使用Microsoft WSUS配置ISE版本1.4狀態

目錄

簡介 必要條件 需求 採用元件 設定 網路圖表 Microsoft WSUS **ASA** ISE WSUS的狀況補救 <u>WSUS的終端安全評估要求</u> AnyConnect配置檔案 客戶端調配規則 授權配置檔案 授權規則 驗證 具有更新的GPO策略的PC 批准WSUS上的關鍵更新 檢查WSUS上的PC狀態 已建立VPN會話 狀態模組從ISE接收策略並執行補救 完全網路訪問 疑難排解 重要附註 WSUS補救的選項詳細資訊 Windows更新服務 SCCM整合 相關資訊

簡介

本文檔介紹當思科身份服務引擎(ISE)終端安全評估功能與Microsoft Windows Server Update Services(WSUS)整合時,如何對其進行配置。

附註:當您訪問網路時,您將重定向到ISE for Cisco AnyConnect Security Mobility Client Version 4.1 provisioning with a posture module,該模組會檢查WSUS上的合規性狀態並安裝 必要的更新,以使工作站合規。一旦將站點報告為符合要求,ISE允許完全網路訪問。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco ISE部署、身份驗證和授權
- 有關ISE和Cisco AnyConnect狀態代理運行方式的基本知識
- •思科自適應安全裝置(ASA)的配置
- •基本VPN和802.1x知識
- Microsoft WSUS的配置

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Microsoft Windows版本7
- Microsoft Windows版本2012(WSUS版本6.3)
- Cisco ASA 9.3.1及更高版本
- Cisco ISE軟體版本1.3及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

本節介紹如何配置ISE和相關網路元素。

網路圖表

以下拓撲用於本文檔中的示例:



以下是流量傳輸,如網路圖所示:

- 1. 遠端使用者通過Cisco AnyConnect連線,以通過VPN訪問ASA。這可以是任何型別的整合存 取,例如終止於交換器上的802.1x/MAC驗證略過(MAB)有線作業階段,或終止於無線LAN控 制器(WLC)上的無線作業階段。
- 作為身份驗證過程的一部分,ISE確認終端站的狀態不等於相容(ASA-VPN_quarantine授權規則),並且重定向屬性在Radius Access-Accept消息中返回。因此,ASA會將所有HTTP流量重定向到ISE。
- 使用者開啟Web瀏覽器並輸入任何地址。重定向到ISE後,站點上會安裝Cisco AnyConnect 4狀態模組。安全評估模組隨後從ISE下載策略(WSUS要求)。
- 4. 狀態模組搜尋Microsoft WSUS並執行補救。
- 5. 成功修復後,狀態模組向ISE傳送報告。
- 6. ISE發出Radius授權更改(CoA),為合規的VPN使用者(ASA-VPN_compliant authorization rule)提供完全網路訪問。

附註:要使補救起作用(能夠在PC上安裝Microsoft Windows更新),使用者應具有本地管理 許可權。

Microsoft WSUS

附註:WSUS的詳細配置不在本檔案的範圍之內。有關詳細資訊,請參閱<u>組織Microsoft文檔中</u> <u>的「部署Windows Server</u>更新服務」。

WSUS服務通過標準TCP埠8530進行部署。請務必記住,為了補救,還使用其他埠。因此,將WSUS的IP位址安全地新增到ASA上的重新導向存取控制清單(ACL)中(稍後詳述於本檔案中)。

U _1		Internet Infor	mation Se	ervices (IIS) Ma	anager	
	 WSUS Adr 	ministration 🕨				
File View Help						
Connections	<u>مر</u>	CUC Admini	stration	Homo		
🗟 - 🗟 🖄 🎭	S AA	SUS Admini	stration	Home		
Start Page	Filter:		🛒 Go 🕞 🐺	Show All Grou	up by: Area	- 📰 -
2 Application Pools			Si	te Bindings		? X
⊿ 🙆 Sites						
⊿ erault web site	Туре	Host Name	Port	IP Address	Binding	Add
4 😜 WSUS Administration	http		8530 8531			Edit
▷-()* ApiRemoting30 ▷-(3*) ClientWebService						
Content						Remove
⊳-@ DssAuthWebService						Browse
▷-; ReportingWebService						
þ 🔝 Selfupdate						
▷-@* ServerSyncWebService						
, C. and						
	<		Ш		>	
						Close
						ciose

域的組策略已針對Microsoft Windows更新進行配置,並指向本地WSUS伺服器:

<u>s</u>	Group Policy M	Aanagement Editor 📃 🗕
File Action View Help		
🗢 🏓 📶 🗟 📓 🕅 🝸 👘	🎐 Specify i	intranet Microsoft update service location 📃 🗖 🗙
Security Center A Server for NIS Shutdown Options	🔚 Specify intranet Microsoft update servi	Previous Setting Next Setting
Smart Card Sound Recorder Sync your settings	Not Configured Comment: Enabled	<u>^</u>
▷ Tablet PC ○ Task Scheduler ○ Windows Calendar	ं Disabled Supported on: विव हर	t least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, Automatic Service Service Pack 3, Automatic Service Ser
 Windows Color System Windows Customer E Windows Defender Windows Error Report 	Options:	Help:
 Windows Installer Windows Logon Opti Windows Mail 	Set the intranet update service for detecting updates:	g Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.
🧰 Windows Media Cent 🎬 Windows Media Digit 🛅 Windows Media Plays	Set the intranet statistics serven http://172.16.31.103:8530	This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.
 Windows Messenger Windows Mobility Ce Windows PowerShell Windows Reliability A Windows Remote Ma Windows Remote She 	(example: http://intranetUpd01)	To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.
Windows Update Work Folders Workplace Join Workplace Join All Settings Preferences Workplace Join		If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying
P Colorign data Policies P Colorign data P Preferences		OK Cancel Apply

以下是針對基於不同嚴重性級別的精細策略啟用的建議更新:

💛 Windows Update		
Turn on recommended updates via	Setting	State
Automatic Updates	🗈 Do not display 'Install Updates and Shut Down' option in Sh	Not configured
	📰 Do not adjust default option to 'Install Updates and Shut Do	Not configured
Edit policy setting	📰 Enabling Windows Update Power Management to automati	Not configured
Requirements:	Always automatically restart at the scheduled time	Not configured
At least Windows Vista	📰 Configure Automatic Updates	Enabled
Description: Specifies whether Automatic Updates will deliver both important as well as recommended updates from the Windows Update update service.	📰 Specify intranet Microsoft update service location	Enabled
	Automatic Updates detection frequency	Enabled
	📰 Do not connect to any Windows Update Internet locations	Not configured
	Allow non-administrators to receive update notifications	Not configured
	Turn on Software Notifications	Not configured
When this policy is enabled.	🗄 Allow Automatic Updates immediate installation	Not configured
Automatic Updates will install	📰 Turn on recommended updates via Automatic Updates 👘 👘	Enabled
recommended updates as well as	📰 No auto-restart with logged on users for scheduled automat	Not configured
important updates from Windows	📰 Re-prompt for restart with scheduled installations	Not configured
Update update service.	Delay Restart for scheduled installations	Not configured
When disabled or not configured	📰 Reschedule Automatic Updates scheduled installations	Not configured
Automatic Updates will continue to	📰 Enable client-side targeting	Enabled
deliver important updates if it is already configured to do so.	🖹 Allow signed updates from an intranet Microsoft update ser	Not configured

ASA

遠端使用者採用簡單的安全套接字層(SSL)VPN訪問(其詳細資訊不在本文檔的討論範圍之內)。

以下是組態範例:

```
interface GigabitEthernet0/0
nameif outside
security-level 10
ip address 172.16.32.100 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 172.16.31.100 255.255.255.0
aaa-server ISE protocol radius
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
key cisco
webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable
error-recovery disable
group-policy POLICY internal
group-policy POLICY attributes
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
tunnel-group SSLVPN type remote-access
tunnel-group SSLVPN general-attributes
address-pool POOL-VPN
authentication-server-group ISE
accounting-server-group ISE
default-group-policy POLICY
ip local pool POOL-VPN 172.16.50.50-172.16.50.60 mask 255.255.255.0
在ASA上配置訪問清單非常重要,該清單用於確定應重定向到ISE的流量(針對尚未合規的使用者
) :
```

access-list Posture-redirect extended deny udp any any eq domain access-list Posture-redirect extended deny ip any host 172.16.31.103 access-list Posture-redirect extended deny ip any host 172.16.31.202 access-list Posture-redirect extended deny icmp any any access-list Posture-redirect extended permit tcp any any eq www 非合規使用者只允許域名系統(DNS)、ISE、WSUS和網際網路控制消息協定(ICMP)流量。所有其他 流量(HTTP)重定向到ISE進行AnyConnect 4調配,該調配負責狀態和補救。

ISE

附註:AnyConnect 4調配和狀態超出本文檔的範圍。請參閱<u>AnyConnect 4.0與ISE版本1.3整</u> <u>合配置示例</u>,瞭解更多詳細資訊,例如如何將ASA配置為網路裝置並安裝Cisco AnyConnect 7應用。

WSUS的狀況補救

完成以下步驟,以便為WSUS配置狀態補救:

- 1. 導航到Policy > Conditions > Posture > Remediation Actions > Windows Server Update Services Remediation以建立新規則。
- 2. 驗證「*Microsoft Windows Updates*」設定是否設定為「嚴重性**級別」**。此部分負責檢測補救 過程是否啟動。

然後,Microsoft Windows Update Agent連線到WSUS,並檢查該PC是否有任何*Critical*更新等待安裝:

Authentication 🧕 Authorization	🛃 Profiling	Posture	Client Provisioning	🚊 TrustSec 🛛 🔒 Polic
Dictionaries Conditions Results				
Results	₽	Windows Server Up Windows Server Validate Wind Windows Updates In Installation Wiza Save Reset	date Services Remediations I er Update Services Re * Name WSUS-Ren Description Remediation Type Automatii Interval 0 Retry Count 0 ows updates using Cisco R ates Severity Level Critical Update stallation Source Microso rd Interface Setting Show U	ist > WSUS-Remediation mediation c c v ules Severity Level v to latest OS Service Pack R Server Managed Server I O No UI

WSUS的終端安全評估要求

導航到Policy > Conditions > Posture > Requirements以建立新規則。規則使用名為*pr_WSURule*的 虛設條件,這意味著在需要補救時,將聯絡WSUS以檢查條件(*關鍵更*新)。

滿足此條件後,WSUS將安裝已為該電腦配置的更新。這些更新可能包括任何型別的更新,也可能 包括嚴重性級別較低的更新:

Requirements

Name	Operating Systems	Conditions	Remediation Actions
Any_AS_Definition_Mac	for Mac OSX met	f ANY_as_mac_def els	 AnyASDefRemediationM ac
Any_AV_Installation_Win	for Windows All met	f ANY_av_win_inst els	e Message Text Only
Any_AV_Definition_Win	for Windows All met	f ANY_av_win_def els	 AnyAVDefRemediationWi n
Any_AS_Installation_Win	for Windows All met	f ANY_as_win_inst els	e Message Text Only
Any_AS_Definition_Win	for Windows All met	f ANY_as_win_def els	e AnyASDefRemediationWi n
Any_AV_Installation_Mac	for Mac OSX met	f ANY_av_mac_inst els	 Message Text Only
Any_AV_Definition_Mac	for MacOSX met	f ANY_av_mac_def els	AnyAVDefRemediationM ac
Any_AS_Installation_Mac	for Mac OSX met	f ANY_as_mac_inst els	e Message Text Only
WSUS	for Windows All met	f pr_WSUSRule els	WSUS-Remediation

AnyConnect配置檔案

配置終端安全評估模組配置檔案以及AnyConnect 4配置檔案(如<u>AnyConnect 4.0與ISE版本1.3整合</u> <u>配置示例中所述</u>):

ዿ Authentication 🛛 🧔 Authorization	Received Profiling Posture Dig Client Provision	ioning 🚊 TrustSec 🔥 Policy Elements
Dictionaries Conditions Results		
Results	AnyConnect Configuration > AnyConnect Con	hguration
	* Select AnyConnect Package:	AnyConnectDesktopWindows 4.1.2011.0 *
 Profiling 	* Configuration Name:	AnyConnect Configuration
Posture Clent Provisioning E Resources TrustSec	Description:	
	Description	Value
	* Compliance Module	AnyConnectComplianceModuleWindows 3.6.5*
	AnyConnect Module Selection	
	ISE Posture	v/
	VPN	\checkmark
	Network Access Manager	
	Web Security	
	AMP Enabler	
	ASA Posture	
	Start Before Logon	
	Diagnostic and Reporting Tool	
	Profile Selection	
	* ISE Posture	AC4 profile 🔹
	VPN	

客戶端調配規則

AnyConnect配置檔案準備就緒後,可從客戶端調配策*略中引*用它:

ciso	1. O Ide	entity Services Engine			<u>ن</u> ک	fome Operations •	Poli	cy 🛛 🔻 Guest Access 🗍	Administration	
	Authentic	cation 🧕 Authorization	[🔨 Profiling	💽 Posl	ure 🛛 🔂 Client Pro	visionin	TrustSec	4 Policy Elements	
Chien Define For Age For Nat	t Prov the Clien ent Confi ive Supp	Isioning Policy It Provisioning Policy to determine guration: version of agent, agent, slicant Configuration: wizard profi	e wha profile le and	d users will receive e, agent compliant d/or wizard. Drag a	e upon k se modul and drop	igin and user session init e, and/or agent customiz rules to change the orde	iation: ation pao r.	:kage.		
		Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
21 21 22 22 22 22 22 22 22 22 22 22 22 2	2	AC4	lŕ	Any	and	Windows All	and	Condition(s)	then	AnyConnect Configuration

整個應用程式以及配置都安裝在終端上,該終端重定向到「客戶端調配」門戶頁面。AnyConnect 4可能會升級,並安裝額外的模組(狀態)。

授權配置檔案

建立用於重定向到客戶端調配配置檔案的授權配置檔案:

Authentication S Authorization	🔀 Profiling 😿 Posture 🔯 Client Provisioning 📄 TrustSec 💦 Policy Elements
Dictionaries Conditions Results	
Results	Authorization Profiles > Posture * Name Posture Description
Clent Provisioning TructSec	✓ Common Tasks
· //485300	VLAN VLAN Voice Domain Permission
	Web Redirection (CWA, MDM, NSP, CPP)
	Client Provisioning (Posture) * ACL Posture-redirect Value Client Provisioning Portal *

授權規則

此圖顯示授權規則:

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First	t Matcheo	l Rule Applies 🔹				
►E	xception	; (0)				
St	andard					
	Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
i		ASA-VPN_quarantine	if	(Session:PostureStatus EQUALS Unknown OR Session:PostureStatus EQUALS NonCompliant)	then	Posture
11		ASA-VPN compliant	if	Session:PostureStatus EQUALS Compliant	then	PermitAccess

首次使用ASA-VPN_quarantine規則。因此,將返回Posture授權配置檔案,並將終端重定向到 AnyConnect 4的客戶端調配門戶(使用狀態模組)調配。

一旦符合,將使用ASA-VPN_compliant規則,並允許完全網路訪問。

驗證

本節提供的資訊可用於驗證組態是否正常運作。

具有更新的GPO策略的PC

PC登入到域後,應推送WSUS配置的域策略。這可能在VPN會話建立(帶外)之前或之後發生,如 果使用*Start Before Logon*功能(它也可以用於802.1x有線/無線接入)。 一旦Microsoft Windows客戶端配置正確,可從Windows Update設定反映此問題:

When your computer is online, Windows can automatically check for important updates and using these settings. When new updates are available, you can also install them before shuttir computer. How does automatic updating help me? Important updates	install them 1g down the
Important updates	
Devente and supplementations have been as subjects as to install the sur-	
Install new updates: Every day at 9:00 AM	
Recommended updates	
Give me recommended updates the same way I receive important updates	

如果需要,可以使用組策略對象(GPO)刷新和Microsoft Windows Update代理伺服器發現:

C:\Users\Administrator>**gpupdate /force** Updating Policy...

User Policy update has completed successfully. Computer Policy update has completed successfully.

C:\Users\Administrator>wuauclt.exe /detectnow

C:\Users\Administrator>

批准WSUS上的關鍵更新

批准流程可從以下客戶端站點目標中獲益:



如果需要,使用waucrt重新傳送報告。

檢查WSUS上的PC狀態

此圖顯示如何檢查WSUS上的PC狀態:

藏		Update S	Services	
📷 File Action View Window	/ Help			
🗢 🔿 🙎 📰 🚺				
📷 Update Services	All Computers (1 computers	of 2 shown, 2 total)		
⊿ 📷 WIN-LT802K5CFQU ⊿ 👼 Updates	Status: Any	🝷 📿 Refresh	1	
🗐 All Updates	① Name	IP Address	Operating System	Insta Last Status Report
Security Undetes	🔺 admin-pc.example.com	192.168.10.21	Windows 7 Profes	99% 6/27/2015 12:41 AM
 WSUS Updates Computers All Computers Unassigned Comp Computer-Updat Downstream Servers Synchronizations Reports Options 				
	admin-pc.example.com			
	Status Updates with e Updates neede Updates install Updates with r	errors: ed: led/not applicable: 1 no status:	Group me 0 1 035 0	embership: All Computer s, Unassigne d Computer

應安裝一個更新,以便下次使用WSUS刷新。

已建立VPN會話

建立VPN會話後,使用*ASA-VPN_quarantine* ISE授權規則,該規則返回*Posture授*權配置檔案。因 此,來自終端的HTTP流量將重定向以進行AnyConnect 4更新和狀態模組調配:



此時,ASA上的會話狀態表示通過HTTP流量重定向到ISE來限制訪問:

asav# show vpn-sessiondb detail anyconnect Session Type: AnyConnect Detailed Username : cisco Index : 69 Assigned IP : 172.16.50.50 Public IP : 192.168.10.21 <...some output omitted for clarity...> ISE Posture: Redirect URL : https://ise14.example.com:8443/portal/gateway?sessionId=ac101f64000

```
45000556b6a3b&portal=283258a0-e96e-...
Redirect ACL : Posture-redirec
```

狀態模組從ISE接收策略並執行補救

狀態模組從ISE接收策略。ise-psc.log調試顯示傳送到終端安全評估模組的需求:

```
2015-06-05 07:33:40,493 DEBUG [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1:::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
  <version>2</version>
  <encryption>0</encryption>
  <package>
        <id>>10</id>
```

<version/> <description>This endpoint has failed check for any AS installation</description> <type>10</type> <optional>0</optional>

```
<remediation_type>l</remediation_type>
<remediation_retry>0</remediation_retry>
<remediation_delay>0</remediation_delay>
<action>l0</action>
<check>
```

</check> <criteria/> </package> </cleanmachines>

安全狀態模組會自動觸發Microsoft Windows Update代理連線到WSUS並下載在WSUS策略中配置 的更新(所有更新均自動執行,無需任何使用者干預):

G v Control Panel > System and Security > Win	dows Update	- 4 €	Search Control Panel 🔎
MAC Agent WSUS Update The updates are being installed		×	0
Installation status: Initializing installation done! Installing Security Update for Windows 7 for x64-based Systems (K	B3000483) (update 1 of	*	computer.
1)		Ŧ	. View update history em administrator :es from Windows Update
Installing:			pility Client 🗖 🖾 🔀
	Ca	ncel	VPN-ASA.
See also Installed Updates	Updat	em Scan: ing require	Details ment 1 of 1. 30% Cancel
🍕 Windows Anytime Upgrade	\$ ()		aljuaju. cisco

附註:某些更新可能需要重新啟動系統。

G v Control Panel > System and Security > Win	dows Update 👻 👻	Search Control Panel
🖑 NAC Agent WSUS Update		× 0
You must restart your computer for the updates to take effe	ct.	computer. View update history em administrator res from Windows Update
	Restart Now Close	VPN-ASA. Disconnect IPv4
See also Installed Updates Windows Anytime Upgrade	System Se Updating res	can: Details quirement 1 of 1. 30% Cancel
	\$ ()	ofinite cisco

完全網路訪問

在AnyConnect終端安全評估模組將工作站報告為合規後,您將看到以下內容:

Control Panel +	System and Security 🕨 Windows Update 🗸 😽 Search Control Panel 🔎
Control Panel Home	Windows Update
Change settings View update history Restore hidden updates	Windows is up to date There are no updates available for your computer.
Updates: frequently asked questions	Most recent check for updates: Today at 3:10 PM Updates were installed: 6/25/2015 at 11:59 AM. View update history You receive updates: Managed by your system administrator Check online for updates from Windows Update
	Cisco AnyConnect Secure Mobility Client
See also Installed Updates & Windows Anytime Upgrade	System Scan: Complant. Network access allowed.

報告傳送到ISE,ISE重新評估策略並達到*ASA-VPN_compliant授*權規則。這樣可提供完整的網路訪 問(通過Radius CoA)。 導覽至**Operations > Authentications**以確認這點:

cisco Identity Ser	vices Engine			Guest Access	Administration 🔻
Authentications	Reports	Adaptive Network C	antrol 🔪 Traubleshoot		
Misconfi	gured Supplica	nts 🕐	Misconfigured Network Device	s ®	RADIUS Drops (i)
	0		0		0
🗂 Show Live Sessions	🙀 Add or Ren	nove Columns 👻 🍪 Refre	sh 💿 Reset Repeat Counts		
Time	Status	Repeat C Identity	Authorization Policy (1)	Authorization Profiles	Event 🕐
	All T	1 Vicipation 64 C 10000			
2015-06-05 11:13:13	· 🗹 🔒			PermitAccess	Dynamic Authorization succeeded
2015-06-05 11:13:11	. 🕕 🔒	0 cisco			Session State is Postured
2015-06-05 11:11:33	. 🗹 🛛 🚡	cisco	Default >> ASA-VPN_quarantine	Posture	Authentication succeeded

調試(ise-psc.log)還確認合規狀態、CoA觸發器和終端安全評估的最終設定:

DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureManager -:cisco: ac101f6400039000556b4200:::- Posture report token for endpoint mac 08-00-27-DA-EF-AD is Healthy DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco: ac101f6400039000556b4200:::- entering triggerPostureCoA for session ac101f6400039000556b4200 DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco:ac 101f6400039000556b4200:::- Posture CoA is scheduled for session id

[ac101f6400039000556b4200]

DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco: ac101f6400039000556b4200:::- DM_PKG report non-AUP:html = <!--X-Perfigo-DM-Error=0--> <!--error=0--><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--> <!--X-Perfigo-Auto-Close-Login-Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--> <!--user role=--><!--X-Perfigo-OrigRole=--><!--X-Perfigo-UserKey=dummykey--> <!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-Perfigo-Session=--> <!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter--> <!--X-Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4--> <!--X-Perfigo-DHCP-Renew-Delay=1--><!--X-Perfigo-Client-MAC=08:00:27:DA:EF:AD-->

DEBUG [pool-183-thread-1][]cisco.cpm.posture.runtime.PostureCoA -:cisco: ac101f6400036000556b3f52:::- Posture CoA is triggered for endpoint [08-00-27-da-ef-ad] with session [ac101f6400039000556b4200] 此外,ISE詳細狀態評估報告確認該站點符合以下要求:

Posture More Detail Assessment

Time Range: From 05/30/2015 12:00:00 AM to 06/05/2015 11:59:59 PM Generated At: 2015-06-05 20:09:00.047

Client Details

Username:	cisco
Mac Address:	08:00:27:DA:EF:AD
IP address:	172.16.50.50
Session ID:	ac101f6400036000556b3f52
Client Operating System:	Windows 7 Professional 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.1.02011
PRA Enforcement:	0
CoA:	Received a posture report from an endpoint
PRA Grace Time:	0
PRA Interval:	0
PRA Action:	N/A
User Agreement Status:	NotEnabled
System Name:	ADMIN-PC
System Domain:	example.com
System User:	Administrator
User Domain:	EXAMPLE
AV Installed:	ClamWin Free Antivirus; 0.98.5; 55.20615; 06/26/2015;
AS Installed:	Windows Defender; 6.1.7600.16385; 1.201.171.0; 06/26/2015;

Posture Report

Posture Status:	Compliant
Logged At:	2015-06-05 07:28:49.194

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed Conditions
WSUS	WSUS	Mandatory			Missing windows updates: 0

附註:由於ACIDEX擴展,已知Microsoft Windows PC上物理網路介面的準確介質訪問控制 (MAC)地址。

疑難排解

目前尚無適用於此組態的疑難排解資訊。

重要附註

本節提供有關本檔案中所述組態的一些重要資訊。

WSUS補救的選項詳細資訊

區分需求條件和補救措施非常重要。AnyConnect觸發Microsoft Windows Update代理檢查符合性 ,具體取決於*Validate Windows updates using* remediation設定。

Windows Server Update Server	rices Remediation	
* Name	WSUS-Remediation (i)	
Description		
Remediation Type	Automatic 🔹	
Interval	0	(in secs) (Valid Range 0 to 9999)
Retry Count	0	(Valid Range 0 to 99)
Validate Windows updates using	🔵 Cisco Rules 💿 Severity Level	
Windows Updates Severity Level	Medium -	
Mindows Undetex Installation Course		
windows Opdates installation Source	Microsoft Server 🕑 Managed Server	
Installation Wizard Interface Setting	💿 Show UI 🔘 No UI	

在本例中,使用*Severity Level*。使用*Critical*設定,Microsoft Windows代理將檢查是否存在任何掛 起(未安裝)的重要更新。如果存在,則補救開始。

然後,補救過程可能根據WSUS配置安裝所有重要和不太重要的更新(針對特定電腦批准的更新)。

通過使用*使用***Cisco Rules**設定驗證Windows更新,該要求中詳細列出的條件將決定該工作站是否合 規。

Windows更新服務

對於不帶WSUS伺服器的部署,可以使用另一種稱為Windows Update Remediation的補救型別:

Windows Update	Remediations Lis	st > New	Windows	Update	Remediation
----------------	------------------	----------	---------	--------	-------------

Windows Update Remediation				
* Name	WindowsUpdate			
Description				
Remediation Type	Automatic •			
Interval	0	(in secs) (Valid Range 0 to 9999)		
Retry Count	0	(Valid Range 0 to 99)		
Windows Update Setting	Automatically do 🔻			
Override User's Windows Update setting with administrator's				

此補救型別允許控制Microsoft Windows Update設定並允許您執行即時更新。用於此補救型別的典型條件是*pc_AutoUpdateCheck*。這允許您檢查終結點上是否啟用了Microsoft Windows Update設定。否則,您可以啟用它並執行更新。

SCCM整合

ISE版本1.4的新功能patch management允許與許多第三方供應商整合。視供應商而定,條件和補救 都有多個可用選項。

對於Microsoft,同時支援System Management Server(SMS)和System Center Configuration Manager(SCCM)。

相關資訊

- 思科ISE配置指南上的終端安全評估服務
- 思科身份服務引擎管理員指南,版本1.4
- 思科身份服務引擎管理員指南,版本1.3
- 在組織中部署Windows Server Update服務
- 技術支援與文件 Cisco Systems