FORTRA™

REPORT CATALOG (TRIPWIRE)

Tripwire Enterprise:

System, Compliance Policy, and File Integrity Monitoring Reports

Controlling change and enforcing internal or external policies requires not only trusted change and compliance data, but the ability to quickly transform that data into relevant, meaningful information. Fortra's Tripwire® Enterprise is known for its unparalleled ability to assess and validate configuration settings and manage configuration changes, but it's also the most dependable source available for the business-critical change and compliance information modern IT organizations depend on.

Tripwire Enterprise's comprehensive portfolio of customizable ready-to-use reports and dashboards cover all your information needs. There's even easy report-linking, which allows users to "drill down" to view the most granular detail about system changes and compliance. By being able to generate timely and critical information about enterprise infrastructures, these reports are leveraged daily by auditors, IT management, and operations teams. Tripwire Enterprise provides nearly 40 reports, with additional in development.

This Report Catalog provides detailed information and screenshots of each report and dashboard. As new reports are continuously being developed, please refer to the Tripwire website for information on newly-added reports.

Change Auditing:

Report Drilldowns and Linking

Tripwire Enterprise reports have a built-in linking function, providing drilldown capability so users can dig into change information and discover the details of a change, when and where it was made, and even the ID of the user who made it.

In this example, a change manager used Tripwire Enterprise reports to review the ratio of approved to unapproved changes and validate the overall efficacy of the change process. He started at his dashboard (1) and quickly generated a Change Process Compliance report (2), which showed all changes made to the selected machines in the given time period, as well as the proportion of approved to unapproved changes.

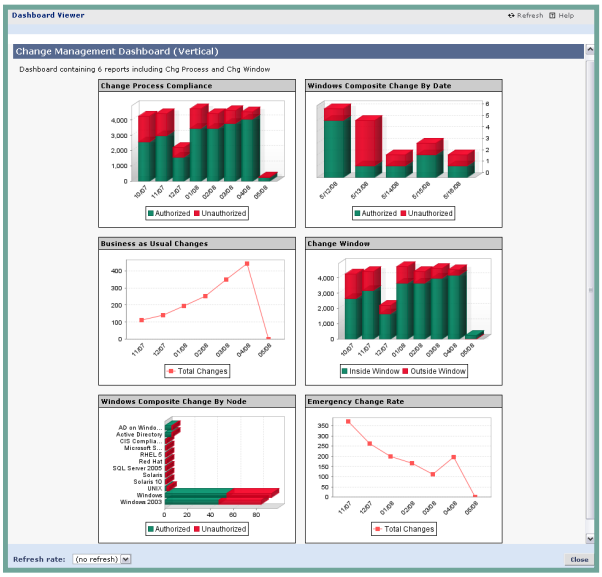


Fig. 1 Change Management dashboard

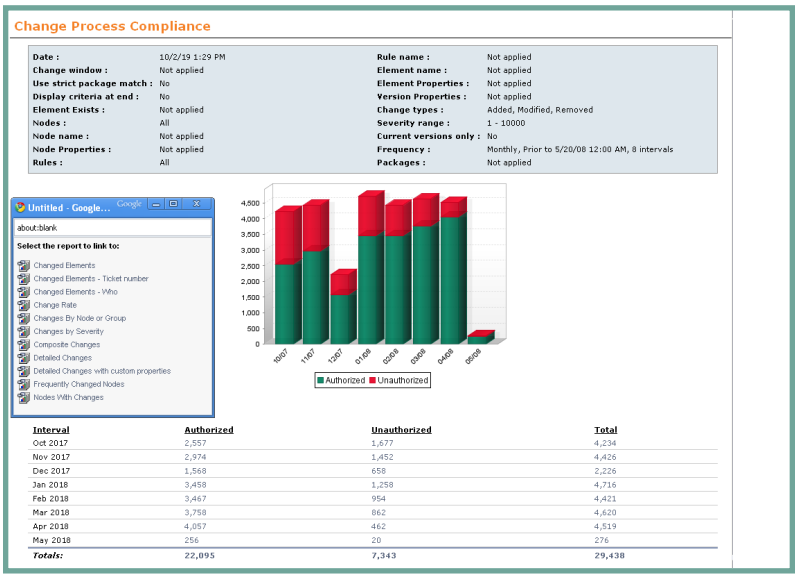
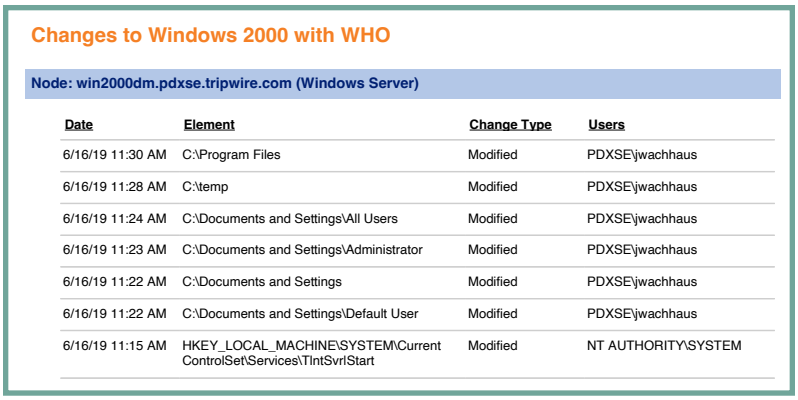


Fig. 2 Change Process Compliance report

Drilldowns and Linking

Next, by selecting a specific node and a linking option, the user invoked a “Changed Elements – Who” report, and obtained specific information on the ID of the user making the detected changes. In this case, it looks like the changes were made by a junior admin. But what was their extent? What’s the potential risk?

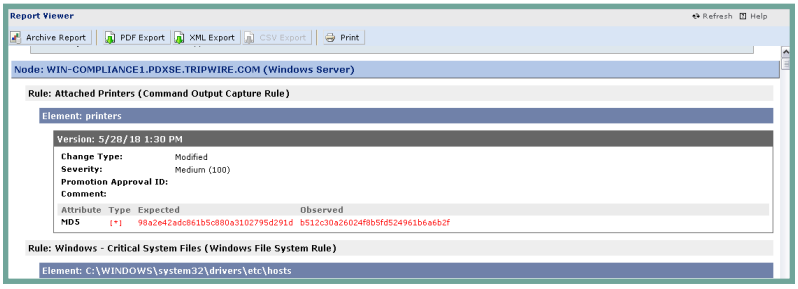


Changes to Windows 2000 with WHO

Node: win2000dm.pdxse.tripwire.com (Windows Server)

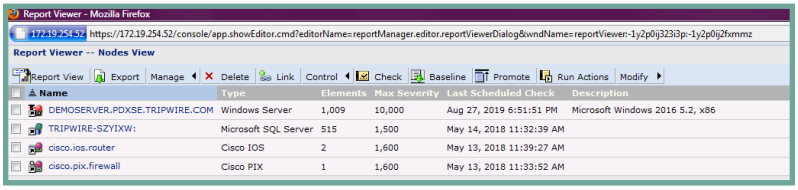
Date	Element	Change Type	Users
6/16/19 11:30 AM	C:\Program Files	Modified	PDXSE\jwachhaus
6/16/19 11:28 AM	C:\temp	Modified	PDXSE\jwachhaus
6/16/19 11:24 AM	C:\Documents and Settings\All Users	Modified	PDXSE\jwachhaus
6/16/19 11:23 AM	C:\Documents and Settings\Administrator	Modified	PDXSE\jwachhaus
6/16/19 11:22 AM	C:\Documents and Settings	Modified	PDXSE\jwachhaus
6/16/19 11:22 AM	C:\Documents and Settings\Default User	Modified	PDXSE\jwachhaus
6/16/19 11:15 AM	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TIntSvrlStart	Modified	NT AUTHORITY\SYSTEM

At this point the change manager decided to follow the trail and review all changes made by this user in detail by running a “Detailed Changes” report to drill down into the node, revealing every changed element, as well as the affected rule.



Lastly, the change manager decided to reconcile and remediate the changes directly from the Tripwire Enterprise console. To facilitate this, some reports have “action” toggles that allow the user to switch directly from the report to console operator’s view of the same infrastructure.

When the action toggle is engaged the view switches to a node view of the impacted servers and devices, where the user can reconcile, promote, or run other actions against the detected changes.



Compliance Policy Management:

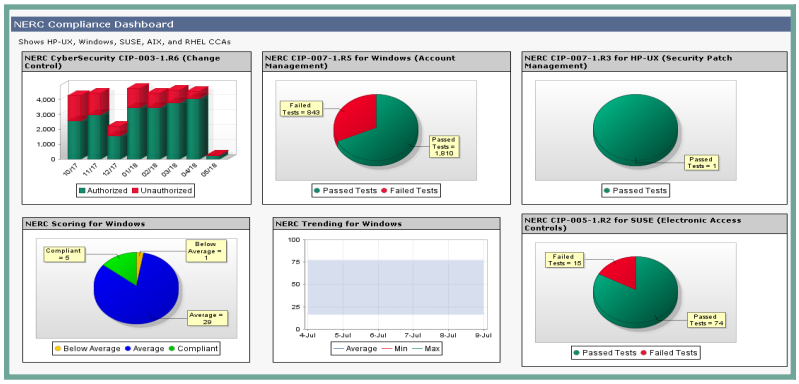
Report Drilldowns and Linking

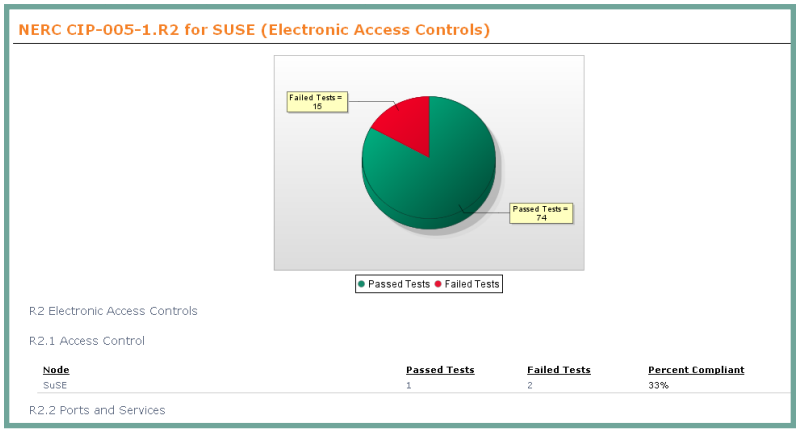
Users who rely on Tripwire Enterprise to assess the state of their systems against standards and policies can also benefit from the linked, drillable report structure.

In this example, an energy company compliance officer starts from a standard dashboard to obtain an understanding of how compliant his systems are against NERC (North American Energy Reliability Corporation) cybersecurity standards for his organization's different platforms.

He notes that his SUSE Linux nodes have experienced 15 failed tests, and clicks on that image to generate a "Test Results Summary" report. This report sums up the overall passing/failing scores for his SUSE Linux servers and shows and an overall policy score as a percentage.

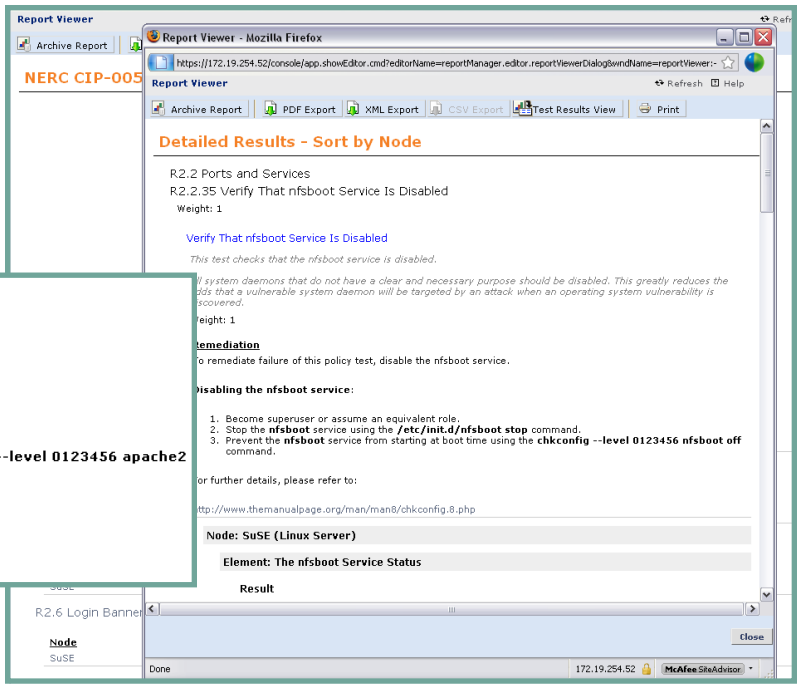
But what about specific details on the tests that failed? And how can the compliance officer provide his operations team with a "punch list" of instructions for how to get these systems back into alignment?





Remediation Instructions

By next clicking on the machine identifier under the “node” column, the compliance officer can generate a “Detailed Test Results” report. This report spells out the governing requirement for the control if applicable as well as the current condition of the element being tested.



Weight: 1

Remediation

To remediate failure of this policy test, disable the apache2 service.

Disabling the apache2 service:

1. Become superuser or assume an equivalent role.
2. Stop the **apache2** service using the **/etc/init.d/apache2 stop** command.
3. Prevent the **apache2** service from starting at boot time using the **chkconfig --level 0123456 apache2 off** command.

For further details, please refer to:

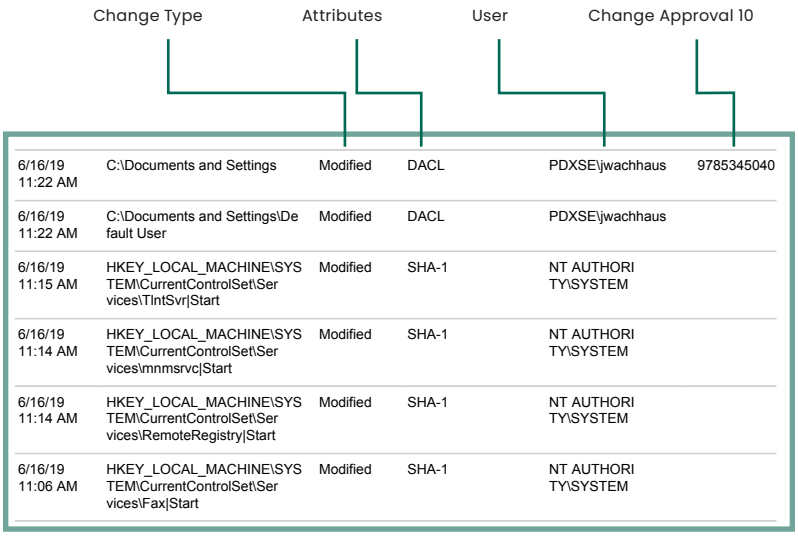
http://www.cisecurity.org/tools2/linux/CIS_SUSE_Linux_Benchmark_v2.0.pdf

Embedded in this report is a set of complete remediation steps. To begin getting these systems back into alignment with the NERC standards, the compliance manager can forward these instructions to the operational owner of the server or device, dramatically simplifying and acce the entire remediation process.

Report Customization

The criteria defining each Tripwire Enterprise report are entirely customizable, allowing users to specify exactly what information is revealed in each report. The depth of detail can be increased or decreased, as well as the overall scope and coverage of each report, from the included nodes and devices to the specific tests and rules. Of course all customized reports can be saved and rerun whenever needed.

Reports are available in HTML, XML and PDF formats, and can be scheduled to be generated and automatically emailed to appropriate personnel.



The display of these and other columns is user configurable

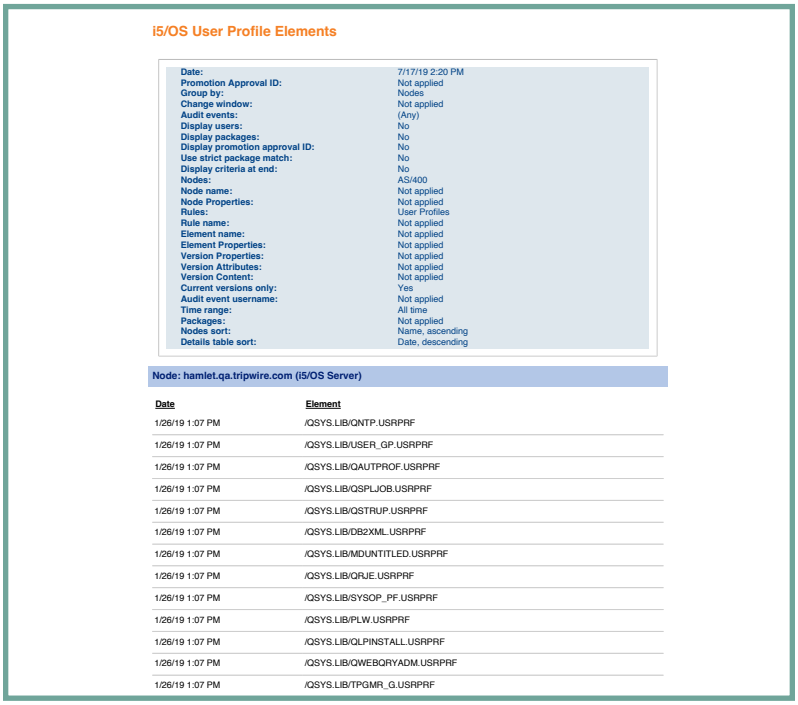
Tripwire Enterprise Reports

	Report Name	Displays Users	Dynamic, with Control Option	Displays Approval ID	Contains Links	Can be Linked	Can be Dashboarded	Examples
File Integrity Monitoring Reports	Baseline Elements	✔		✔				p 7
	Change Process Compliance				✔	✔	✔	p 7
	Change Rate				✔	✔	✔	p 8
	Change Window				✔	✔	✔	p 8
	Change Variance							p 9
	Changed Elements	✔	✔	✔	✔	✔		p 9
	Changes by Node or Node Group				✔	✔	✔	p 10
	Changes by Severity							p 10
	Changes by Rule or Rule Group							p 11
	Composite Changes by Node				✔	✔	✔	p 11
	Detailed Changes	✔				✔		p 12
	Elements		✔					p 12
	Frequently Changed Elements				✔			p 12
	Frequently Changed Nodes				✔	✔	✔	p 13
	Missing Elements							p 13
	Change Audit Coverage							p 14
	Nodes with Changes		✔		✔	✔	✔	p 14
	Reference Node Variance							p 15
	Unchanged Elements							p 15
	Unmonitored Nodes							p 15
	Unreconciled Change Aging				✔	✔	✔	p 16
Compliance Policy Reports	Compliance History				✔	✔	✔	p 17
	Detailed Test Inventory							p 17
	Detailed Test Results					✔		p 18
	Detailed Waivers							p 18
	Test Results by Node					✔		p 18
	Remediation Assessment							p 19
	Remediation Work Order Details							p 20
	Scoring						✔	p 21
	Scoring History						✔	p 22
	Test Results Summary				✔	✔	✔	p 23
System Reports	Device Inventory							p 24
	Last Node Check Status							p 24
	Element Contents				✔	✔		p 24
	Inventory Changes				✔		✔	p 25
	System Access Control							p 25
	System Log					✔		p 26
	Tasks					✔	✔	p 26
	User Roles							p 27
	User Roles All Object Types							p 27
	Sample Dashboards							p 28

File Integrity Monitoring Reports

Baseline Elements

The Baseline Elements report lists details about baseline elements for specified nodes. By reporting all changes promoted to the current baseline, including who made the change, approval IDs, and comments that indicate why the change was approved, this report satisfies the audit requirement of showing that changes are authorized.



i5/OS User Profile Elements

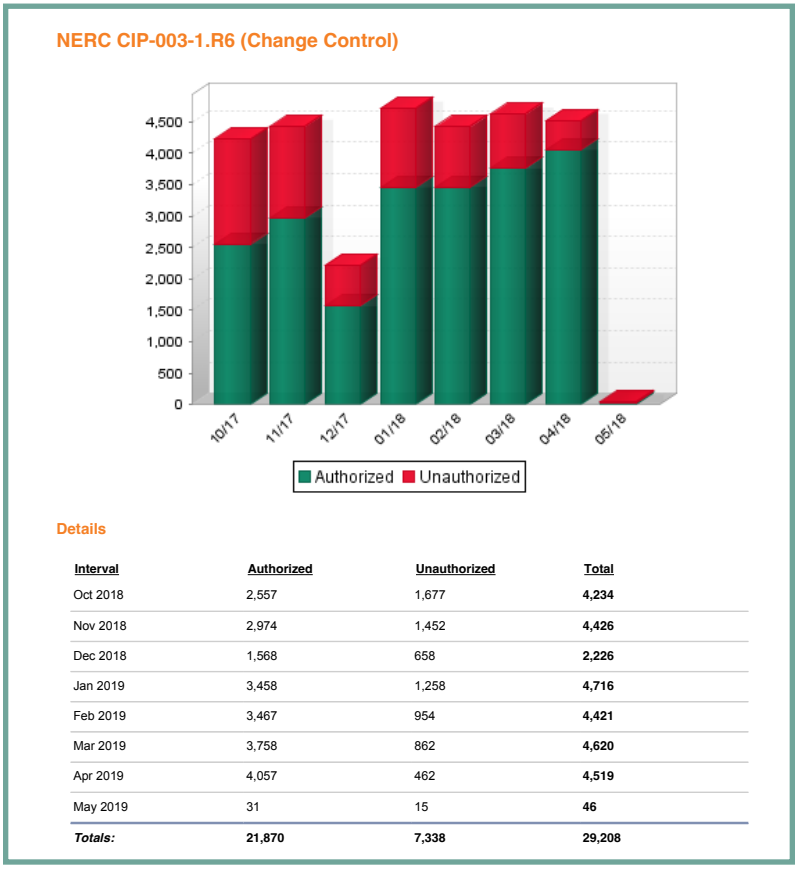
Date:	7/17/19 2:20 PM
Promotion Approval ID:	Not applied
Group by:	Nodes
Change window:	Not applied
Audit events:	(Any)
Display users:	No
Display packages:	No
Display promotion approval ID:	No
Use strict package match:	No
Display criteria at end:	No
Nodes:	AS/400
Node name:	Not applied
Node Properties:	Not applied
Rules:	User Profiles
Rule name:	Not applied
Element name:	Not applied
Element Properties:	Not applied
Version Properties:	Not applied
Version Attributes:	Not applied
Version Content:	Not applied
Current versions only:	Yes
Audit event username:	Not applied
Time range:	All time
Packages:	Not applied
Nodes sort:	Name, ascending
Details table sort:	Date, descending

Node: hamlet.qa.tripwire.com (i5/OS Server)

Date	Element
1/26/19 1:07 PM	/QSYS.LIB/QNTP.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/USER_GP.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/QAUTPROF.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/QSPLJOB.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/QSTRUP.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/DB2XML.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/MDUNTITLED.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/QRJE.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/SYSOP_PF.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/PLW.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/QLPINSTALL.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/QWEBQRYADM.USRPRF
1/26/19 1:07 PM	/QSYS.LIB/TPGMR_G.USRPRF

Change Process Compliance

This report identifies authorized and unauthorized changes to specified nodes over a period of time. An authorized change is associated with a valid change request ticket ID. This management report displays trends in the effectiveness of—and adherence to—change process controls, and is usually run at least weekly.



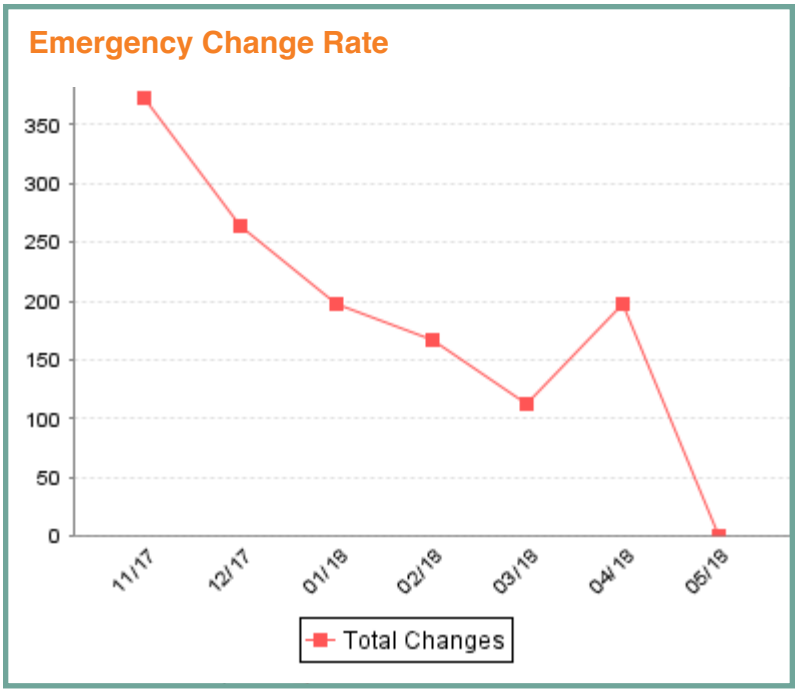
NERC CIP-003-1.R6 (Change Control)

Details

Interval	Authorized	Unauthorized	Total
Oct 2018	2,557	1,677	**4,234**
Nov 2018	2,974	1,452	**4,426**
Dec 2018	1,568	658	**2,226**
Jan 2019	3,458	1,258	**4,716**
Feb 2019	3,467	954	**4,421**
Mar 2019	3,758	862	**4,620**
Apr 2019	4,057	462	**4,519**
May 2019	31	15	**46**
Totals:	**21,870**	**7,338**	**29,208**

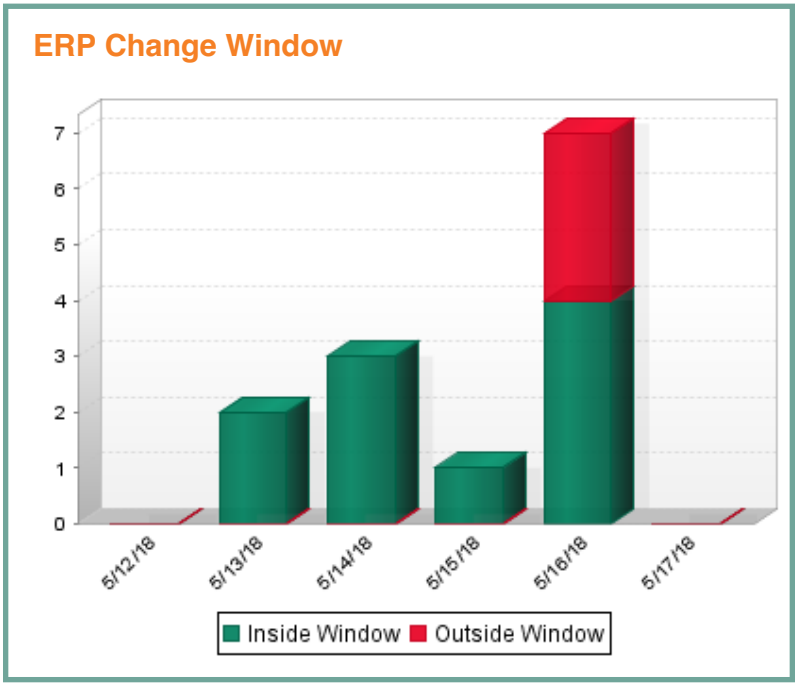
Change Rate

This report shows the total number of changes (additions, removals, and modifications) detected on specified nodes over a period of time. Within the selected time period, the report displays the number of changes at a regular interval (or "frequency"); for instance, daily, weekly, or monthly. This high-level report is used to reveal abnormalities in the change process, and is run monthly or more often, depending on process maturity.



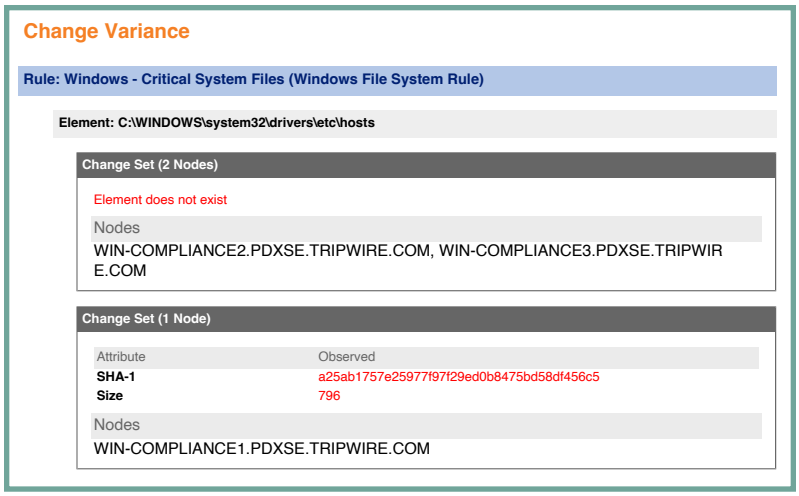
Change Window

This report indicates the number of detected changes for a specified monitored system(s) that have occurred inside and outside a defined change window. Changes outside the change window can potentially affect service quality through downtime or restricted system access. Numerous changes outside change windows are an indicator of process circumvention, a frequent cause of poor system quality. This report is normally run before and after each change window.



Change Variance

This report shows the elements that differ between specified monitored systems. As appropriate, you can limit report output to specific nodes, rules, and/or elements. This report is frequently used to compare changes on nodes after a patch/install has been implemented, so that changes that are inconsistent across the nodes can be flagged and reported. It is typically run ad hoc, though potentially weekly or monthly.



Change Variance

Rule: Windows - Critical System Files (Windows File System Rule)

Element: C:\WINDOWS\system32\drivers\etc\hosts

Change Set (2 Nodes)

Element does not exist

Nodes

WIN-COMPLIANCE2.PDXSE.TRIPWIRE.COM, WIN-COMPLIANCE3.PDXSE.TRIPWIRE.COM

Change Set (1 Node)

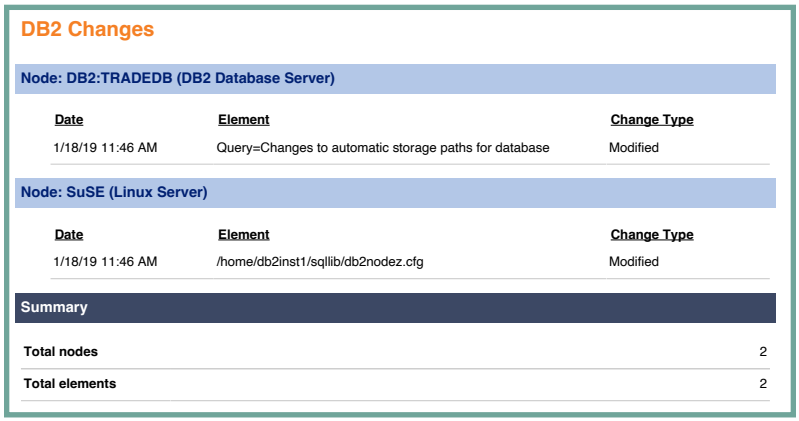
Attribute	Observed
SHA-1	a25ab1757e25977f97f29ed0b8475bd58df456c5
Size	796

Nodes

WIN-COMPLIANCE1.PDXSE.TRIPWIRE.COM

Changed Elements

This report identifies elements that have been added, modified, and/or removed. For each element, the report can also identify a variety of associated data, such as approval IDs or specific attributes that changed. It is generally run as needed, to help Operations identify what changed when a service-affecting problem occurs, thus reducing Mean Time To Repair (MTTR).



DB2 Changes

Node: DB2:TRADEDB (DB2 Database Server)

Date	Element	Change Type
1/18/19 11:46 AM	Query=Changes to automatic storage paths for database	Modified

Node: SuSE (Linux Server)

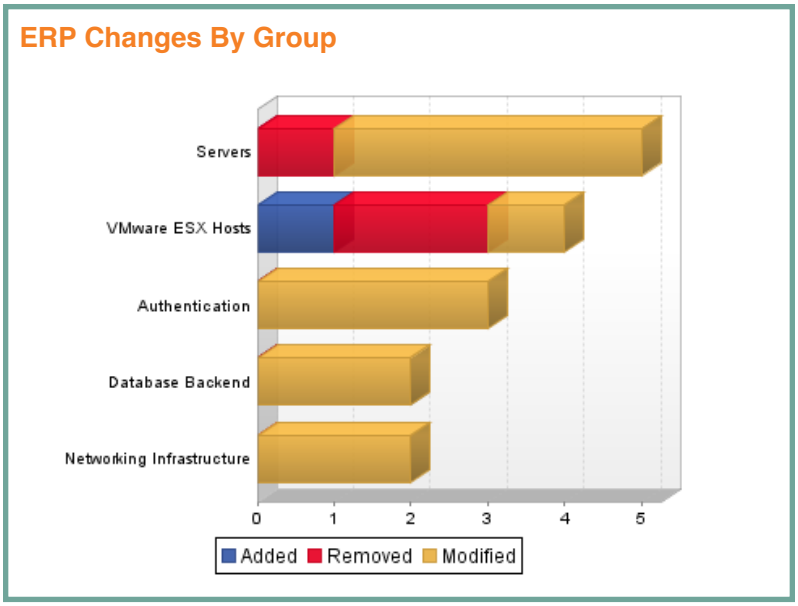
Date	Element	Change Type
1/18/19 11:46 AM	/home/db2inst1/sqllib/db2nodez.cfg	Modified

Summary

Total nodes	2
Total elements	2

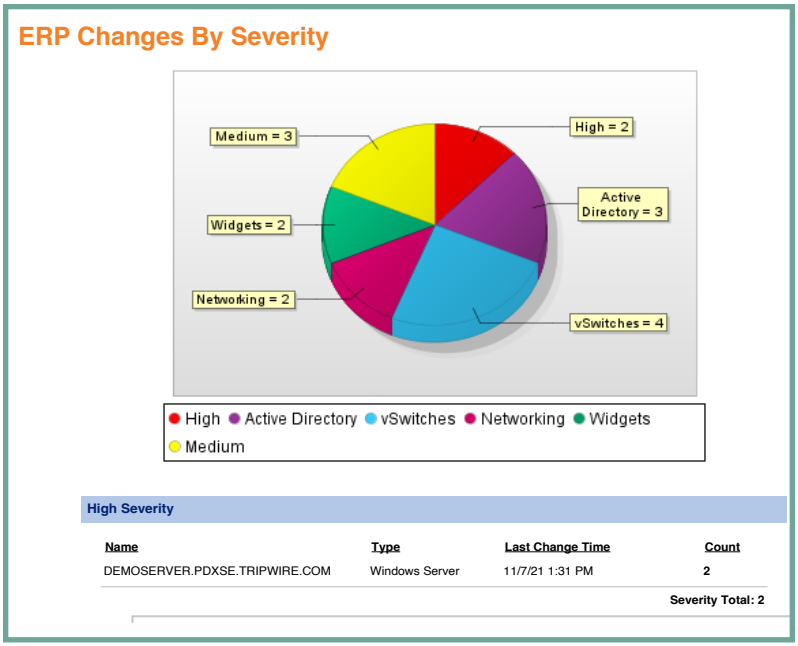
Changes by Node or Group

This report displays the number of changes detected on one or more monitored systems. The change comparison calculates the total number of changes for each system, as well as the totals for each type of change (added, removed, or modified). This is a management report providing an overview of the types and locations of changes, and is typically run weekly.



Changes by Severity

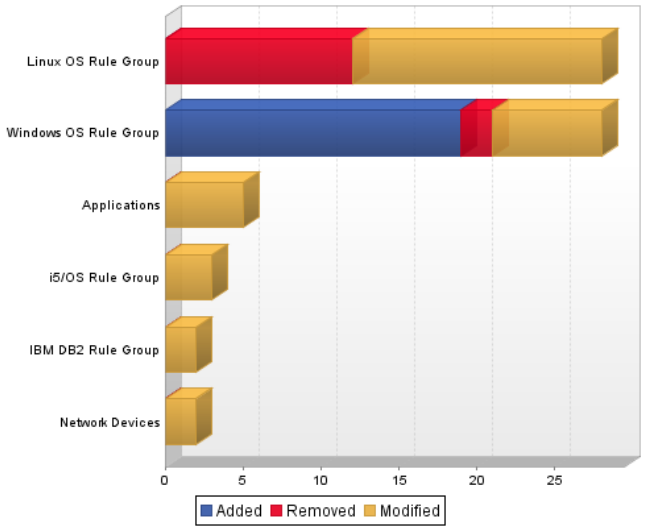
This report shows the total number of changes detected on selected monitored systems that fall within a specified range of severity levels, helping operations staff identify changes that have the potential to adversely impact service quality. It is normally run daily.



Changes by Rule or Group

This report calculates the number of change versions for monitored objects identified by each specified rule or rule group. For each rule or group, the report also calculates the total number of change versions for each type of change, e.g. added, removed, or modified changes. Often used as a means of identifying network resources that experience an abnormally high rate of change.

Changes By Rule or Group



Details

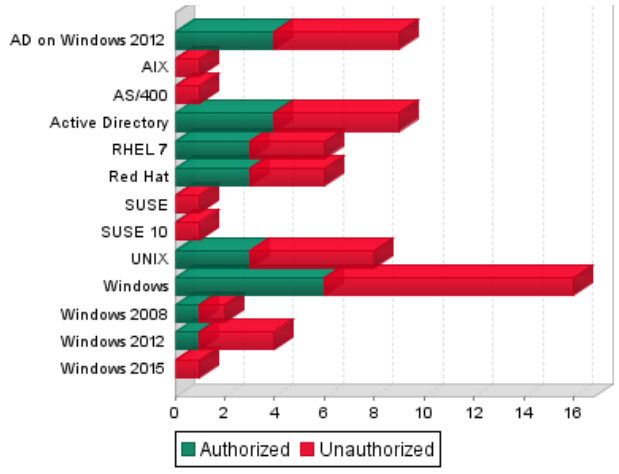
Name	Type	Added	Removed	Modified	Total
Linux OS Rule Group	Rule Group	0	12	16	28
Windows OS Rule Group	Rule Group	19	2	7	28
Applications	Rule Group	0	0	5	5
i5/OS Rule Group	Rule Group	0	0	3	3
IBM DB2 Rule Group	Rule Group	0	0	2	2
Network Devices	Rule Group	0	0	2	2

Total Changes	Added	Removed	Modified	Total
	19	14	35	68

Composite Changes by Node

This report is typically used to enforce change management policies by tabulating the number and authorization of composite changes. A composite change consists of one or more element versions created for a single node in a single time interval specified by the report (such as a day or week). This report calculates the number of authorized and unauthorized composite changes for each specified node and/or node group within a specified period of time.

Composite Changes By Node



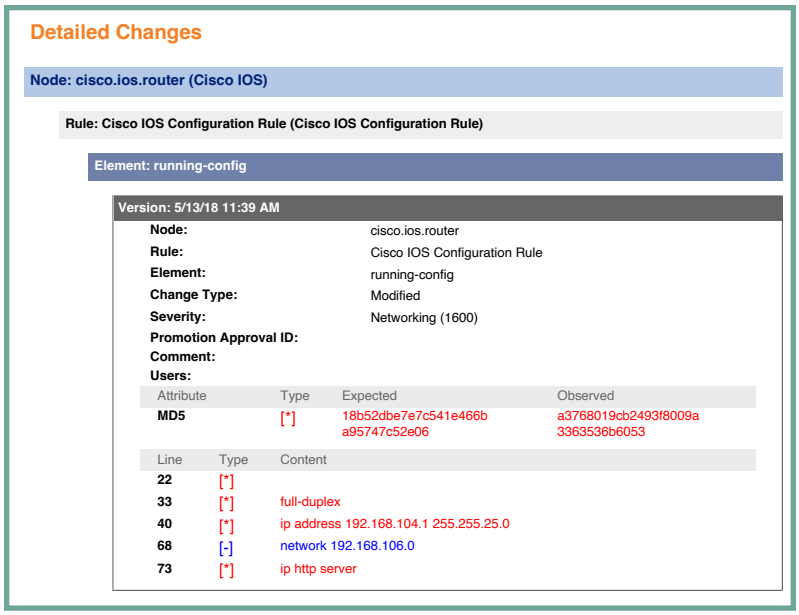
Node Groups

AD on Windows 2012

No changes matching the report criteria were found for this node group

Detailed Changes

This report compiles comprehensive change information for monitored objects associated with specified monitored systems. It is typically run ad hoc to help Operations identify what changed when there is a service affecting problem, in order to reduce MTTR. It can also be used to automatically reconcile authorized changes and to generate alerts for unauthorized changes.



Detailed Changes

Node: cisco.ios.router (Cisco IOS)

Rule: Cisco IOS Configuration Rule (Cisco IOS Configuration Rule)

Element: running-config

Version: 5/13/18 11:39 AM

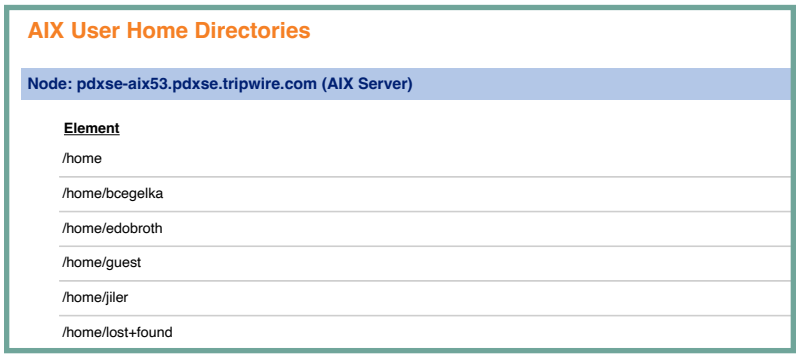
Node:	cisco.ios.router
Rule:	Cisco IOS Configuration Rule
Element:	running-config
Change Type:	Modified
Severity:	Networking (1600)
Promotion Approval ID:	
Comment:	
Users:	

Attribute	Type	Expected	Observed
MD5	[*]	18b52dbe7e7c541e466b a95747c52e06	a3768019cb2493f8009a 3363536b6053

Line	Type	Content
22	[*]	
33	[*]	full-duplex
40	[*]	ip address 192.168.104.1 255.255.25.0
68	[-]	network 192.168.106.0
73	[*]	ip http server

Elements

This report lists all elements identified by the specified criteria. Optionally, the report can also identify the package associated with each element. By identifying the elements, Operations can ensure that the proper systems, files, settings, configurations, etc. are monitored. It is typically run on a monthly basis.



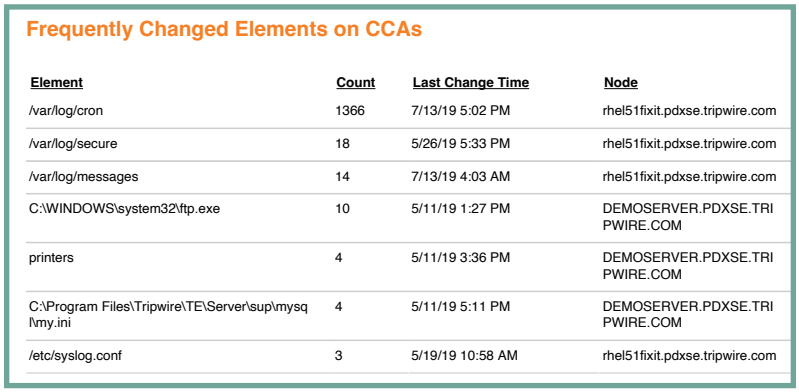
AIX User Home Directories

Node: pdxse-aix53.pdxse.tripwire.com (AIX Server)

Element
/home
/home/bcegelka
/home/edobroth
/home/guest
/home/jiler
/home/lost+found

Frequently Changed Elements

This report ranks the most frequently changed elements that meet the specified criteria. For each element, the report identifies the total number of changes, the time of the most recent change, and the element's node. This management report identifies elements that change on a regular basis as part of normal business processes, the data then being used to tune monitoring rules for more efficient integrity checks. In general usage, it is run weekly until rules are tuned, then monthly.



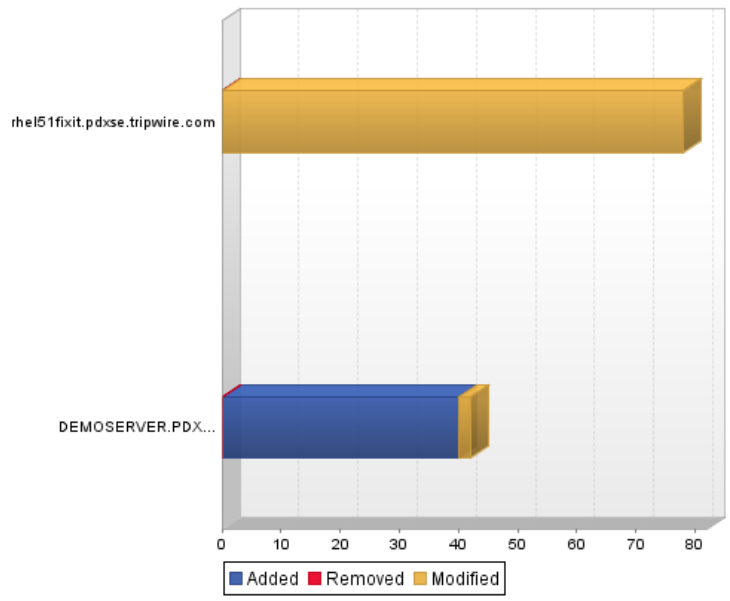
Frequently Changed Elements on CCAs

Element	Count	Last Change Time	Node
/var/log/cron	1366	7/13/19 5:02 PM	rhel51fixit.pdxse.tripwire.com
/var/log/secure	18	5/26/19 5:33 PM	rhel51fixit.pdxse.tripwire.com
/var/log/messages	14	7/13/19 4:03 AM	rhel51fixit.pdxse.tripwire.com
C:\WINDOWS\system32\ftp.exe	10	5/11/19 1:27 PM	DEMOSERVER.PDXSE.TRIPWIRE.COM
printers	4	5/11/19 3:36 PM	DEMOSERVER.PDXSE.TRIPWIRE.COM
C:\Program Files\Tripwire\TE\Server\sup\mysql\my.ini	4	5/11/19 5:11 PM	DEMOSERVER.PDXSE.TRIPWIRE.COM
/etc/syslog.conf	3	5/19/19 10:58 AM	rhel51fixit.pdxse.tripwire.com

Frequently Changed Nodes

This report ranks the most frequently changed monitored systems that meet the specified criteria. The report includes the total number of detected changes for each system, as well as the totals for each type of change (added, removed, or modified). This management report is used to identify nodes that could potentially cause problems due to frequent changes, and is typically generated weekly.

Frequently Changed Critical Cyber Assests



Details

Name	Type	Added	Removed	Modified	Total
rhel51fixit.pdxse.tripwire.com	Linux Server	0	0	78	78
DEMOSERVER.PDXSE.TRIPWIRE.COM	Windows Server	40	0	2	42
Total Changes:		**40**	**0**	**80**	**120**

Missing Elements

This report identifies nodes that lack elements with specific names, or elements created by a specific rule or rule group, allowing users to pick either rules or element names and determine whether or not they are missing on a target set of nodes. This report helps Tripwire Enterprise administrators configure the application to detect configuration drift, and is generally run weekly or monthly.

AIX servers missing BIND

Node: pdxse-aix53.pdxse.tripwire.com (AIX Server)

Rule
Bind - Configuration Files (UNIX File System Rule)
Bind - Zone Files (UNIX File System Rule)

Change Audit Coverage

This report identifies the components associated with each file system, database and directory rule in a Tripwire Enterprise implementation, to determine if the appropriate rules are applied to the correct systems and devices. It is typically run monthly, or whenever new rules are created to ensure that they are correctly defined.

Solaris Core OS Rules

Date:	7/20/19 1:14 PM
Display criteria at end:	No
Rules:	Solaris 10, Solaris 8 and 9, Solaris OS Rule Group
Rule name:	Not applied
Rules sort:	Name, ascending
Start points sort:	Name, ascending
Stop points sort:	Name, ascending

Rule: /dev/audio Permissions

Properties

Type:	Command Output Capture Rule
Description:	
Command Line:	ls -lL /dev/audio 2>/dev/null | awk '{print $1,$3,$4,$NF}'
Severity:	0 (None)

Rule: /etc/inetd.conf Permissions

Properties

Type:	Command Output Capture Rule
Description:	
Command Line:	ls -lL /etc/inetd.conf 2>/dev/null | awk '{print $1,$3,$4,$NF}'
Severity:	0 (None)

Rule: /etc/shells Content

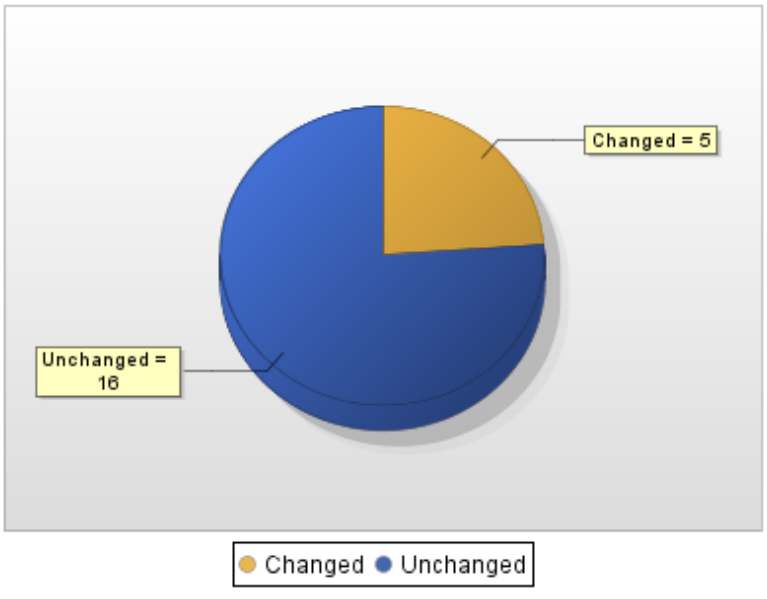
Properties

Type:	Command Output Capture Rule
Description:	
Command Line:	Shells=`(cat /etc/passwd 2>/dev/null; ypcat passwd 2>/dev/null) | awk -F: '{print $7}' \| egrep -v "false$|null$\|true$|sdshell$\|^/sbin/nologin$" | sort -u`; if [-f /etc/shells]; then for Shell in $Shel ls; do if [`egrep -c $Shell /etc/shells 2>/dev/null` -eq 0]; then echo "$Shell does not exist in /etc/ shells"; fi;done; else echo "/etc/shells does not exist";fi
Severity:	0 (None)

Nodes with Changes

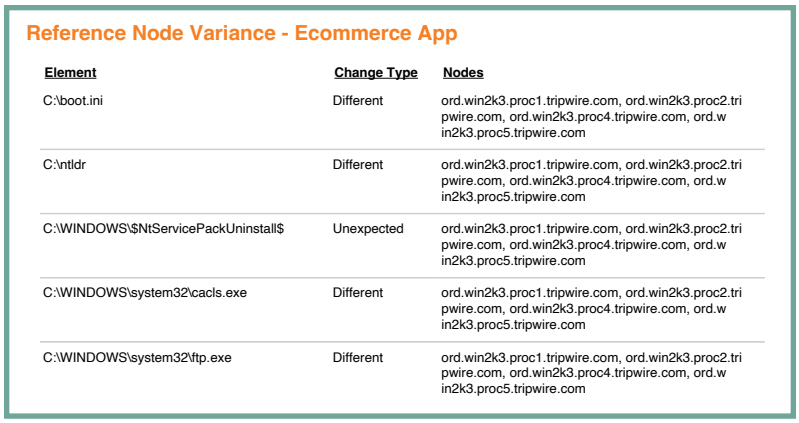
For the specified criteria, this report identifies the number of monitored systems that have changed over a given period of time, providing a synopsis of changed vs. unchanged systems or devices. It is generally run weekly or monthly.

ERP Nodes With Changes



Reference Node Variance

This report identifies all elements that differ between one node (the reference node) and another (the compare node). In a single report the reference node may be compared with one or more compare nodes, readily identifying configuration drift, which can lead to system instability and failure. It is typically run weekly or monthly, as well as following each patch installation.

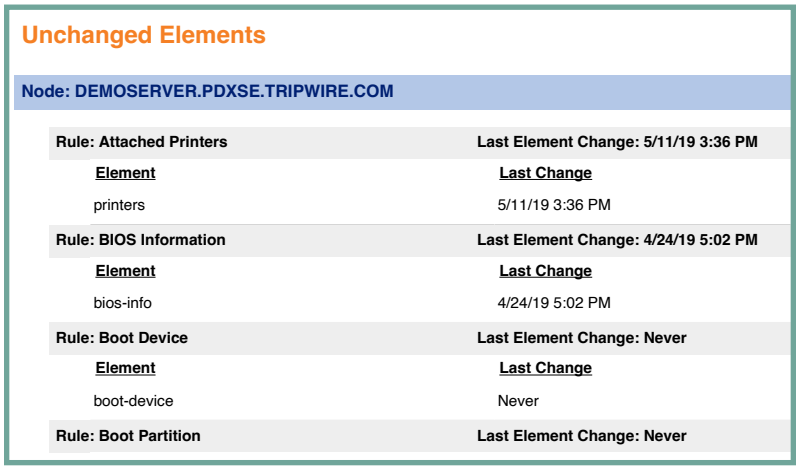


Reference Node Variance - Ecommerce App

Element	Change Type	Nodes
C:\boot.ini	Different	ord.win2k3.proc1.tripwire.com, ord.win2k3.proc2.tripwire.com, ord.win2k3.proc4.tripwire.com, ord.win2k3.proc5.tripwire.com
C:\ntldr	Different	ord.win2k3.proc1.tripwire.com, ord.win2k3.proc2.tripwire.com, ord.win2k3.proc4.tripwire.com, ord.win2k3.proc5.tripwire.com
C:\WINDOWS\$NtServicePackUninstall$	Unexpected	ord.win2k3.proc1.tripwire.com, ord.win2k3.proc2.tripwire.com, ord.win2k3.proc4.tripwire.com, ord.win2k3.proc5.tripwire.com
C:\WINDOWS\system32\cacls.exe	Different	ord.win2k3.proc1.tripwire.com, ord.win2k3.proc2.tripwire.com, ord.win2k3.proc4.tripwire.com, ord.win2k3.proc5.tripwire.com
C:\WINDOWS\system32\ftp.exe	Different	ord.win2k3.proc1.tripwire.com, ord.win2k3.proc2.tripwire.com, ord.win2k3.proc4.tripwire.com, ord.win2k3.proc5.tripwire.com

Unchanged Elements

For one or more nodes, this report identifies all elements for which Tripwire Enterprise did not detect a change in the specified time range. Alternatively, the report can identify the rules used to baseline any unchanged elements. It is used to detect elements that were expected to change over a period of time, but did not. This management report is typically run monthly, or as needed.



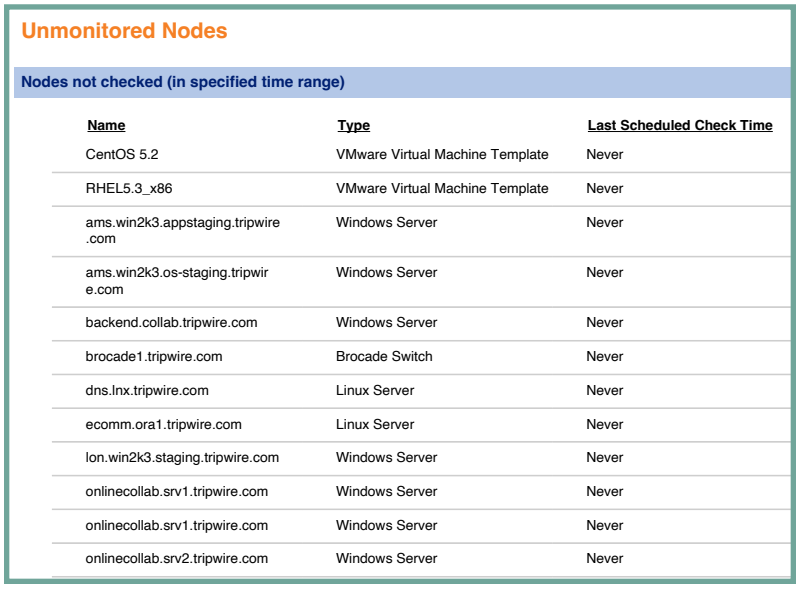
Unchanged Elements

Node: DEMOSERVER.PDXSE.TRIPWIRE.COM

Rule: Attached Printers	**Last Element Change: 5/11/19 3:36 PM**
Element	**Last Change**
printers	5/11/19 3:36 PM
Rule: BIOS Information	**Last Element Change: 4/24/19 5:02 PM**
Element	**Last Change**
bios-info	4/24/19 5:02 PM
Rule: Boot Device	**Last Element Change: Never**
Element	**Last Change**
boot-device	Never
Rule: Boot Partition	**Last Element Change: Never**

Unmonitored Nodes

This administrative report is used to ensure that the proper nodes are being monitored in your Tripwire Enterprise implementation. It identifies: 1) Nodes that lack a valid Tripwire Enterprise license; 2) Nodes that have not been baselined or version checked within a specified period of time and 3) Monitored virtual machines on which a Tripwire Enterprise agent has not been installed and enabled.



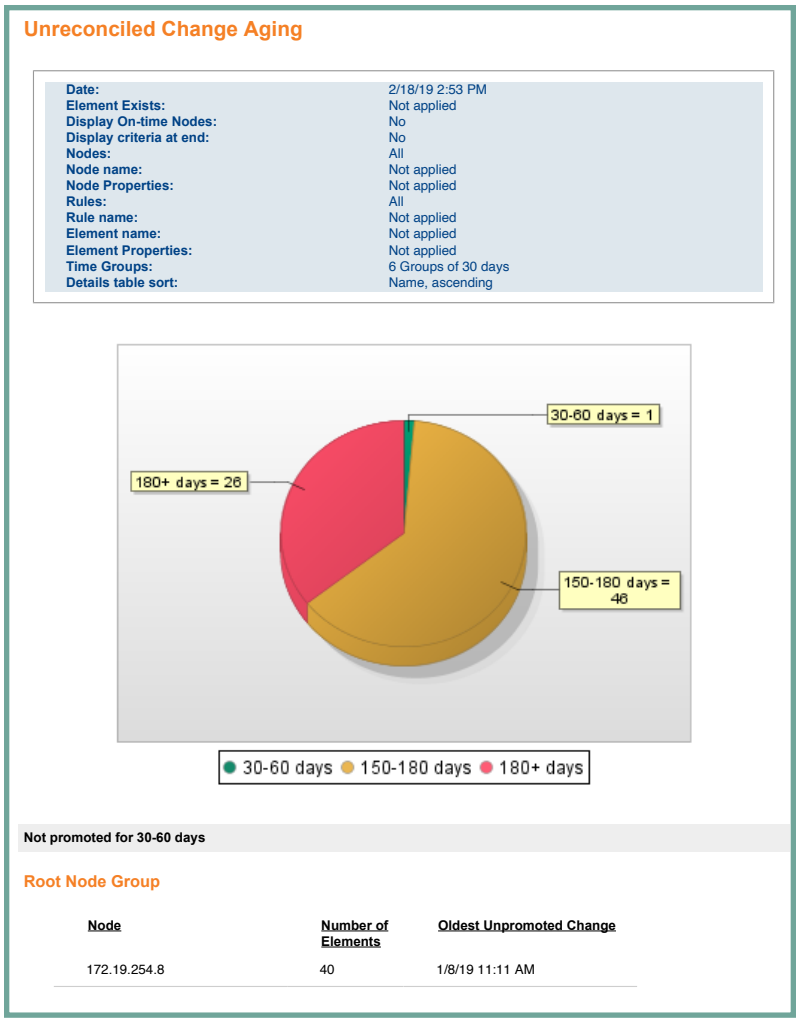
Unmonitored Nodes

Nodes not checked (in specified time range)

Name	Type	Last Scheduled Check Time
CentOS 5.2	VMware Virtual Machine Template	Never
RHEL5.3_x86	VMware Virtual Machine Template	Never
ams.win2k3.appstaging.tripwire.com	Windows Server	Never
ams.win2k3.os-staging.tripwire.com	Windows Server	Never
backend.collab.tripwire.com	Windows Server	Never
brocade1.tripwire.com	Brocade Switch	Never
dns.lnx.tripwire.com	Linux Server	Never
ecomm.ora1.tripwire.com	Linux Server	Never
lon.win2k3.staging.tripwire.com	Windows Server	Never
onlinecollab.srv1.tripwire.com	Windows Server	Never
onlinecollab.srv1.tripwire.com	Windows Server	Never
onlinecollab.srv2.tripwire.com	Windows Server	Never

Unreconciled Change Aging

When an organization strives to adhere to proactive change management practices it's important to know which changes have remained unreconciled the longest, and why. The Unreconciled Change Aging report provides this information graphically, immediately and accurately, detailing the infrastructure changes that have gone the longest without being addressed, and helping prioritize reconciliation efforts.



Unreconciled Change Aging

Date:	2/18/19 2:53 PM
Element Exists:	Not applied
Display On-time Nodes:	No
Display criteria at end:	No
Nodes:	All
Node name:	Not applied
Node Properties:	Not applied
Rules:	All
Rule name:	Not applied
Element name:	Not applied
Element Properties:	Not applied
Time Groups:	6 Groups of 30 days
Details table sort:	Name, ascending

Not promoted for 30-60 days

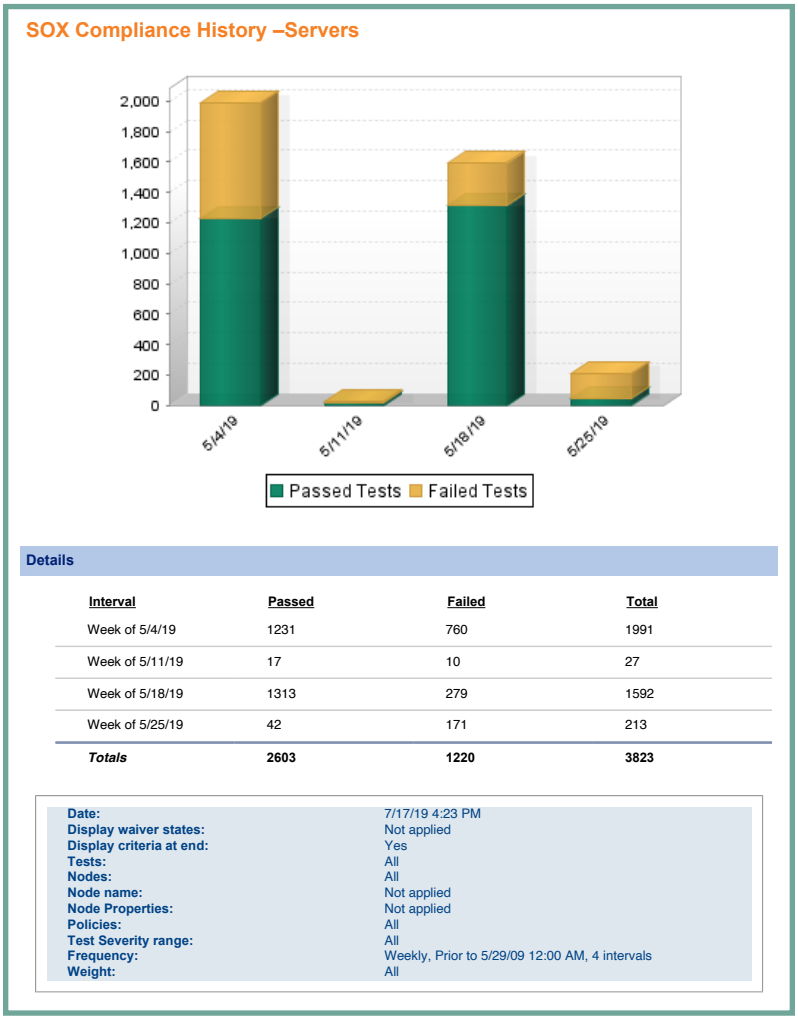
Root Node Group

Node	Number of Elements	Oldest Unpromoted Change
172.19.254.8	40	1/8/19 11:11 AM

Compliance Policy Management Reports

Compliance History

This report calculates the number of passing and failing policy test results created for all specified nodes for each specified time interval. It is typically used as a management report showing the historic trend of compliance with a policy.



SOX Compliance History –Servers

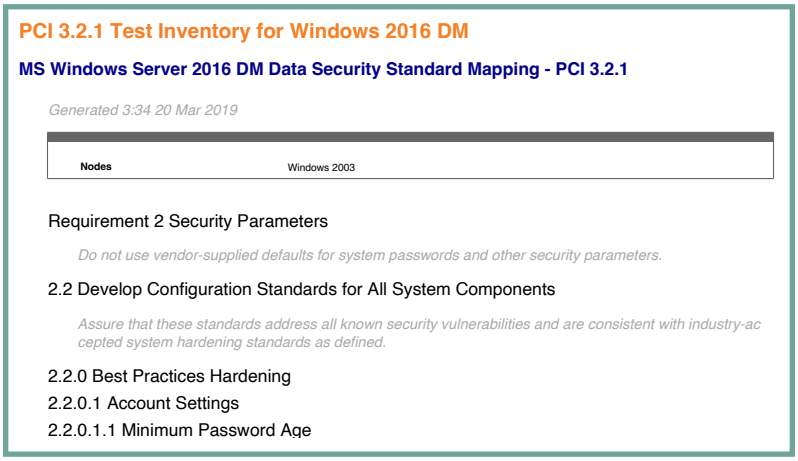
Details

Interval	Passed	Failed	Total
Week of 5/4/19	1231	760	1991
Week of 5/11/19	17	10	27
Week of 5/18/19	1313	279	1592
Week of 5/25/19	42	171	213
Totals	**2603**	**1220**	**3823**

Date:	7/17/19 4:23 PM
Display waiver states:	Not applied
Display criteria at end:	Yes
Tests:	All
Nodes:	All
Node name:	Not applied
Node Properties:	Not applied
Policies:	All
Test Severity range:	All
Frequency:	Weekly, Prior to 5/29/09 12:00 AM, 4 intervals
Weight:	All

Detailed Test Inventory

For each specified test, this report provides a test definition that includes details such as test description, type, severity and weighting. This report makes it easy for management to generate and share formal test documentation, as well as view this information offline. Most often used as a reference list that documents the properties of specified policy tests.



PCI 3.2.1 Test Inventory for Windows 2016 DM

MS Windows Server 2016 DM Data Security Standard Mapping - PCI 3.2.1

Generated 3:34 20 Mar 2019

Nodes	Windows 2003

Requirement 2 Security Parameters

Do not use vendor-supplied defaults for system passwords and other security parameters.

2.2 Develop Configuration Standards for All System Components

Assure that these standards address all known security vulnerabilities and are consistent with industry-ac cepted system hardening standards as defined.

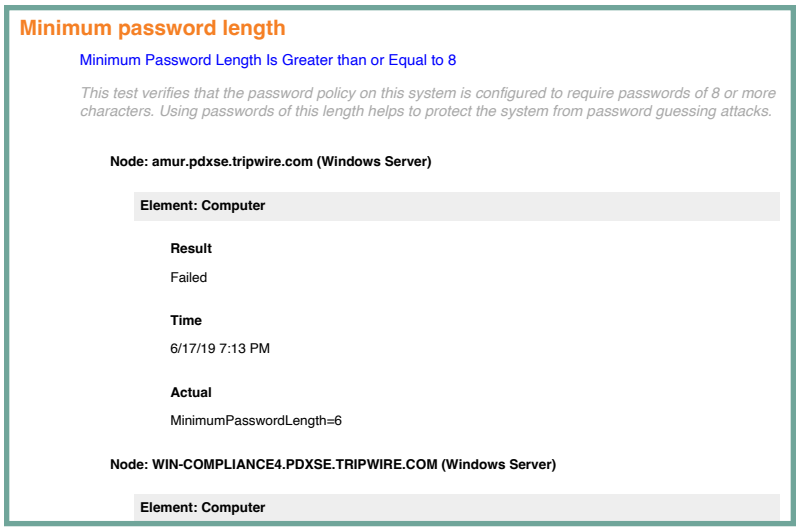
2.2.0 Best Practices Hardening

2.2.0.1 Account Settings

2.2.0.1.1 Minimum Password Age

Detailed Test Results

This report lists all policy results for each specified node that meet the specified report criteria. For each result, the output indicates which element was tested, and the outcome (passed/failed). This report is a means of identifying specific settings that are out of compliance with a policy and that may require modification.



Minimum password length

Minimum Password Length Is Greater than or Equal to 8

This test verifies that the password policy on this system is configured to require passwords of 8 or more characters. Using passwords of this length helps to protect the system from password guessing attacks.

Node: amur.pdxse.tripwire.com (Windows Server)

Element: Computer

Result

Failed

Time

6/17/19 7:13 PM

Actual

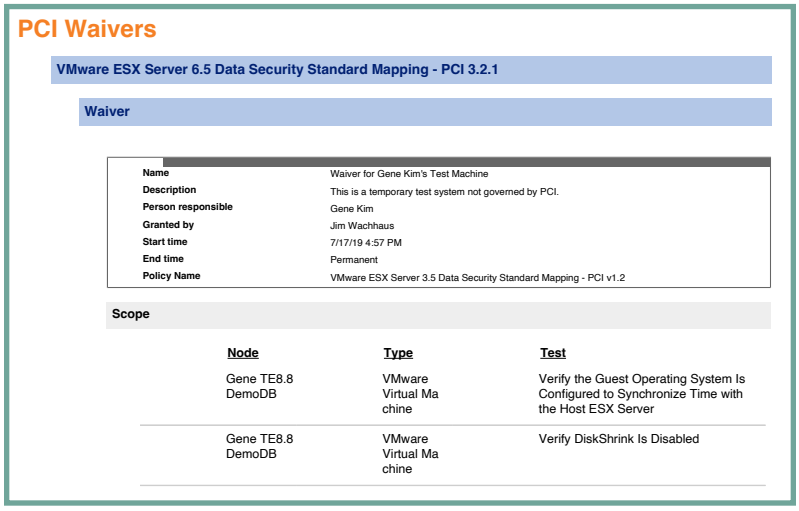
MinimumPasswordLength=6

Node: WIN-COMPLIANCE4.PDXSE.TRIPWIRE.COM (Windows Server)

Element: Computer

Detailed Waivers

This report provides a detailed list documenting the properties of all specified waivers. For each specified node and test, it provides a complete listing of the waivers and related details such as start and end dates, reason for the waiver, and who is responsible for remediation. Security and IT operations can use this report to better manage waivers and remediation with less effort.



PCI Waivers

VMware ESX Server 6.5 Data Security Standard Mapping - PCI 3.2.1

Waiver

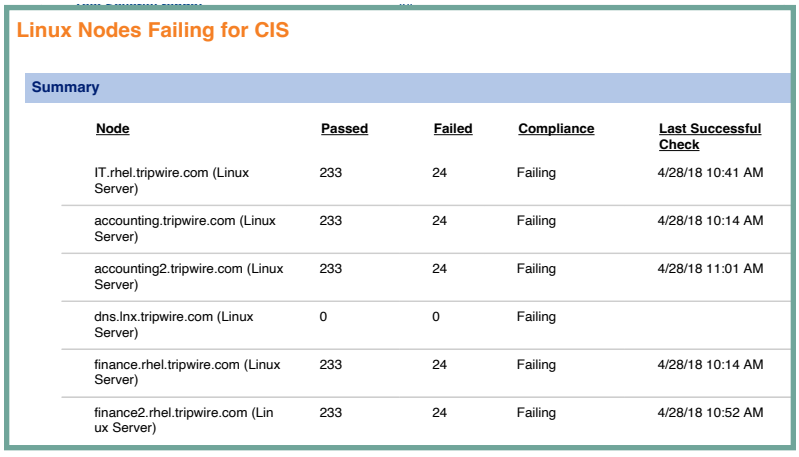
Name	Waiver for Gene Kim's Test Machine
Description	This is a temporary test system not governed by PCI.
Person responsible	Gene Kim
Granted by	Jim Wachhaus
Start time	7/17/19 4:57 PM
End time	Permanent
Policy Name	VMware ESX Server 3.5 Data Security Standard Mapping - PCI v1.2

Scope

Node	Type	Test
Gene TE8.8 DemoDB	VMware Virtual Machine	Verify the Guest Operating System Is Configured to Synchronize Time with the Host ESX Server
Gene TE8.8 DemoDB	VMware Virtual Machine	Verify DiskShrink Is Disabled

Test Results by Node

This report provides a reference list showing failed policy test results that indicate monitored systems requiring remediation. It presents data about policy test results for all nodes specified by the report criteria. The output of the report contains: 1) A summary list of nodes, which includes the total number of policy test results that each node passed and failed; 2) A detailed list of nodes, which includes a sub-list of policy tests run on each node. (For each policy test, this list may also indicate the test's rule(s) and version-attribute conditions); 3) A list of nodes that experienced errors when a policy test was run.



Linux Nodes Failing for CIS

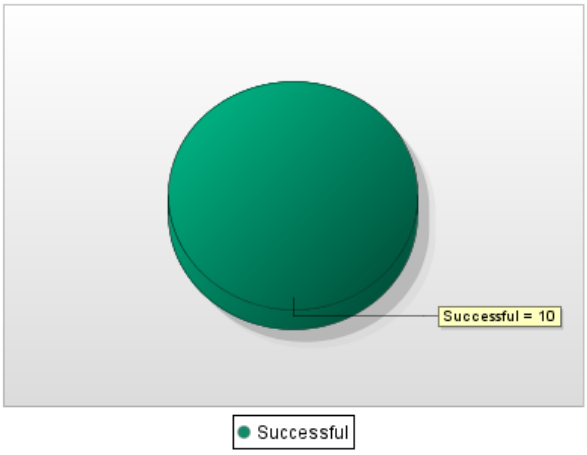
Summary

Node	Passed	Failed	Compliance	Last Successful Check
IT.rhel.tripwire.com (Linux Server)	233	24	Failing	4/28/18 10:41 AM
accounting.tripwire.com (Linux Server)	233	24	Failing	4/28/18 10:14 AM
accounting2.tripwire.com (Linux Server)	233	24	Failing	4/28/18 11:01 AM
dns.lnx.tripwire.com (Linux Server)	0	0	Failing	
finance.rhel.tripwire.com (Linux Server)	233	24	Failing	4/28/18 10:14 AM
finance2.rhel.tripwire.com (Linux Server)	233	24	Failing	4/28/18 10:52 AM

Remediation Assessment

Use this report when you need to know not only which remediations have been performed, but also understand post-remediation actions and dispositions across all work orders. It also shows the total number of nodes remediation was applied to, as well as the number of successful remediations across all work orders. Because this report provides details on a number of remediation runs over a given time period, it provides excellent success metrics for determining Remediation Manager's overall ROI.

This Week's Remediations



Other Account Management Events: Success and Failure

This test determines whether 'Account Management: Other Account Management Events' are being record ed on success and failure. This setting supports system integrity and confidentiality by recording events that change domain policy and access password hashes (precursor to offline dictionary attacks).

Manual Post Remediation Steps

No additional Post Remediation steps

Command Line

```
cscript $(ScriptFile.vbs)
```

Script

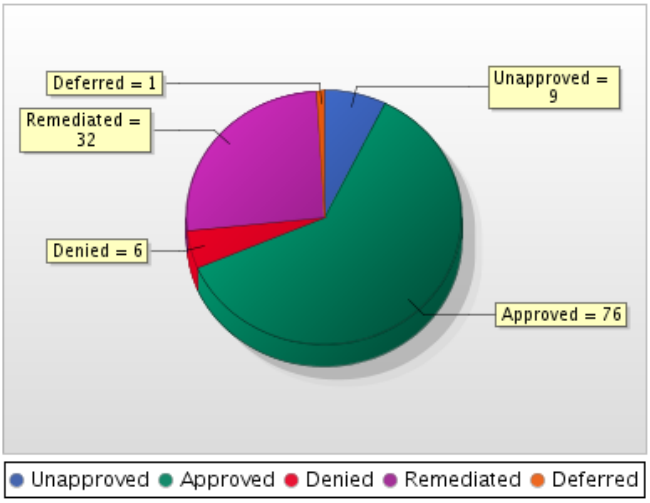
```
'cscript $(ScriptFile.vbs)
On Error Resume Next
' Initialize Variables

SubCategory = "Other Account Management Events"
Audit = "/success:enable /failure:enable"
Description = "Success and Failure"

SetAudit = "cmd /c Auditpol /set /subcategory:""" & SubCategory & """ " & Audit

' Create Exec object to run the command line
Set WSHShell = WScript.CreateObject("WScript.Shell")

' Issue the command to set audit policy
Set OExec = WSHShell.exec(SetAudit)
If (OExec.StdErr.ReadAll = "") Then
    WScript.Echo "SUCCESS-5001: Audit [" & Description &_
        "] applied to [" & SubCategory & "] subcategory"
    WScript.Quit (0)
Else
    WScript.Echo "FAILURE-5001: Could not apply audit [" & Description &_
        "] to [" & SubCategory & "] subcategory"
    WScript.Quit (5001)
End If
```

Remediation Work Order Details

This report provides detailed information about remediation work orders and remediation entries, including how many policy test repairs were Approved, Remediated, Deferred or Denied in the specific work order. This gives an instant overview into the overall effectiveness of a given Remediation Work Order, as well as cost savings, descriptions of the scripts being executed, times they were run, and any alerts or errors that might have occurred.

PCI Remediation Work Order Status

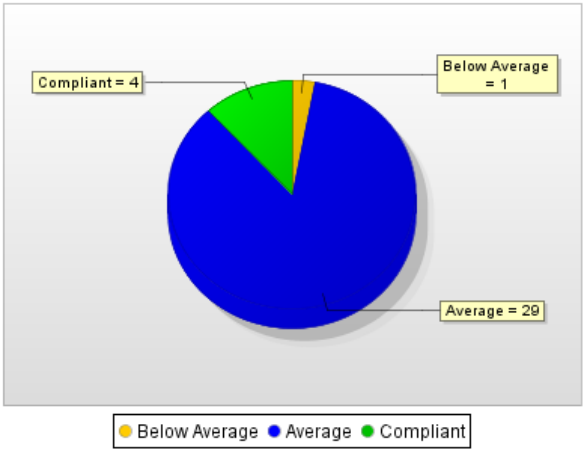
Date:	6/22/19 12:02 PM
Chart type:	Remediation Entry States
Work Order Approval Id:	Not applied
Display Remediation Entries:	Yes
Display Policy Tests:	Yes
Display Nodes:	Yes
Display Elements and Versions:	No
Display Remediator:	No
Display associated log messages:	No
Maximum per item (0 = all):	0
Display criteria at end:	No
Creators:	All
Owners:	All
Work Order States:	Not applied
Remediation Entry States:	Not applied
Nodes:	rhel-crash-box
Node names:	Not applied
Node Properties:	Not applied
Tests:	All
Work Orders sort:	State, ascending
Remediation Entries sort:	State, ascending



Scoring

For each specified policy test or policy test group, this report indicates the number and percentage of nodes that are in full compliance with the test (or group), and the number of nodes that are not in full compliance. This is used as a high-level management report providing a comprehensive view of compliance throughout your organization.

NERC Scoring for Windows



MS Windows Server 2003 DM - NERC v2

Compliant

Node	Score	Waived Tests
WIN-COMPLIANCE2.PDXSE.TRIPWIRE.COM	77.19	0
WIN-COMPLIANCE3.PDXSE.TRIPWIRE.COM	77.19	0
WIN-COMPLIANCE4.PDXSE.TRIPWIRE.COM	77.19	0
WIN-COMPLIANCE5.PDXSE.TRIPWIRE.COM	77.19	0

Average

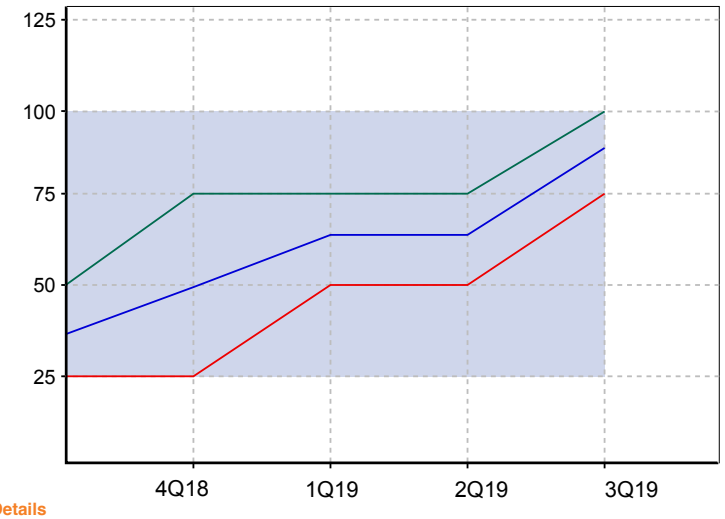
Node	Score	Waived Tests
ams.win2k3.dc1.tripwire.com	76.51	0
ams.win2k3.dc2.tripwire.com	76.51	0
ams.win2k3.dc3.tripwire.com	76.51	0
ams.win2k3.dc4.tripwire.com	76.51	0
ams.win2k3.dc5.tripwire.com	76.51	0
ams.win2k3.dc6.tripwire.com	76.51	0

Scoring History

This is a management report that indicates past trends in the policy scores of monitored nodes For all policy scores that satisfy the report's criteria, this report presents the following data for each period in the specified time range: 1) The highest and lowest policy scores for the period (green and red lines) and 2) The average policy score for the period (blue line).

Linux Scoring History

Date:	7/20/19 3:30 PM
Display raw score (without waivers):	No
Display criteria at end:	No
Nodes:	Red Hat
Node name:	Not applied
Node Properties:	Not applied
Policies:	All
Frequency:	Daily, Prior to report run, 7 intervals



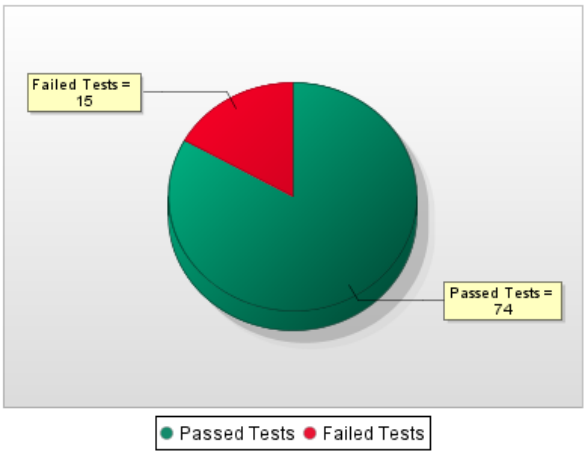
Details

Interval	Average	Min	Max
7/14/19	39.59	1.79	79.16
7/15/19	39.59	1.79	79.16
7/16/19	39.59	1.79	79.16
7/17/19	39.59	1.79	79.16
7/18/19	39.59	1.79	79.16
7/19/19	39.59	1.79	79.16
7/20/19	39.59	1.79	79.16
Totals:	**39.59**	**1.79**	**79.16**

Test Results Summary

This high-level management report provides a comprehensive view of compliance throughout your organization. For each specified Policy Manager object, this report indicates: 1) The number of specified nodes that are not in full compliance with the Policy Manager object; 2) The number and percentage of specified nodes that are in full compliance with the object. Note: In some previous versions of Tripwire Enterprise, this report was known as a 'Policy Scorecard Report.'

NERC CIP-005-1.R2 for SUSE (Electronic Access Controls)



R2 Electronic Access Controls

R2.1 Access Control

R2.1.1 Limit Access to Trusted Networks

Verify That Unlimited Network Access Is Turned off

Node	Passed Tests	Failed Tests	Percent Compliant
SuSE	1	0	100%

R2.1.2 'root' Should Be the Only Entry in /etc/cron.allow

'root' Should Be the Only Entry in /etc/cron.allow

Node	Passed Tests	Failed Tests	Percent Compliant
SuSE	0	1	0%

R2.1.3 'root' Should Be the Only Entry in /etc/at.allow

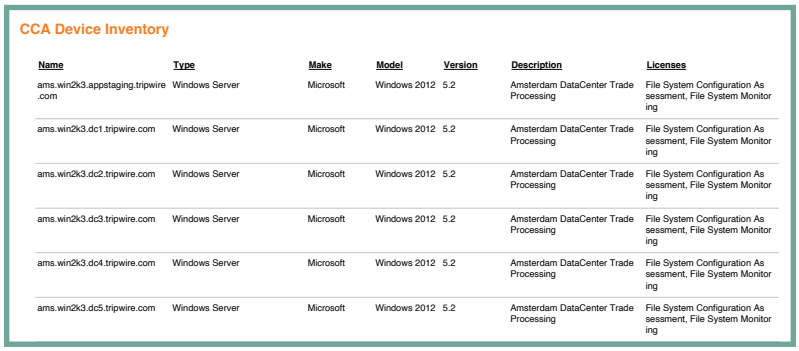
'root' Should Be the Only Entry in /etc/at.allow

Node	Passed Tests	Failed Tests	Percent Compliant

System Reports

Device Inventory

This report provides a reference list of monitored systems. It identifies the make, model, and version of specified monitored systems. This management report showing devices being monitored helps insure that the correct systems and nodes are being controlled. It is generally run monthly, potentially more frequently depending on process maturity.



CCA Device Inventory

Name	Type	Make	Model	Version	Description	Licenses
ams.win2k3.appstaging.tripwire.com	Windows Server	Microsoft	Windows 2012	5.2	Amsterdam DataCenter Trade Processing	File System Configuration Assessment, File System Monitoring
ams.win2k3.dc1.tripwire.com	Windows Server	Microsoft	Windows 2012	5.2	Amsterdam DataCenter Trade Processing	File System Configuration Assessment, File System Monitoring
ams.win2k3.dc2.tripwire.com	Windows Server	Microsoft	Windows 2012	5.2	Amsterdam DataCenter Trade Processing	File System Configuration Assessment, File System Monitoring
ams.win2k3.dc3.tripwire.com	Windows Server	Microsoft	Windows 2012	5.2	Amsterdam DataCenter Trade Processing	File System Configuration Assessment, File System Monitoring
ams.win2k3.dc4.tripwire.com	Windows Server	Microsoft	Windows 2012	5.2	Amsterdam DataCenter Trade Processing	File System Configuration Assessment, File System Monitoring
ams.win2k3.dc5.tripwire.com	Windows Server	Microsoft	Windows 2012	5.2	Amsterdam DataCenter Trade Processing	File System Configuration Assessment, File System Monitoring

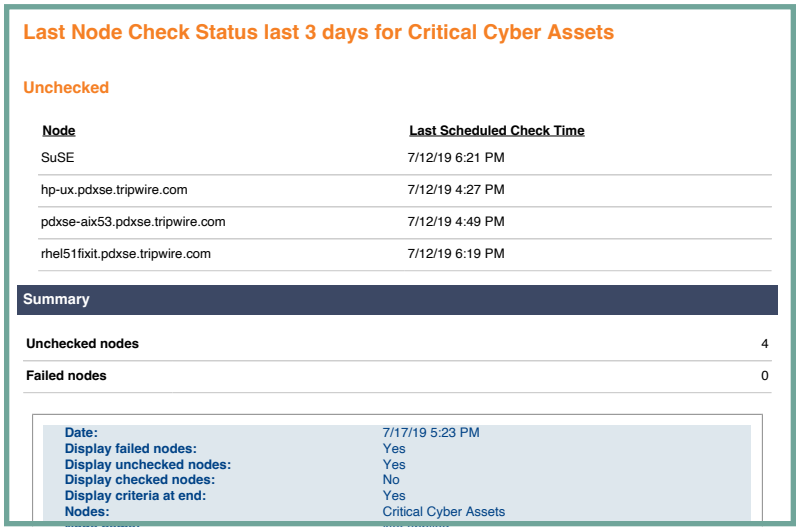
Last Node Check Status

For a specified time range, this report identifies the date and time of the last version check run on one or more monitored systems.

As appropriate, report output can include:

- The names of all nodes for which the last version check ran successfully;
- The names of all nodes for which the last version check failed; and
- The names of all nodes for which a version check was not run.

This management report ensures that nodes are being checked as scheduled without any failures occurring. It is typically run monthly, or more frequently as needed.



Last Node Check Status last 3 days for Critical Cyber Assets

Unchecked

Node	Last Scheduled Check Time
SuSE	7/12/19 6:21 PM
hp-ux.pdxse.tripwire.com	7/12/19 4:27 PM
pdxse-aix53.pdxse.tripwire.com	7/12/19 4:49 PM
rhel51fixit.pdxse.tripwire.com	7/12/19 6:19 PM

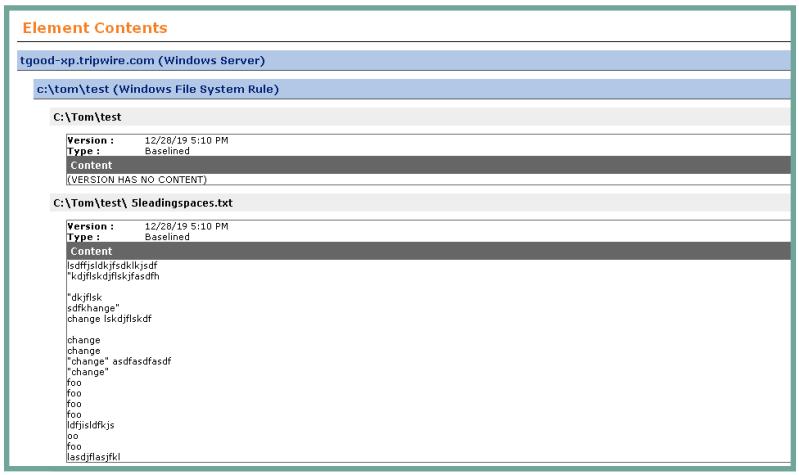
Summary

Unchecked nodes	4
Failed nodes	0

Date:	7/17/19 5:23 PM
Display failed nodes:	Yes
Display unchecked nodes:	Yes
Display checked nodes:	No
Display criteria at end:	Yes
Nodes:	Critical Cyber Assets

Element Contents

The Element Contents report displays the full contents of all Tripwire Enterprise elements—even if the content didn't change from the last baseline. This report is especially useful in conjunction with Command Output Capture Rules (COCR), which gather and output key information about nodes, (e.g., BIOS and OS versions, memory capacities, etc.)



Element Contents

tgood-xp.tripwire.com (Windows Server)

c:\tom\test (Windows File System Rule)

C:\Tom\test

Version : 12/28/19 5:10 PM
Type : Baselined
Content
(VERSION HAS NO CONTENT)

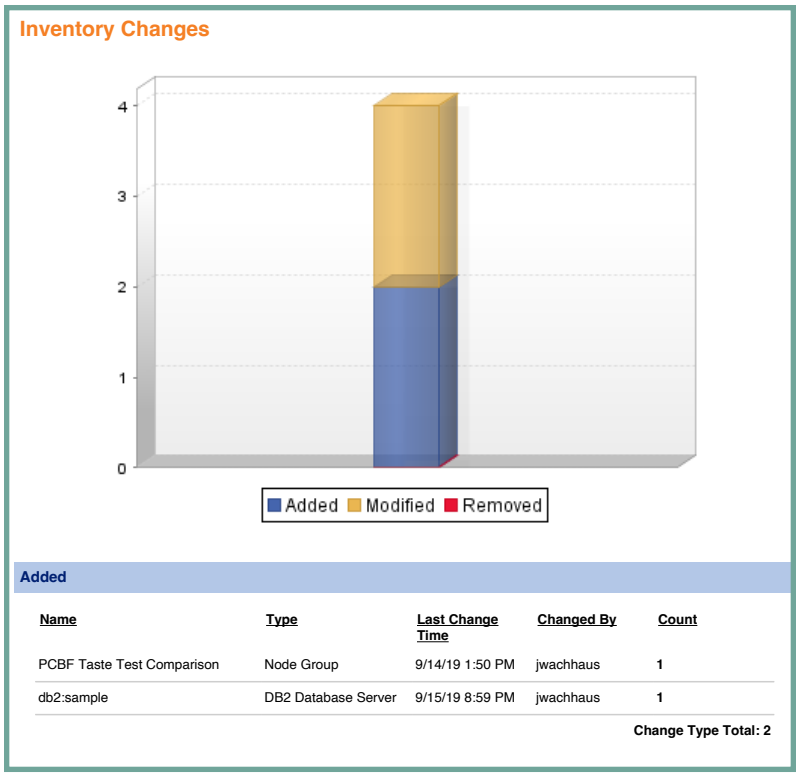
C:\Tom\test\ 5leadingspaces.txt

Version : 12/28/19 5:10 PM
Type : Baselined
Content

```
lsdffjsldkjfsdklkjsdf
"kdjflskdjflskjfasdfh

"dkjflsk
sdfkhange"
change lskdjflskdf

change
change
"change" asdfasdfasdf
"change"
foo
foo
foo
foo
ldfjisldfkjs
oo
foo
lasdjflasjfkl
```

Inventory Changes

This report calculates the number of nodes monitored by the Tripwire Enterprise implementation that have been added, modified, and deleted over a specified period of time. This management report keeps track of systems and nodes on the network, and is normally run at least monthly.



Inventory Changes

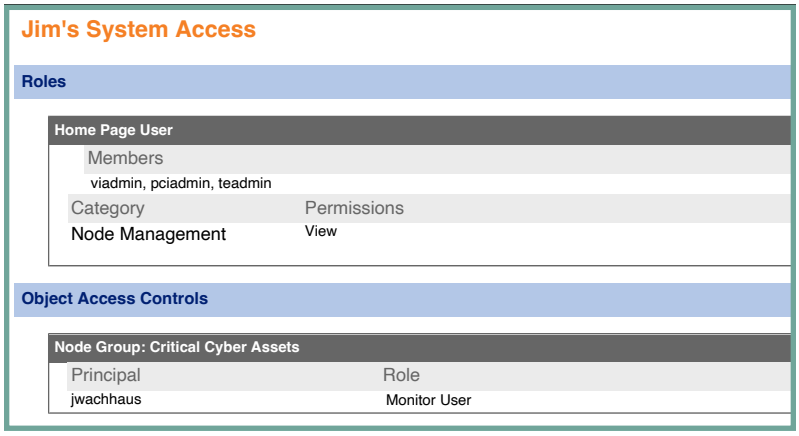
Added

Name	Type	Last Change Time	Changed By	Count
PCBF Taste Test Comparison	Node Group	9/14/19 1:50 PM	jwachhaus	1
db2:sample	DB2 Database Server	9/15/19 8:59 PM	jwachhaus	1

Change Type Total: 2

System Access Control

This report provides security-related information on specified user accounts, user roles, user groups, and/or access controls. This management/ administrator report is used to ensure that correct roles with appropriate access levels are defined, and that the correct users have the correct roles. It is normally run monthly.



Jim's System Access

Roles

Home Page User

Members
viadmin, pciadmin, teadmin

Category	Permissions
Node Management	View

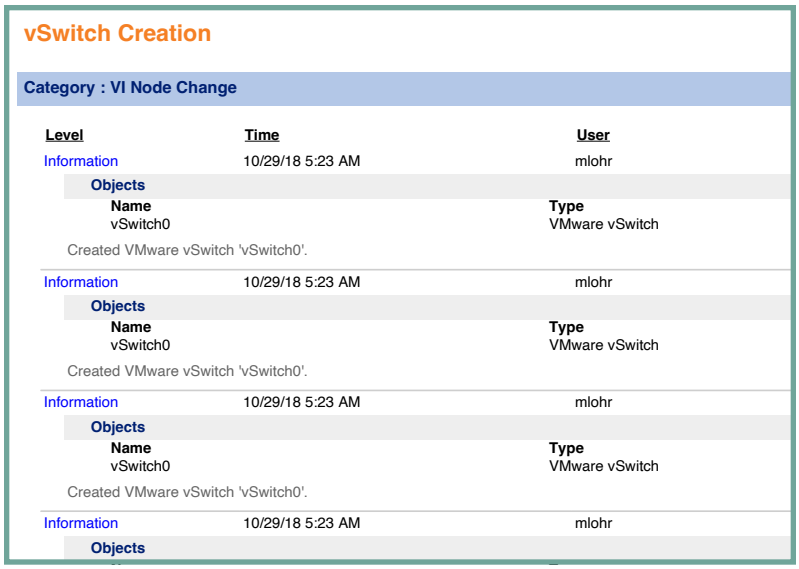
Object Access Controls

Node Group: Critical Cyber Assets

Principal	Role
jwachhaus	Monitor User

System Log

This report identifies Tripwire Enterprise log messages that match specified criteria. This management report is similar to Tripwire Enterprise's log searching capability, but with results in generated report formats. It is normally run on an ad hoc basis.



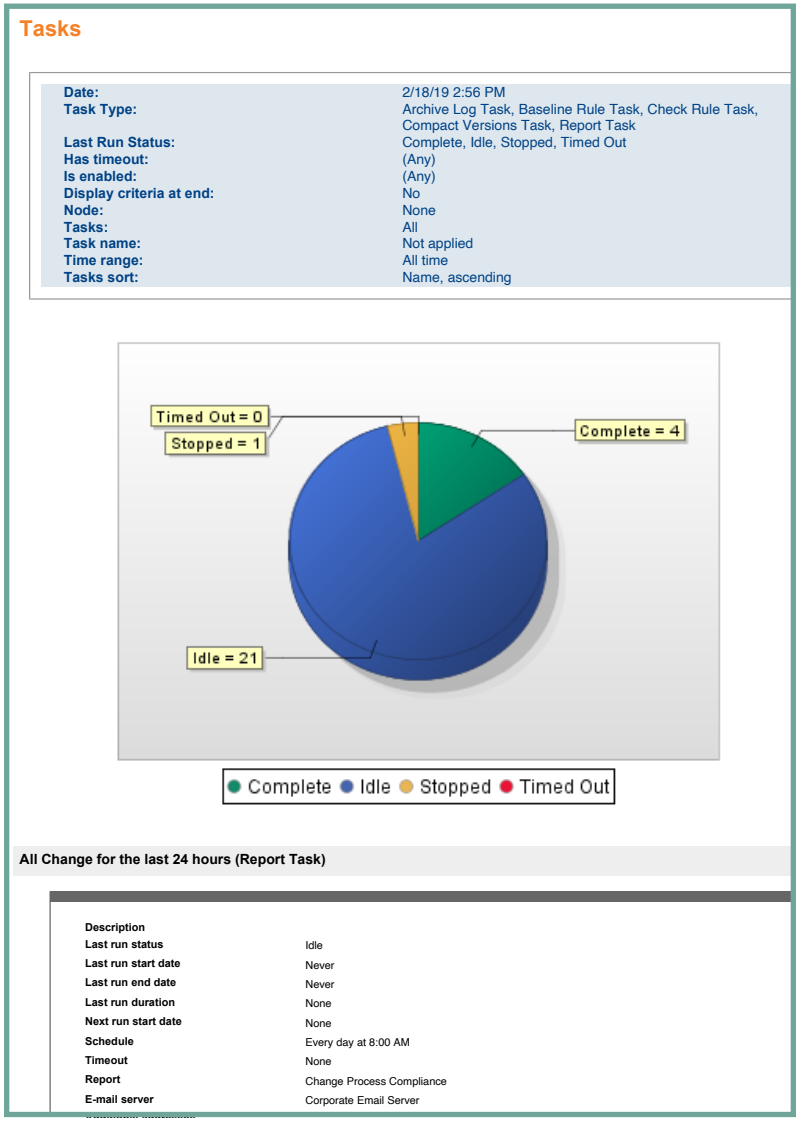
vSwitch Creation

Category : VI Node Change

Level	Time	User
Information	10/29/18 5:23 AM	mlohr
Objects		
Name: vSwitch0		Type: VMware vSwitch
Created VMware vSwitch 'vSwitch0'.		
Information	10/29/18 5:23 AM	mlohr
Objects		
Name: vSwitch0		Type: VMware vSwitch
Created VMware vSwitch 'vSwitch0'.		
Information	10/29/18 5:23 AM	mlohr
Objects		
Name: vSwitch0		Type: VMware vSwitch
Created VMware vSwitch 'vSwitch0'.		
Information	10/29/18 5:23 AM	mlohr
Objects		

Tasks

This report details the state and condition of each of Tripwire Enterprise's scheduled tasks: when tasks were last completed, whether any tasks have stalled or timed out, the parameters for all currently scheduled tasks, etc. This provides quick insight into the workings of the Tripwire Enterprise system.



Tasks

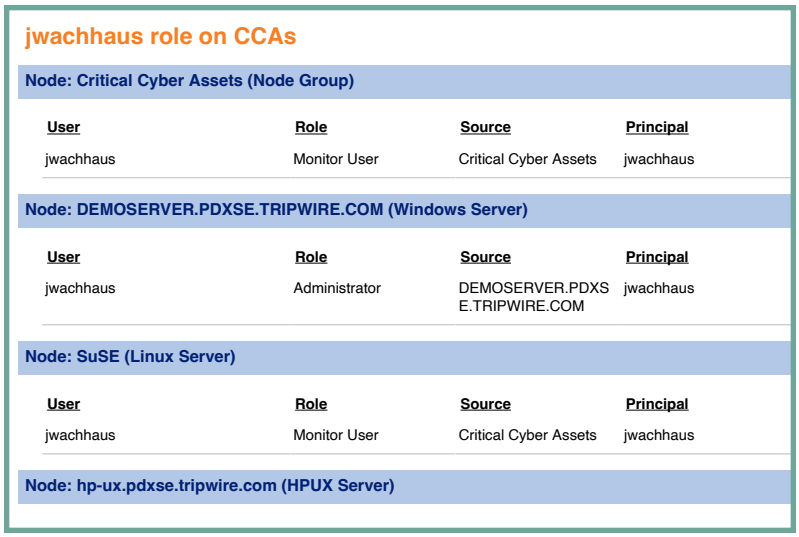
Date:	2/18/19 2:56 PM
Task Type:	Archive Log Task, Baseline Rule Task, Check Rule Task, Compact Versions Task, Report Task
Last Run Status:	Complete, Idle, Stopped, Timed Out
Has timeout:	(Any)
Is enabled:	(Any)
Display criteria at end:	No
Node:	None
Tasks:	All
Task name:	Not applied
Time range:	All time
Tasks sort:	Name, ascending

All Change for the last 24 hours (Report Task)

Description	
Last run status	Idle
Last run start date	Never
Last run end date	Never
Last run duration	None
Next run start date	None
Schedule	Every day at 8:00 AM
Timeout	None
Report	Change Process Compliance
E-mail server	Corporate Email Server

User Roles

For a specified node or node group, this report identifies the effective user role for a selected user account. The effective user role is the actual level of control that the user has over the specified node or node group. This management report shows who has access to what in the Tripwire Enterprise Server, and is typically run monthly, potentially more often depending on process maturity.



jwachhaus role on CCAs

Node: Critical Cyber Assets (Node Group)

User	Role	Source	Principal
jwachhaus	Monitor User	Critical Cyber Assets	jwachhaus

Node: DEMOSERVER.PDXSE.TRIPWIRE.COM (Windows Server)

User	Role	Source	Principal
jwachhaus	Administrator	DEMOSERVER.PDXSE.TRIPWIRE.COM	jwachhaus

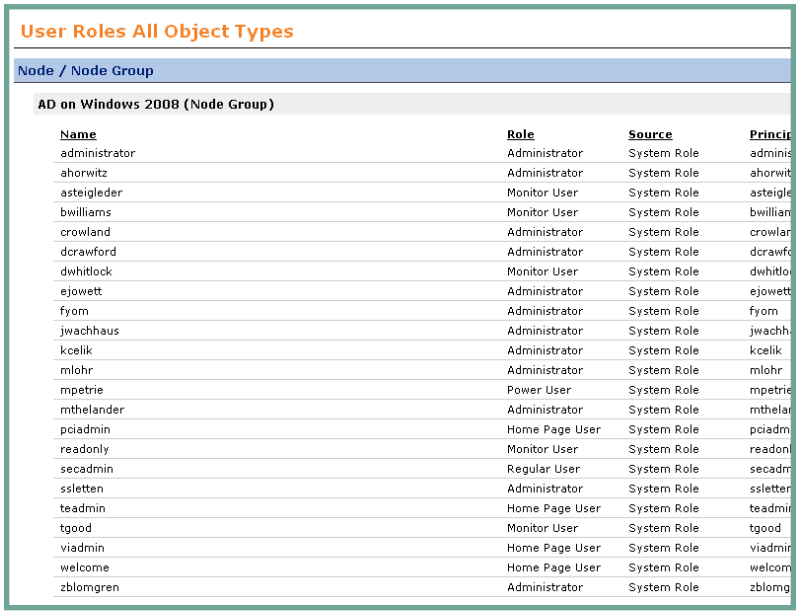
Node: SuSE (Linux Server)

User	Role	Source	Principal
jwachhaus	Monitor User	Critical Cyber Assets	jwachhaus

Node: hp-ux.pdxse.tripwire.com (HPUX Server)

User Roles All Object Types

This report is means of ensuring that proper levels of control have been assigned to existing user accounts. For one or more Tripwire Enterprise objects, it identifies the effective user role for each specified user account.



User Roles All Object Types

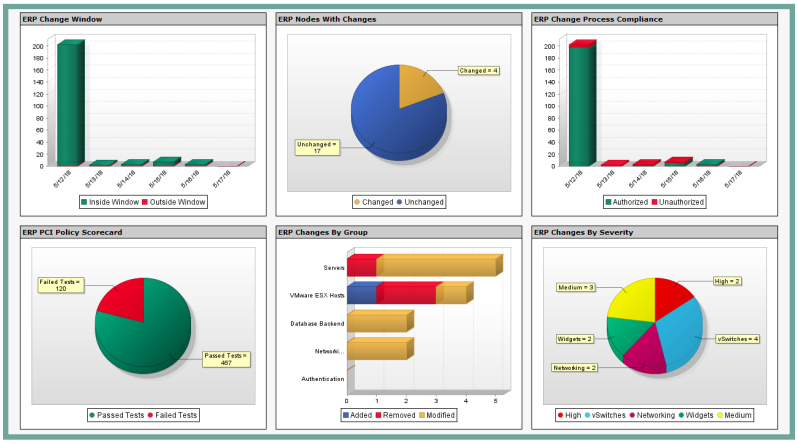
Node / Node Group

AD on Windows 2008 (Node Group)

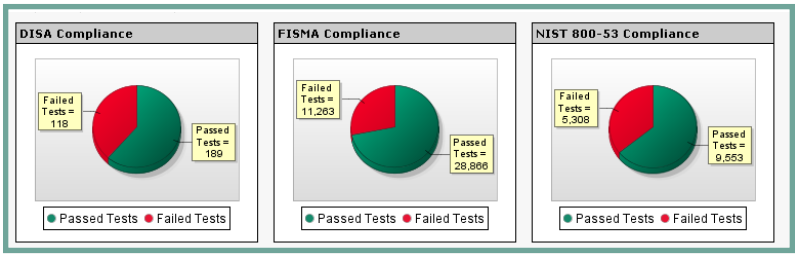
Name	Role	Source	Princip
administrator	Administrator	System Role	adminis
ahorwitz	Administrator	System Role	ahorwit
asteigleder	Monitor User	System Role	asteigle
bwilliams	Monitor User	System Role	bwillian
crowland	Administrator	System Role	crowlar
dcrawford	Administrator	System Role	dcrawfo
dwhitlock	Monitor User	System Role	dwhitlo
ejowett	Administrator	System Role	ejowett
fyom	Administrator	System Role	fyom
jwachhaus	Administrator	System Role	jwachh
kcelik	Administrator	System Role	kcelik
mlohr	Administrator	System Role	mlohr
mpetrie	Power User	System Role	mpetrie
mthelander	Administrator	System Role	mthelar
pciadmin	Home Page User	System Role	pciadm
readonly	Monitor User	System Role	readonl
secadmin	Regular User	System Role	secadm
ssletten	Administrator	System Role	ssletten
teadmin	Home Page User	System Role	teadmi
tgood	Monitor User	System Role	tgood
viadmin	Home Page User	System Role	viadmi
welcome	Home Page User	System Role	welcom
zblomgren	Administrator	System Role	zblomg

Sample Dashboards

Tripwire Enterprise's customizable dashboards provide at-a-glance confirmation of your infrastructure's change and compliance status. When integrated with user homepages, these dashboards allow each user of the system to have a customized display that provides high-level compliance information, fine-grained views of systems or elements, or any level in between.



An enterprise change and compliance dashboard



A federal government compliance dashboard

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.