater.`

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSiz
e
```

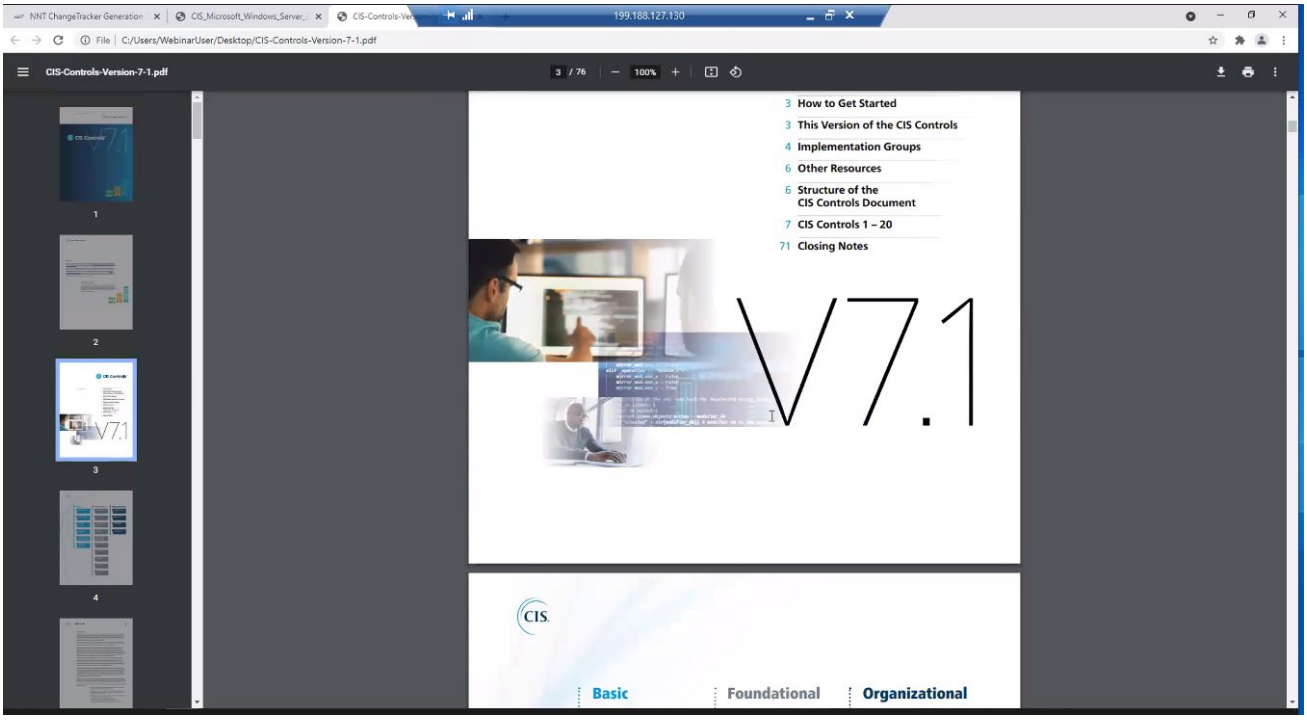
Remediation:

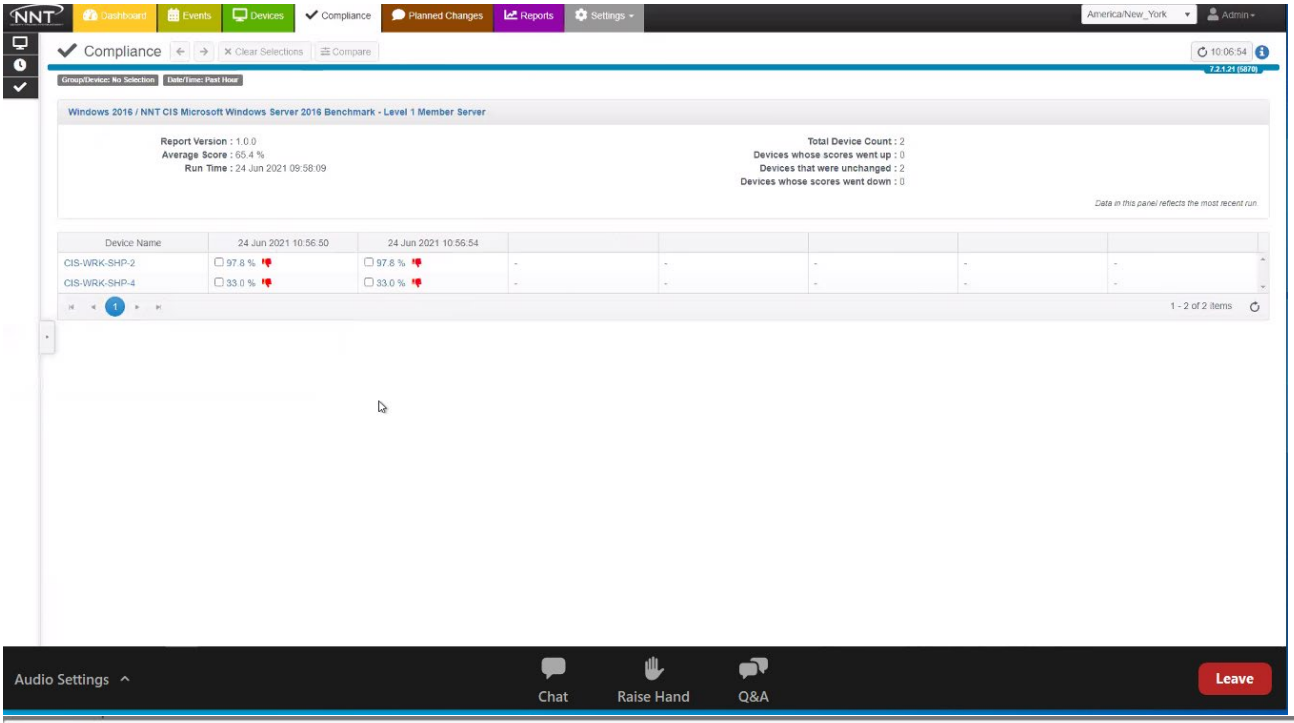
To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater:`

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\System\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

CIS Controls v7.1





Change Details

Rule Title	CIS-WRK-SHP-2	CIS-WRK-SHP-4	Reason for change
2.2.21 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	✔	✘	FAILED: (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' : securitypolicy (). Remediation : To establish the recommended configuration via GP, set the following UI path to include Guests, Local account:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact:If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.
2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	✔	✘	FAILED: (L1) Ensure 'Restore files and directories' is set to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To establish the recommended configuration via GP, set the following UI path to Administrators:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories Impact:If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.
			FAILED: (L1) Ensure 'Shut down the system' is set to 'Administrators' : securitypolicy

Account Lockout Policy

Account Policies Rules

1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'

Pass

Pass: PASSED: '15'.

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Pass

Pass: PASSED: '5'.

1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'

Pass

Pass: PASSED: '15'.

Local Policies

User Rights Assignment

Local Policies Rules

2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'

Pass

Pass: PASSED: securitypolicy ().

2.2.2 (L1) Configure 'Access this computer from the network'

Pass

Pass: PASSED: securitypolicy (2 items: NT AUTHORITY\AUTHENTICATED USERS, BUILTIN\ADMINISTRATORS).

2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'

Pass

Pass: PASSED:.

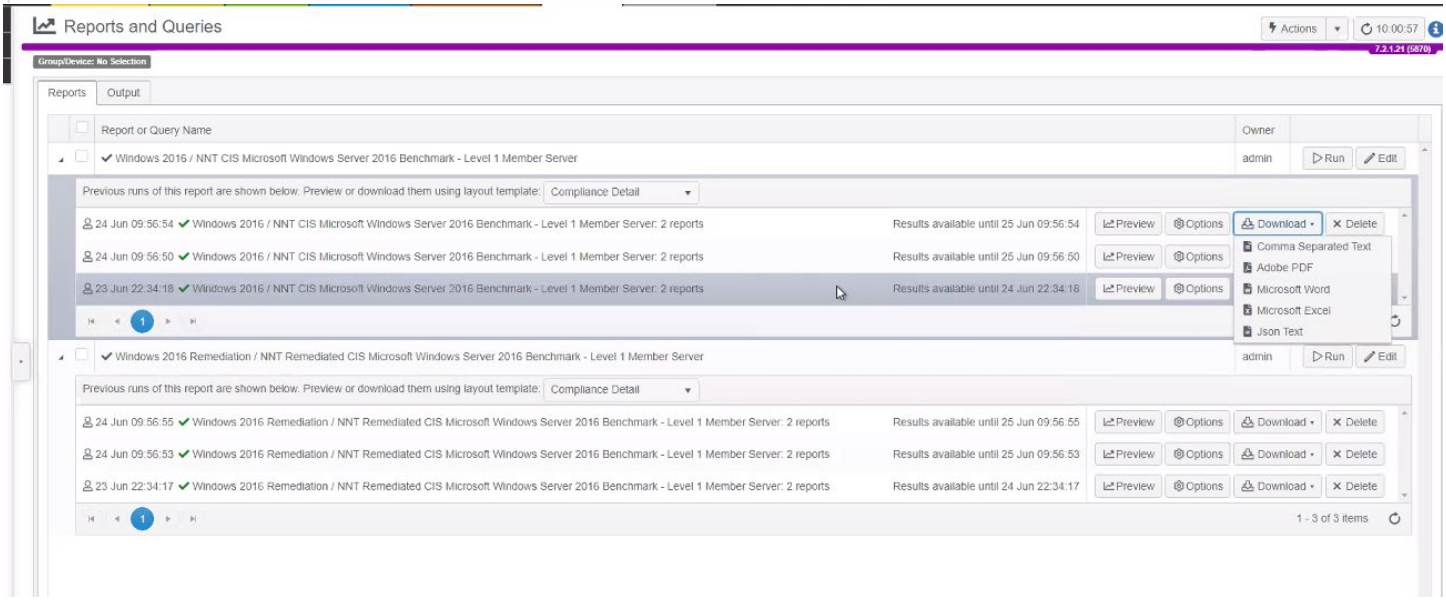
2.2.5 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

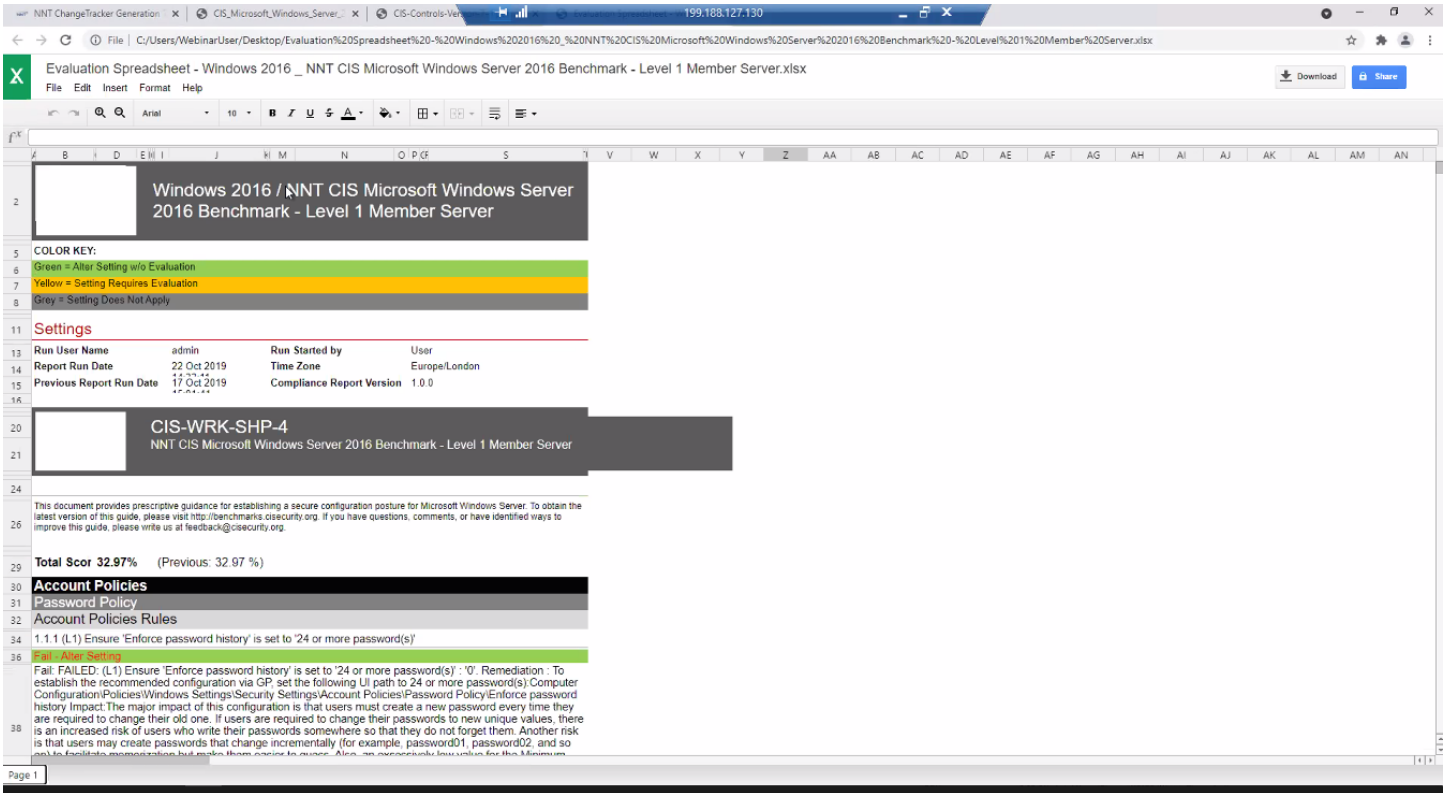
Pass

Pass: PASSED: securitypolicy (3 items: NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, BUILTIN\ADMINISTRATORS).

2.2.6 (L1) Configure 'Allow log on locally'

Pass





Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account Impact:You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.).

2.3.1.6 (L1) Configure 'Accounts: Rename guest account'

Fail - Alter Setting

Fail: FAILED: (L1) Configure 'Accounts: Rename guest account' : '"Guest"'. Remediation : To establish the recommended configuration via GP, configure the following UI path:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account Impact:There should be little impact, because the Guest account is disabled by default.

Audit Rules

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Fail - Alter Setting

Fail: FAILED: (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' : ''. Remediation : To establish the recommended configuration via GP, set the following UI path to Enabled:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Impact:None - this is the default configuration.

Devices Rules

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'

Fail - Alter Setting

Fail: FAILED: (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' : ''. Remediation : To establish the recommended configuration via GP, set the following UI path to Administrators:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact:None - this is the default configuration.

Interactive logon Rules

2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'

Fail - Alter Setting

Fail: FAILED: (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' : '0'. Remediation : To establish the recommended configuration via GP, set the following UI path to Enabled:Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name Impact:The name of the last user to successfully log on is not be displayed in the Windows logon screen.

2.3.7.3 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'

Fail - Alter Setting

Fail: FAILED: (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' :

setting to reduce help desk calls.Note: With this setting configured as recommended, the default error message displayed when a user attempts to perform an operation or run a program requiring privilege elevation (without Administrator rights) is "This program will not run. This program is blocked by group policy. For more information, contact your system administrator." Some users who are not used to seeing this message may believe that the operation or program they attempted is specifically blocked by group policy, as that is what the message seems to imply. This message may therefore result in user questions as to why that specific operation/program is blocked, when in fact, the problem is that they need to perform the operation or run the program with an Administrative account (or "Run as Administrator" if it is already an Administrator account), and they are not doing that.

Windows Firewall With Advanced Security

Domain Profile

Windows Firewall With Advanced Security Rules

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'

Fail - Setting Does Not Apply - Utilizing 3rd Party Tool

Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' : .". Remediation : To establish the recommended configuration via GP, set the following UI path to On (recommended):Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall state Impact:None - this is the default configuration.

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'

Fail - Setting Does Not Apply - Utilizing 3rd Party Tool

Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' : .". Remediation : To establish the recommended configuration via GP, set the following UI path to Block (default):Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound connections Impact:None - this is the default configuration.

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'

Fail - Setting Does Not Apply - Utilizing 3rd Party Tool

Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' : .". Remediation : To establish the recommended configuration via GP, set the following UI path to Allow (default):Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections Impact:None - this is the default configuration.

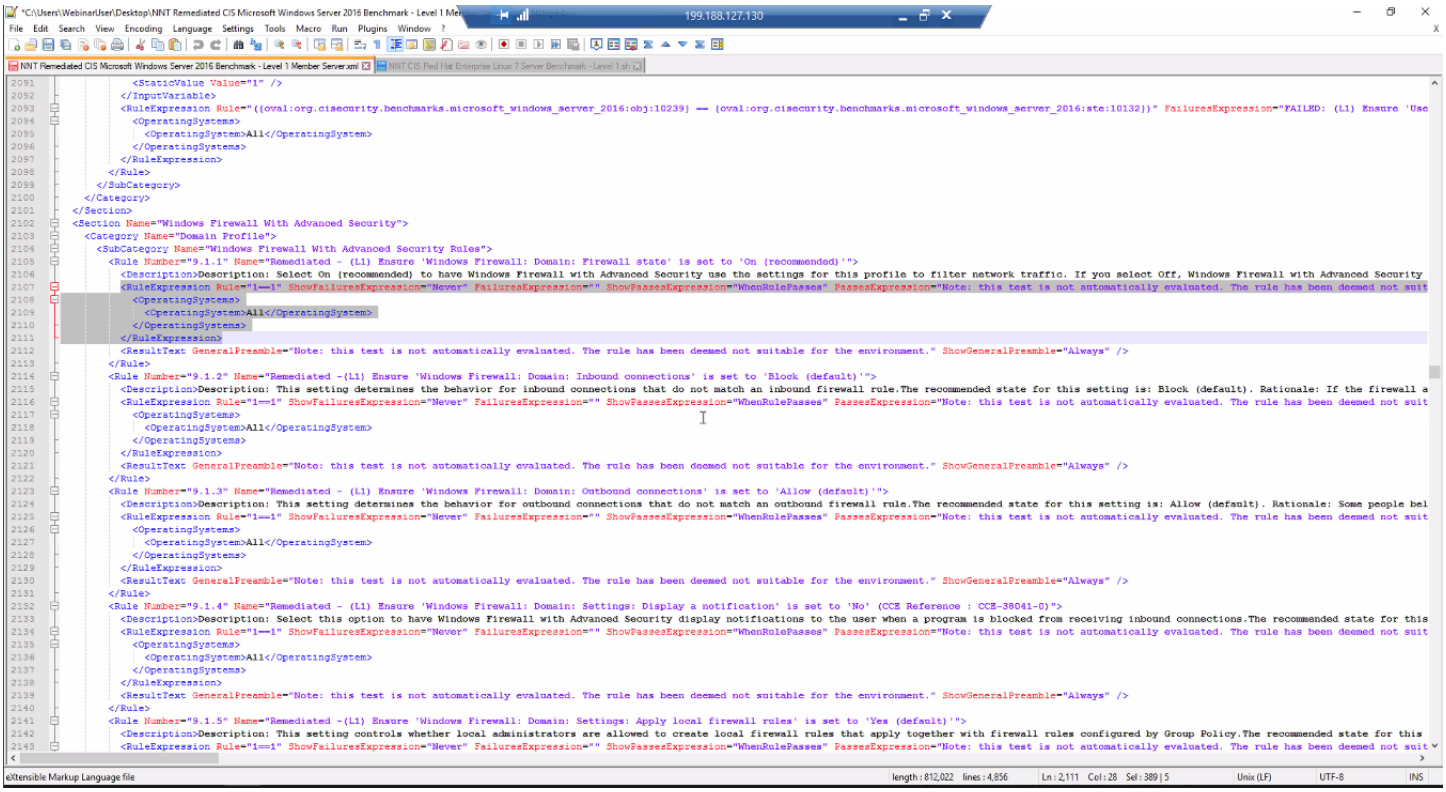
9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-38041-0)

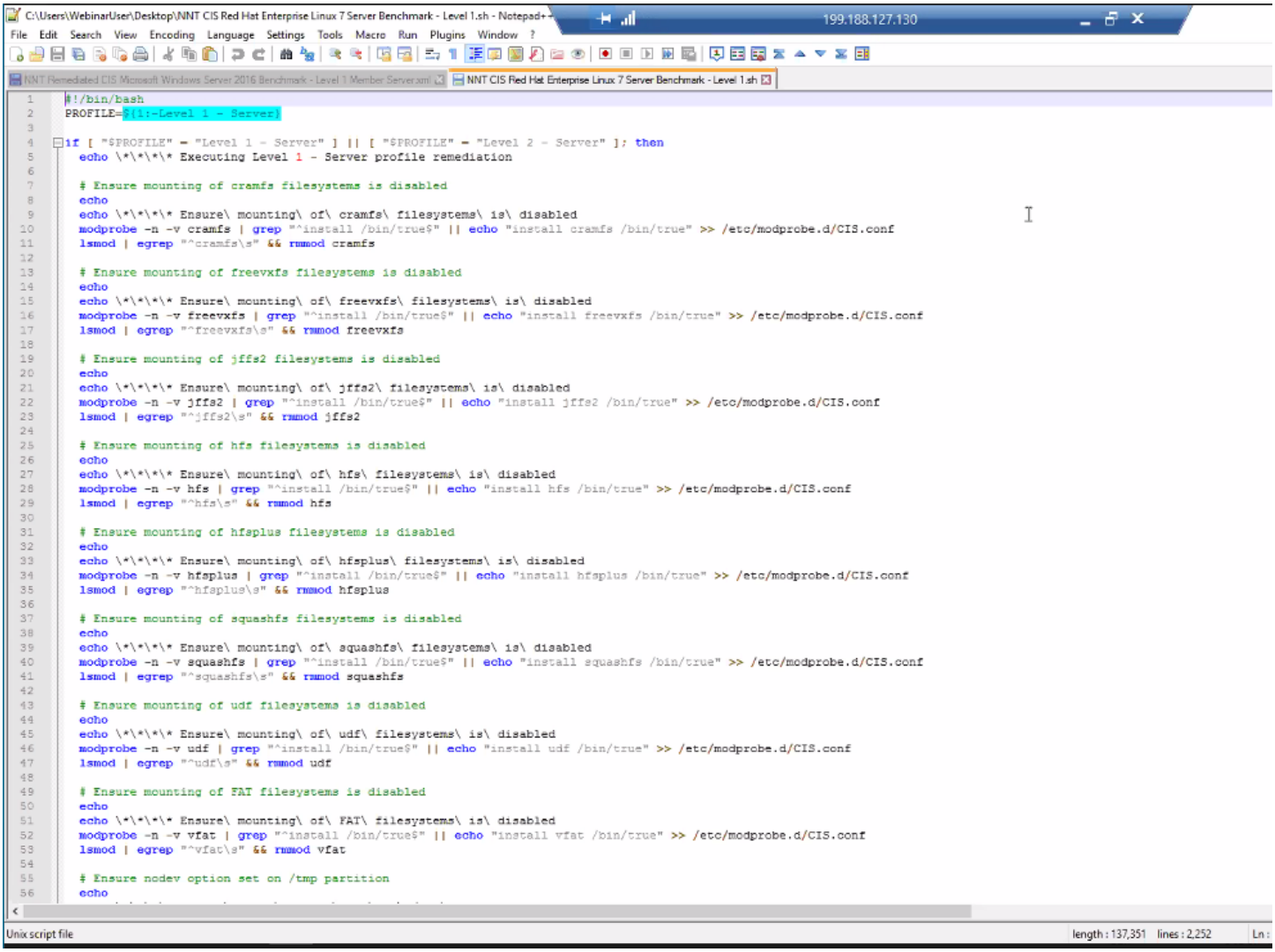
Fail - Setting Does Not Apply - Utilizing 3rd Party Tool

Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' : .". Remediation : To establish the recommended configuration via GP, set the following UI path to No:Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a

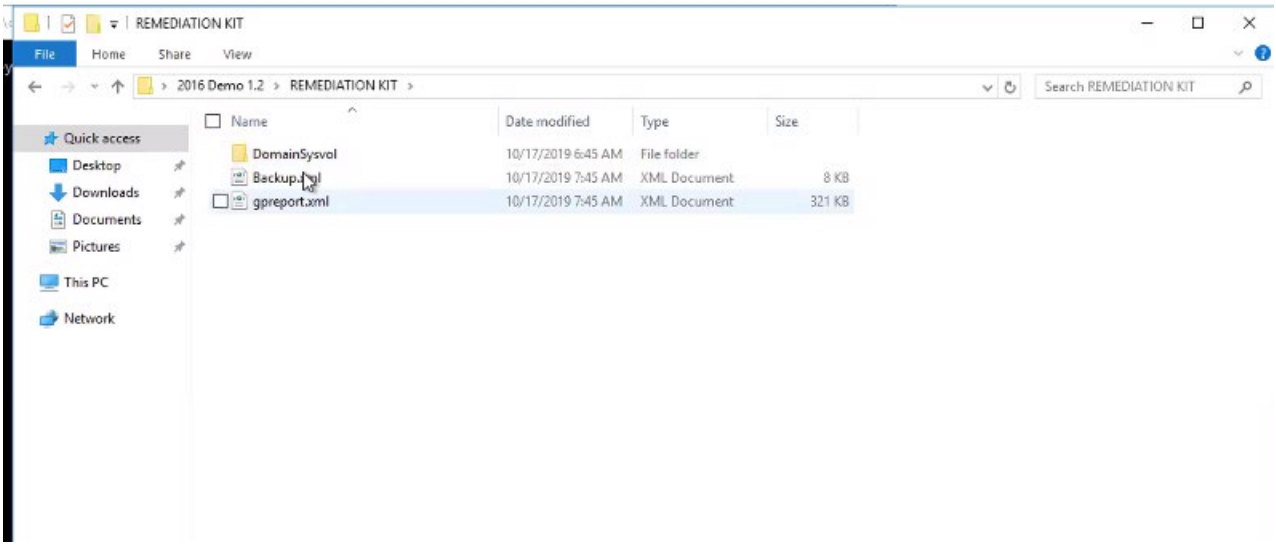
Page 1

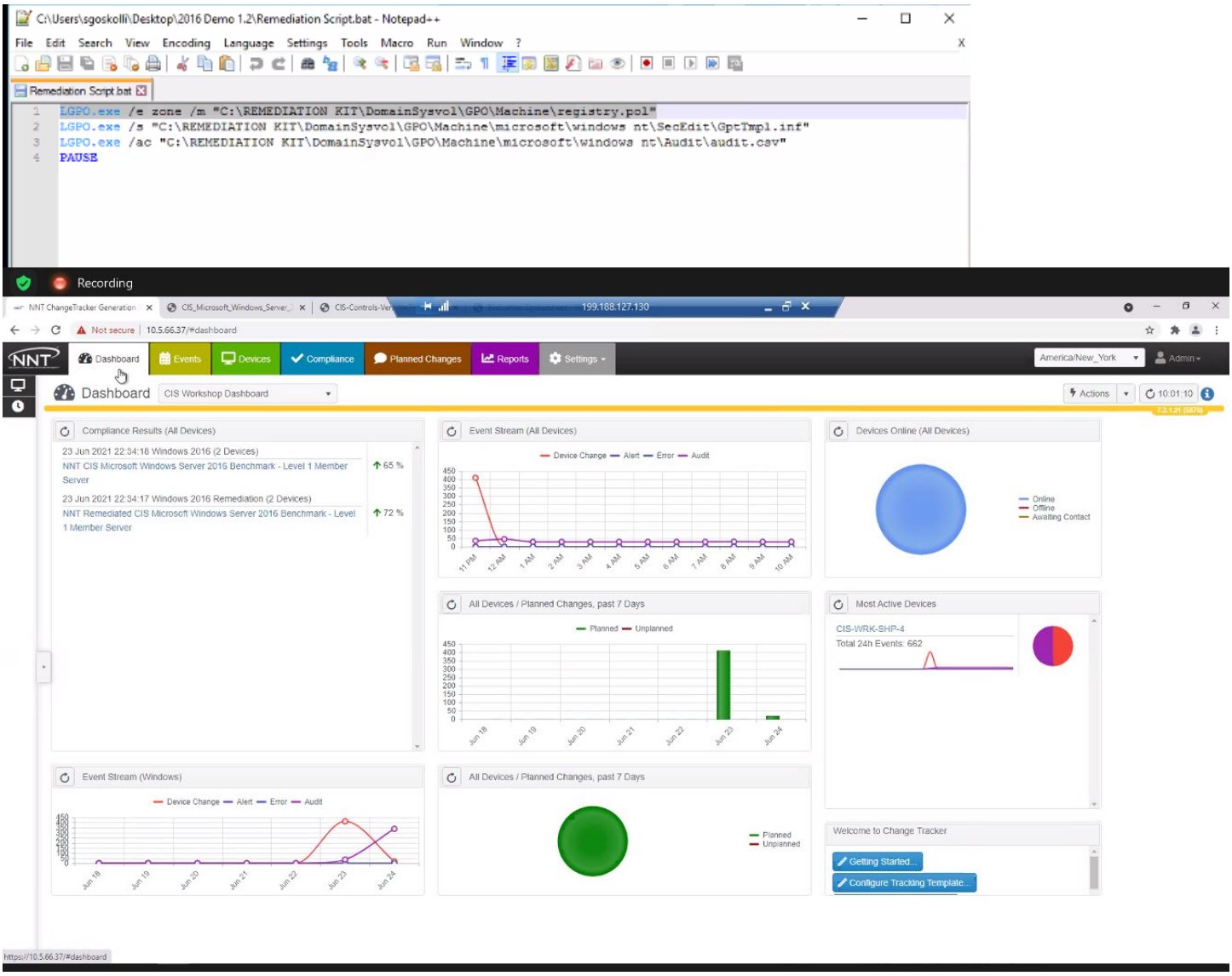
Remediation kit

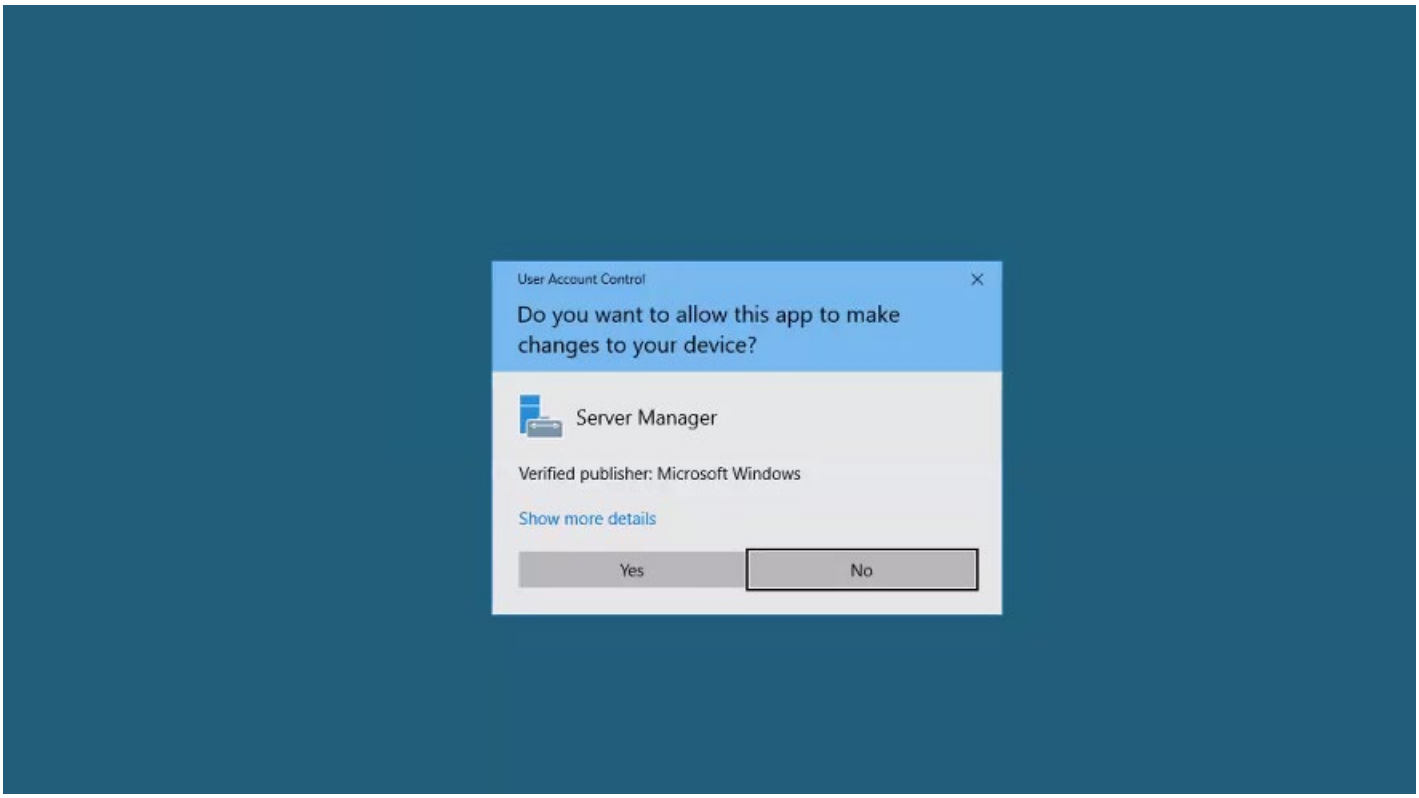



C:\Users\WebinarUser\Desktop\NNT CIS Red Hat Enterprise Linux 7 Server Benchmark - Level 1.sh - Notepad++
199.188.127.130
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server.xml
NNT CIS Red Hat Enterprise Linux 7 Server Benchmark - Level 1.sh
#!/bin/bash
PROFILE=${1:-Level 1 - Server}
if ["$PROFILE" = "Level 1 - Server"] || ["$PROFILE" = "Level 2 - Server"]; then
echo **** Executing Level 1 - Server profile remediation
Ensure mounting of cramfs filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ cramfs\ filesystems\ is\ disabled
modprobe -n -v cramfs | grep "^install /bin/true$" || echo "install cramfs /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^cramfs\s" && rmmod cramfs
Ensure mounting of freevxfs filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ freevxfs\ filesystems\ is\ disabled
modprobe -n -v freevxfs | grep "^install /bin/true$" || echo "install freevxfs /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^freevxfs\s" && rmmod freevxfs
Ensure mounting of jffs2 filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ jffs2\ filesystems\ is\ disabled
modprobe -n -v jffs2 | grep "^install /bin/true$" || echo "install jffs2 /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^jffs2\s" && rmmod jffs2
Ensure mounting of hfs filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ hfs\ filesystems\ is\ disabled
modprobe -n -v hfs | grep "^install /bin/true$" || echo "install hfs /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^hfs\s" && rmmod hfs
Ensure mounting of hfsplus filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ hfsplus\ filesystems\ is\ disabled
modprobe -n -v hfsplus | grep "^install /bin/true$" || echo "install hfsplus /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^hfsplus\s" && rmmod hfsplus
Ensure mounting of squashfs filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ squashfs\ filesystems\ is\ disabled
modprobe -n -v squashfs | grep "^install /bin/true$" || echo "install squashfs /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^squashfs\s" && rmmod squashfs
Ensure mounting of udf filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ udf\ filesystems\ is\ disabled
modprobe -n -v udf | grep "^install /bin/true$" || echo "install udf /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^udf\s" && rmmod udf
Ensure mounting of FAT filesystems is disabled
echo
echo **** Ensure\ mounting\ of\ FAT\ filesystems\ is\ disabled
modprobe -n -v vfat | grep "^install /bin/true$" || echo "install vfat /bin/true" >> /etc/modprobe.d/CIS.conf
lsmod | egrep "^vfat\s" && rmmod vfat
Ensure nodev option set on /tmp partition
echo
Unix script file
length : 137,351 lines : 2,252
Ln :

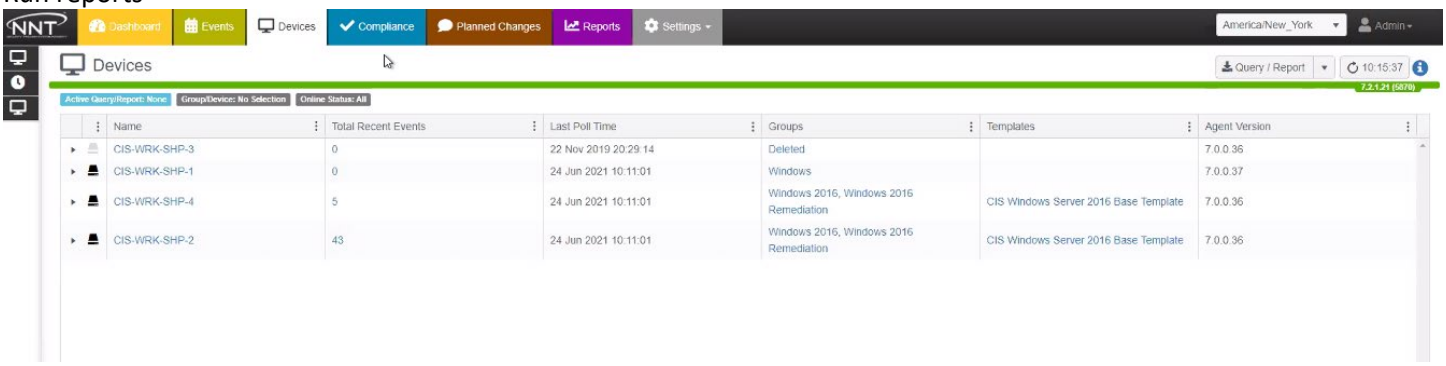
Workshop

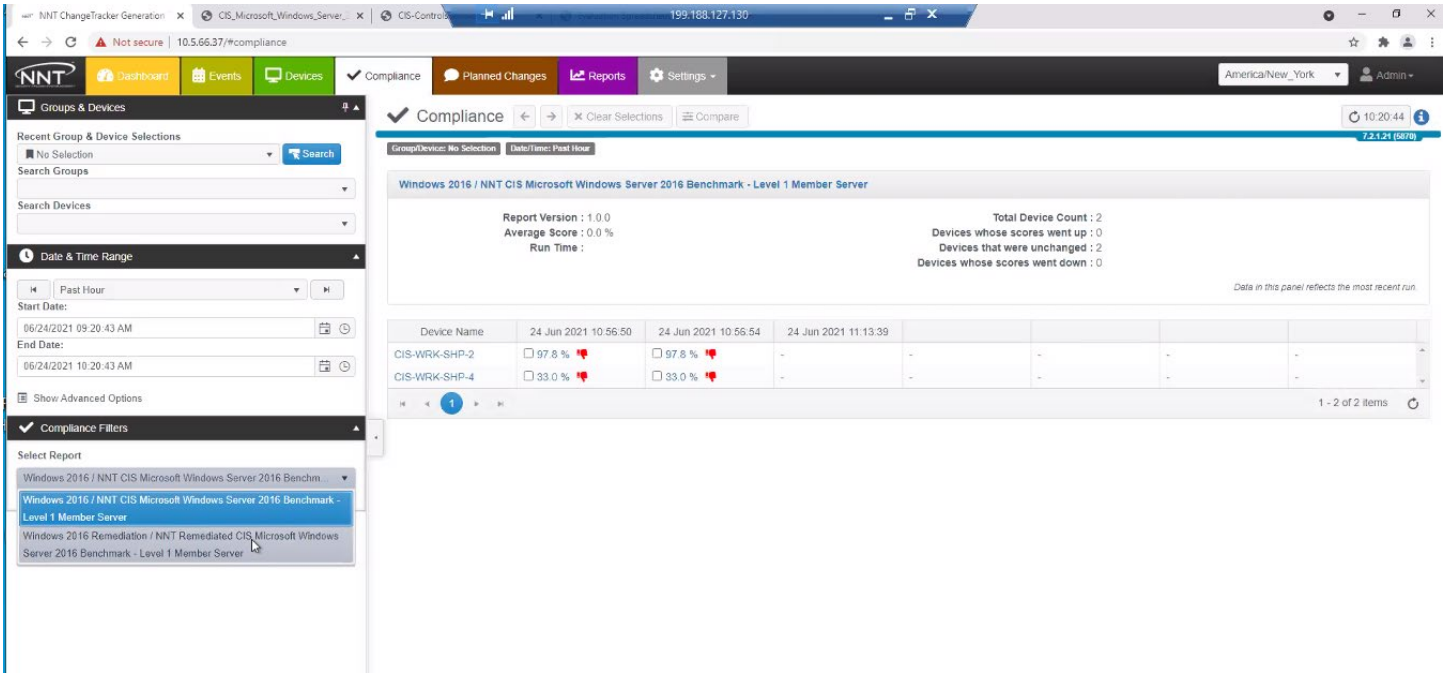

REMEDIATION KIT
File Home Share View
2016 Demo 1.2 › REMEDIATION KIT ›
Search REMEDIATION KIT
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
DomainSysvol
10/17/2019 6:45 AM
File folder
Backup.xml
10/17/2019 7:45 AM
XML Document
8 KB
gpreport.xml
10/17/2019 7:45 AM
XML Document
321 KB

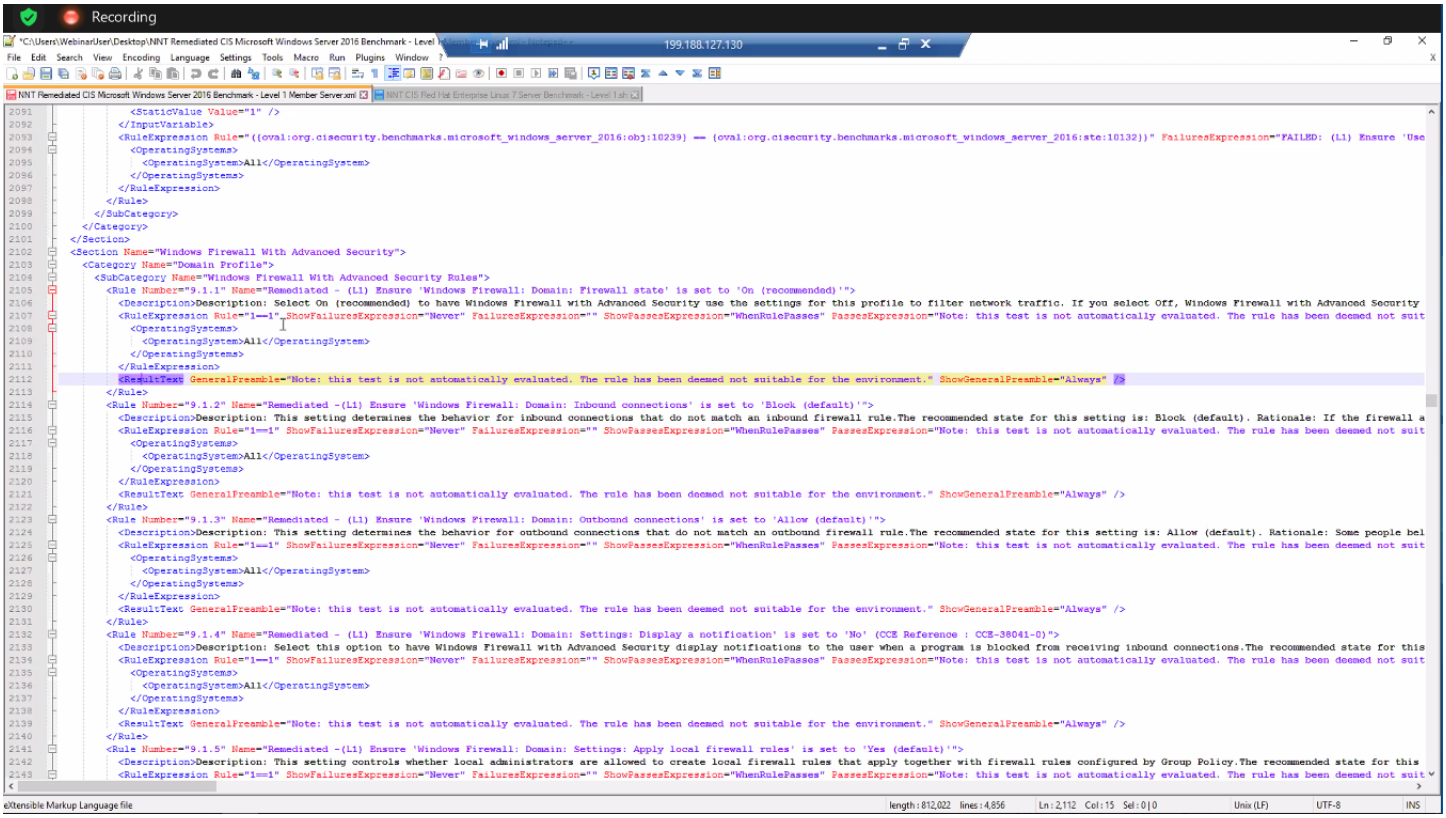

C:\Users\sgoskolli\Desktop\2016 Demo 1.2\Remediation Script.bat - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Window ?
Remediation Script.bat
1 LGPO.exe /e zone /m "C:\REMEDIATION KIT\DomainSysvol\GPO\Machine\registry.pol"
2 LGPO.exe /s "C:\REMEDIATION KIT\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf"
3 LGPO.exe /ac "C:\REMEDIATION KIT\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv"
4 PAUSE
Recording
199.188.127.130
Not secure | 10.5.66.37/#dashboard
Dashboard
Events
Devices
Compliance
Planned Changes
Reports
Settings
America/New_York
Admin
Dashboard
CIS Workshop Dashboard
Actions
10:01:10
Compliance Results (All Devices)
23 Jun 2021 22:34:18 Windows 2016 (2 Devices)
NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
65 %
23 Jun 2021 22:34:17 Windows 2016 Remediation (2 Devices)
NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
72 %
Event Stream (All Devices)
Device Change
Alert
Error
Audit
Devices Online (All Devices)
Online
Offline
Awaiting Contact
All Devices / Planned Changes, past 7 Days
Planned
Unplanned
Most Active Devices
CIS-WRK-SHP-4
Total 24h Events: 662
Event Stream (Windows)
All Devices / Planned Changes, past 7 Days
Welcome to Change Tracker
Getting Started...
Configure Tracking Template...
https://10.5.66.37/#dashboard

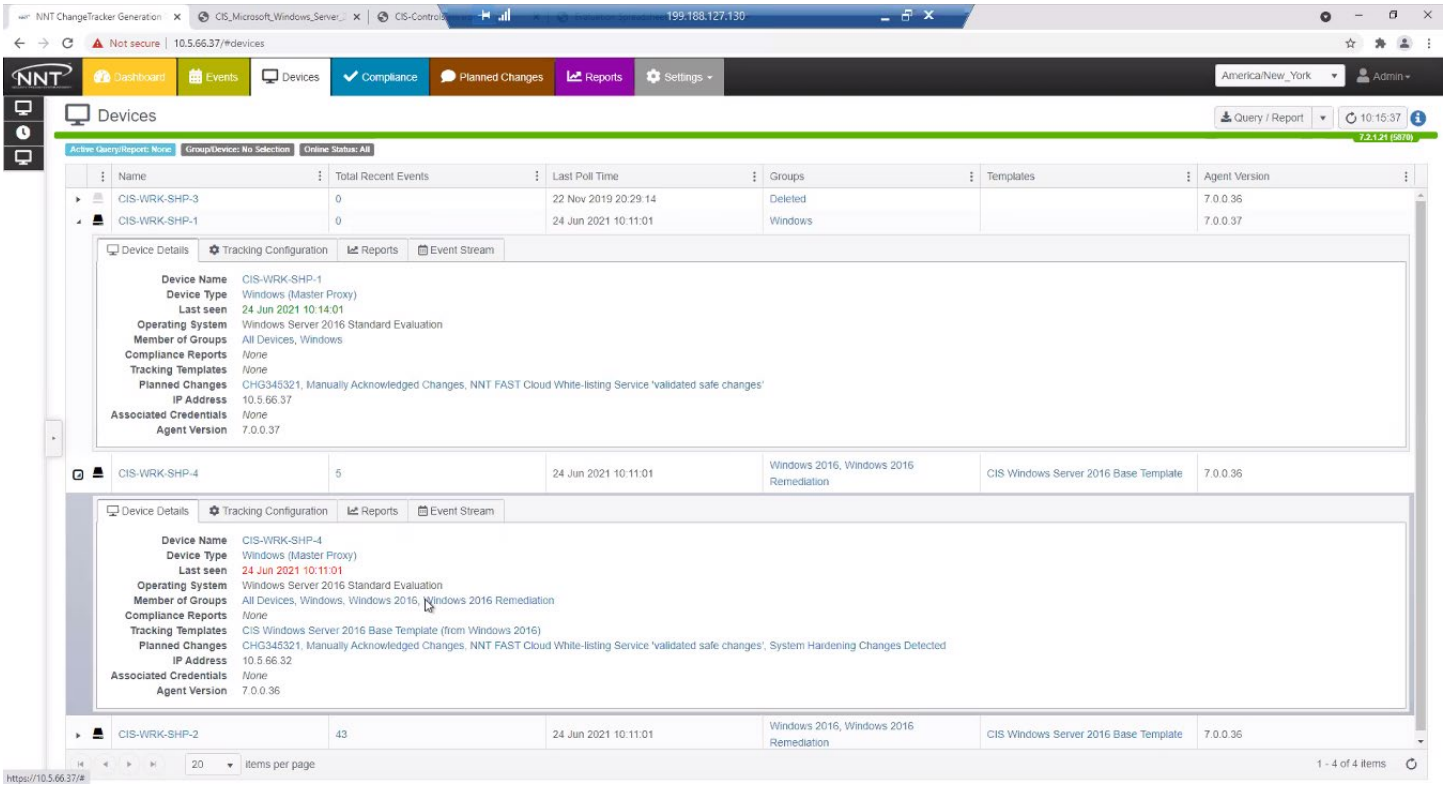

User Account Control
Do you want to allow this app to make changes to your device?
Server Manager
Verified publisher: Microsoft Windows
Show more details
Yes
No

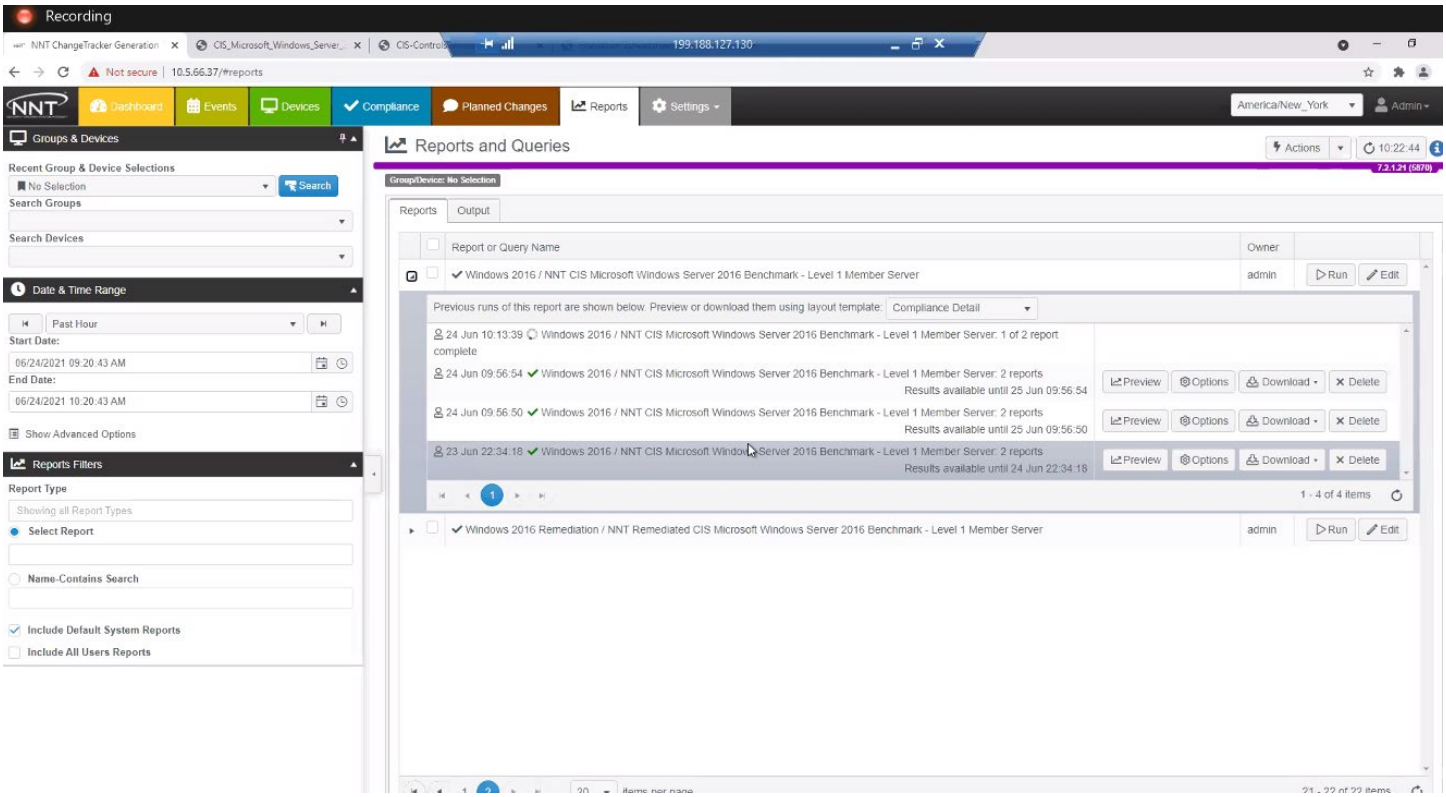
Run reports

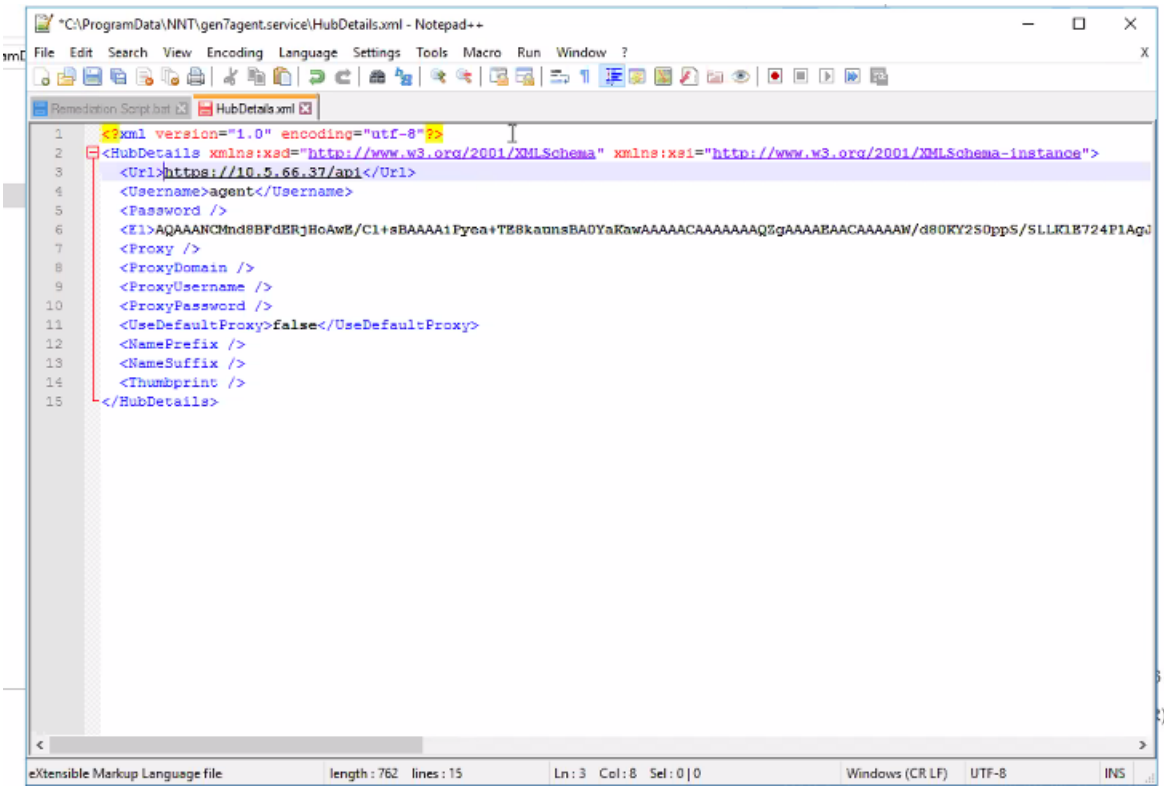

Dashboard
Events
Devices
Compliance
Planned Changes
Reports
Settings
America/New_York
Admin
Devices
Query / Report
Name
Total Recent Events
Last Poll Time
Groups
Templates
Agent Version
CIS-WRK-SHP-3
0
22 Nov 2019 20:29:14
Deleted
7.0.0.36
CIS-WRK-SHP-1
0
24 Jun 2021 10:11:01
Windows
7.0.0.37
CIS-WRK-SHP-4
5
24 Jun 2021 10:11:01
Windows 2016, Windows 2016 Remediation
CIS Windows Server 2016 Base Template
7.0.0.36
CIS-WRK-SHP-2
43
24 Jun 2021 10:11:01
Windows 2016, Windows 2016 Remediation
CIS Windows Server 2016 Base Template
7.0.0.36

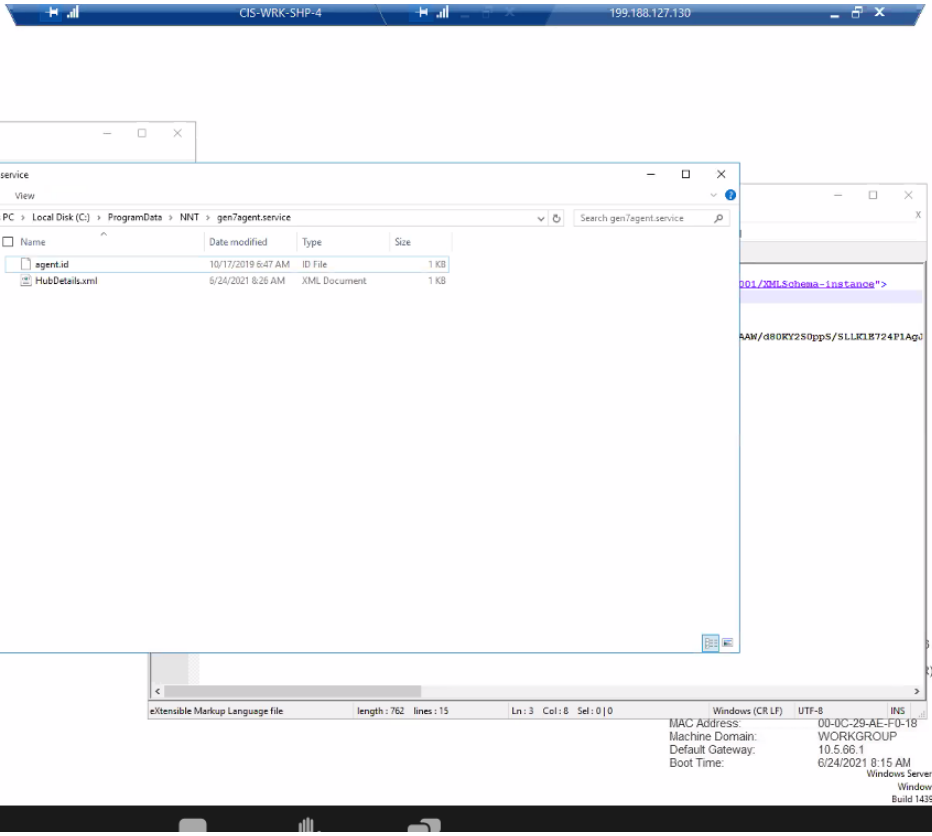

Not secure | 10.5.66.37/#compliance
Groups & Devices
Recent Group & Device Selections
No Selection
Search
Search Groups
Search Devices
Date & Time Range
Past Hour
Start Date:
06/24/2021 09:20:43 AM
End Date:
06/24/2021 10:20:43 AM
Show Advanced Options
Compliance Filters
Select Report
Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchm...
Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
Compliance
Clear Selections
Compare
Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
Report Version : 1.0.0
Average Score : 0.0 %
Run Time :
Total Device Count : 2
Devices whose scores went up : 0
Devices that were unchanged : 2
Devices whose scores went down : 0
Data in this panel reflects the most recent run
Device Name
24 Jun 2021 10:56:50
24 Jun 2021 10:56:54
24 Jun 2021 11:13:39
CIS-WRK-SHP-2
97.8 %
97.8 %
CIS-WRK-SHP-4
33.0 %
33.0 %
1 - 2 of 2 items

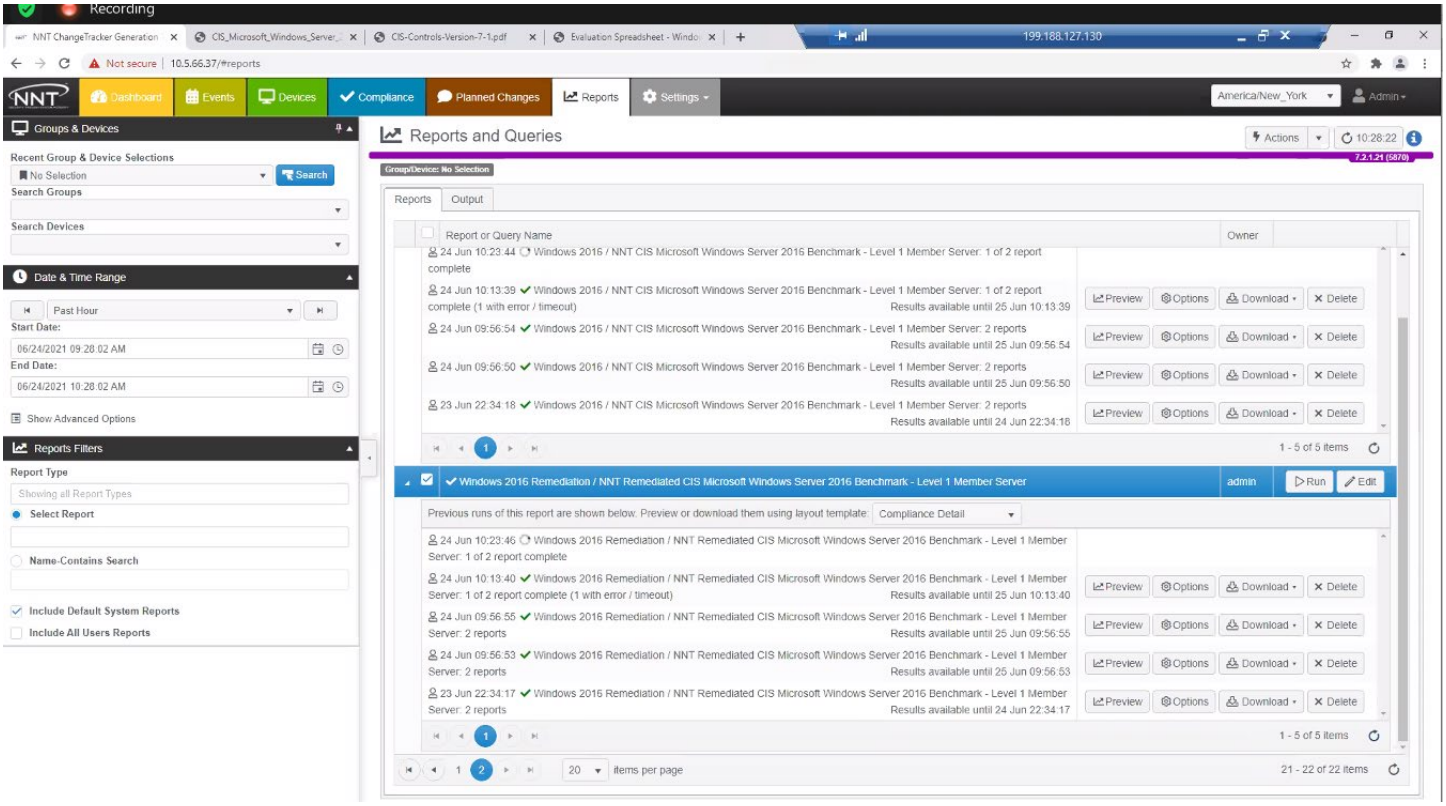

Recording
199.188.127.130
NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server.xml
NNT CIS Red Hat Enterprise Linux 7 Server Benchmark - Level 1.sh
<StaticValue Value="1" />
</InputVariable>
<RuleExpression Rule="((oval:org.cisecurity.benchmarks.microsoft_windows_server_2016:obj:10239) == (oval:org.cisecurity.benchmarks.microsoft_windows_server_2016:ste:10132))" FailuresExpression="FAILED: (L1) Ensure 'Use
<OperatingSystems>
<OperatingSystem>All</OperatingSystem>
</OperatingSystems>
</RuleExpression>
</Rule>
</SubCategory>
</Category>
</Section>
<Section Name="Windows Firewall With Advanced Security">
<Category Name="Domain Profile">
<SubCategory Name="Windows Firewall With Advanced Security Rules">
<Rule Number="9.1.1" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'">
<Description>Description: Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security
<RuleExpression Rule="1==1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
<OperatingSystems>
<OperatingSystem>All</OperatingSystem>
</OperatingSystems>
</RuleExpression>
<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
</Rule>
<Rule Number="9.1.2" Name="Remediated -(L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'">
<Description>Description: This setting determines the behavior for inbound connections that do not match an inbound firewall rule.The recommended state for this setting is: Block (default). Rationale: If the firewall a
<RuleExpression Rule="1==1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
<OperatingSystems>
<OperatingSystem>All</OperatingSystem>
</OperatingSystems>
</RuleExpression>
<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
</Rule>
<Rule Number="9.1.3" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'">
<Description>Description: This setting determines the behavior for outbound connections that do not match an outbound firewall rule.The recommended state for this setting is: Allow (default). Rationale: Some people bel
<RuleExpression Rule="1==1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
<OperatingSystems>
<OperatingSystem>All</OperatingSystem>
</OperatingSystems>
</RuleExpression>
<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
</Rule>
<Rule Number="9.1.4" Name="Remediated - (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-38041-0)">
<Description>Description: Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.The recommended state for this
<RuleExpression Rule="1==1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
<OperatingSystems>
<OperatingSystem>All</OperatingSystem>
</OperatingSystems>
</RuleExpression>
<ResultText GeneralPreamble="Note: this test is not automatically evaluated. The rule has been deemed not suitable for the environment." ShowGeneralPreamble="Always" />
</Rule>
<Rule Number="9.1.5" Name="Remediated -(L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'">
<Description>Description: This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy.The recommended state for this
<RuleExpression Rule="1==1" ShowFailuresExpression="Never" FailuresExpression="" ShowPassesExpression="WhenRulePasses" PassesExpression="Note: this test is not automatically evaluated. The rule has been deemed not suit
eXtensible Markup Language file
length : 812,022 lines : 4,856
Ln : 2,112 Col : 15 Sel : 0 | 0
Unix (LF)
UTF-8
INS


NNT ChangeTracker Generation
199.188.127.130
Not secure | 10.5.66.37/#devices
Dashboard
Events
Devices
Compliance
Planned Changes
Reports
Settings
America/New_York
Admin
Devices
Query / Report
10:15:37
7.2.1.21 (5870)
Active Query/Report: None
Group/Device: No Selection
Online Status: All
Name
Total Recent Events
Last Poll Time
Groups
Templates
Agent Version
CIS-WRK-SHP-3
0
22 Nov 2019 20:29:14
Deleted
7.0.0.36
CIS-WRK-SHP-1
0
24 Jun 2021 10:11:01
Windows
7.0.0.37
Device Details
Tracking Configuration
Reports
Event Stream
Device Name CIS-WRK-SHP-1
Device Type Windows (Master Proxy)
Last seen 24 Jun 2021 10:14:01
Operating System Windows Server 2016 Standard Evaluation
Member of Groups All Devices, Windows
Compliance Reports None
Tracking Templates None
Planned Changes CHG345321, Manually Acknowledged Changes, NNT FAST Cloud White-listing Service 'validated safe changes'
IP Address 10.5.66.37
Associated Credentials None
Agent Version 7.0.0.37
CIS-WRK-SHP-4
5
24 Jun 2021 10:11:01
Windows 2016, Windows 2016 Remediation
CIS Windows Server 2016 Base Template
7.0.0.36
Device Details
Tracking Configuration
Reports
Event Stream
Device Name CIS-WRK-SHP-4
Device Type Windows (Master Proxy)
Last seen 24 Jun 2021 10:11:01
Operating System Windows Server 2016 Standard Evaluation
Member of Groups All Devices, Windows, Windows 2016, Windows 2016 Remediation
Compliance Reports None
Tracking Templates CIS Windows Server 2016 Base Template (from Windows 2016)
Planned Changes CHG345321, Manually Acknowledged Changes, NNT FAST Cloud White-listing Service 'validated safe changes', System Hardening Changes Detected
IP Address 10.5.66.32
Associated Credentials None
Agent Version 7.0.0.36
CIS-WRK-SHP-2
43
24 Jun 2021 10:11:01
Windows 2016, Windows 2016 Remediation
CIS Windows Server 2016 Base Template
7.0.0.36
20
items per page
1 - 4 of 4 items
https://10.5.66.37/#


Recording
NNT ChangeTracker Generation
199.188.127.130
Not secure | 10.5.66.37/#reports
Dashboard
Events
Devices
Compliance
Planned Changes
Reports
Settings
America/New_York
Admin
Groups & Devices
Recent Group & Device Selections
No Selection
Search
Search Groups
Search Devices
Date & Time Range
Past Hour
Start Date:
06/24/2021 09:20:43 AM
End Date:
06/24/2021 10:20:43 AM
Show Advanced Options
Reports Filters
Report Type
Showing all Report Types
Select Report
Name-Contains Search
Include Default System Reports
Include All Users Reports
Reports and Queries
Actions
10:22:44
7.2.1.21 (5870)
Group/Device: No Selection
Reports
Output
Report or Query Name
Owner
Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
admin
Run
Edit
Previous runs of this report are shown below. Preview or download them using layout template: Compliance Detail
24 Jun 10:13:39 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete
24 Jun 09:56:54 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 25 Jun 09:56:54
Preview
Options
Download
Delete
24 Jun 09:56:50 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 25 Jun 09:56:50
23 Jun 22:34:18 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 24 Jun 22:34:18
1 - 4 of 4 items
Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
admin
Run
Edit


*C:\ProgramData\NNT\gen7agent.service\HubDetails.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Window ?
Remediation Script.bat
HubDetails.xml
<?xml version="1.0" encoding="utf-8"?>
<HubDetails xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Url>https://10.5.66.37/api</Url>
<Username>agent</Username>
<Password />
<El>AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAA1Pyea+TE8kaunsBA0YaKawAAAAACAAAAAAAQZgAAAAEAACAAAAAW/d80KY2S0ppS/SLLKlE724P1AgJ
<Proxy />
<ProxyDomain />
<ProxyUsername />
<ProxyPassword />
<UseDefaultProxy>false</UseDefaultProxy>
<NamePrefix />
<NameSuffix />
<Thumbprint />
</HubDetails>
eXtensible Markup Language file
length : 762 lines : 15
Ln : 3 Col : 8 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS


CIS-WRK-SHP-4
199.188.127.130
Task Manager
File Options View
Processes Performance Users Details
gen7agent.service
File Home Share View
This PC > Local Disk (C:) > ProgramData > NNT > gen7agent.service
Search gen7agent.service
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
agent.id 10/17/2019 6:47 AM ID File 1 KB
HubDetails.xml 6/24/2021 8:26 AM XML Document 1 KB
2 items
MAC Address: 00-0C-29-AE-F0-18
Machine Domain: WORKGROUP
Default Gateway: 10.5.66.1
Boot Time: 6/24/2021 8:15 AM
Windows Server 2016 Standard Evaluation
Windows License valid for 32 days
Build 14393.rs1_release.161220-1747


Recording
NNT ChangeTracker Generation
CIS_Microsoft_Windows_Server_...
CIS-Controls-Version-7-1.pdf
Evaluation Spreadsheet - Windo
199.188.127.130
Not secure | 10.5.66.37/#reports
NNT
Dashboard
Events
Devices
Compliance
Planned Changes
Reports
Settings
America/New_York
Admin
Groups & Devices
Recent Group & Device Selections
No Selection
Search
Search Groups
Search Devices
Date & Time Range
Past Hour
Start Date:
06/24/2021 09:28:02 AM
End Date:
06/24/2021 10:28:02 AM
Show Advanced Options
Reports Filters
Report Type
Showing all Report Types
Select Report
Name-Contains Search
Include Default System Reports
Include All Users Reports
Reports and Queries
Actions
10:28:22
7.2.1.21 (5870)
Group/Device: No Selection
Reports
Output
Report or Query Name
Owner
24 Jun 10:23:44 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete
24 Jun 10:13:39 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete (1 with error / timeout)
Results available until 25 Jun 10:13:39
24 Jun 09:56:54 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 25 Jun 09:56:54
24 Jun 09:56:50 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 25 Jun 09:56:50
23 Jun 22:34:18 Windows 2016 / NNT CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 24 Jun 22:34:18
Preview
Options
Download
Delete
1 - 5 of 5 items
Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server
admin
Run
Edit
Previous runs of this report are shown below. Preview or download them using layout template:
Compliance Detail
24 Jun 10:23:46 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete
24 Jun 10:13:40 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 1 of 2 report complete (1 with error / timeout)
Results available until 25 Jun 10:13:40
24 Jun 09:56:55 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 25 Jun 09:56:55
24 Jun 09:56:53 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 25 Jun 09:56:53
23 Jun 22:34:17 Windows 2016 Remediation / NNT Remediated CIS Microsoft Windows Server 2016 Benchmark - Level 1 Member Server: 2 reports
Results available until 24 Jun 22:34:17
1 - 5 of 5 items
20
items per page
21 - 22 of 22 items