採用Novell客戶端身份驗證的思科安全服務客戶端 配置示例

目錄

<u>簡介</u> <u>背景資訊</u> <u>採用元件</u> <u>支援的功能</u> <u>不支援的功能</u> <u>安裝說明</u> <u>慣例</u> <u>Novell無上下文和無樹登入</u> <u>使用Novell客戶端的思科安全服務客戶端身份驗證</u> <u>思科安全服務客戶端配置</u> 相關資訊

<u>簡介</u>

本文檔提供了如何在Windows 2000和Windows XP上使用Novell客戶端為Cisco安全服務客戶端配置 身份驗證的示例。

<u>背景資訊</u>

<u>採用元件</u>

本節列出本文中所用的軟體版本。

- 思科安全服務使用者端版本4.0可從<u>Cisco.com Software Center</u>(僅限註冊客戶)下載Cisco Secure Services Client。
- Novell客戶端版本4.91 SP1(帶修補程式TID2972711)註:為了確保Novell Client的4.91 SP1版本與SSC應用程式相容,必須下載並安裝修補程式工具包。有關修補程式套件的詳細資訊,請參閱<u>Novell Client Post-4.91 SP1修補程式套件「A」 TID2973054</u>。
- Novell Server 6.0 SP5或更高版本

<u>支援的功能</u>

本節列出本檔案支援的功能。

- Novell客戶端正常登入(指定了上下文和樹)
- Novell客戶端LDAP無上下文登入

<u>不支援的功能</u>

本節列出本檔案不支援的功能。

- Novell客戶端無樹登入
- Novell客戶端DSCAT無上下文登入

安裝說明

您可以在安裝思科安全服務客戶端之前或之後安裝Novell客戶端。但是,如果從電腦中刪除Novell Client然後重新安裝,則必須刪除Cisco Secure Services Client,重新啟動電腦,然後重新安裝 Cisco Secure Services Client。此過程對於思科安全服務客戶端設定相應的登錄檔值是必需的。

<u>慣例</u>

如需檔案慣例的詳細資訊,請參閱<u>思科技術提示慣例</u>。

<u>Novell無上下文和無樹登入</u>

在Novell網路中,身份驗證需要使用者名稱和密碼,以及使用者所屬的Novell目錄樹和上下文。當對 樹或上下文結構進行更改時,使用者需要在「新穎登入」對話方塊中更改其上下文資訊。此過程會 導致IT成本增加,以便管理和支援更改。

較大的Novell客戶使用LDAP無上下文登入,允許將多個樹合併到一個全域性樹中。無上下文登入不 要求使用者管理對其上下文或目錄層次結構中的位置的更改。可在後端更改上下文,而無需與管理 和支援這些更改相關的高成本。

除了無上下文登入外,Novell客戶端還支援無樹登入。使用無樹登入,使用者無需指定其所屬的 Novell目錄樹。這以相同的方式促進使用者在不同樹之間的移動,無上下文允許使用者在上下文之 間的移動對使用者是透明的。

使用Novell客戶端的思科安全服務客戶端身份驗證

當您通過單點登入(SSO)使用思科安全服務客戶端登入前連線功能時,使用者可以通過無情登入登入到Novell網路。但是,使用者必須輸入其樹和伺服器資訊。要獲得完整功能,系統必須配置單獨的身份驗證過程,該過程使用Cisco安全服務客戶端電腦身份驗證或Cisco安全服務客戶端上的登入前身份驗證,後者提示使用者輸入其IEEE 802.1X憑證。當您將802.1X與Novell環境的無上下文功能結合使用時,Cisco Secure Services Client將承擔上下文查詢功能;因此,Novell客戶端的配置方式可能會影響Cisco安全服務客戶端連線到網路所需的時間。

注意:當使用者在Novell登入過程中指定上下文時,Novell客戶端中不需要任何特殊設定。

預設情況下,Novell客戶端儲存上次成功登入的資訊。您可以配置登入欄位以顯示部分或不顯示預 設值。也就是說,出於安全原因,可以將欄位留空,也可以使用預設值填充這些欄位以方便使用。

注意:使用無上下文登入時,情景不會顯示在Novell Login對話方塊中,因為在使用者輸入其使用者 名稱和密碼並且Cisco安全服務客戶端已經通過網路驗證之前,情景查詢被抑制。

思科安全服務客戶端使用Novell客戶端中配置的資訊執行上下文查詢。您必須配置Novell客戶端以向

Novell網路進行身份驗證,就像始終指定上下文一樣。如果上下文查詢是從以前的成功登入中儲存 的,則思科安全服務客戶端所需的登入時間最多可縮短一分鐘。

注意:如果將Novell Client配置為儲存配置檔案以及使用者更改的上下文,則必須從Novell Client登 入螢幕中刪除它,以強制思科安全服務客戶端執行上下文查詢。

當上下文儲存在公共機器或具有多個使用者、需要不同上下文的機器上時,安全性會受到危害。為 確保安全性不受影響,您可以禁用儲存使用者配置檔案的Novell客戶端預設設定。

要禁用Novell客戶端預設設定以儲存使用者配置檔案,請完成以下步驟:

- 1. 按一下右鍵Novell系統托盤圖示,然後選擇屬性。
- 2. 按一下Location Profiles頁籤。
- 3. 選擇預設配置檔案,然後按一下Properties按鈕。
- 4. 從下拉選單中選擇Login Service。
- 5. 驗證服務例項是否設定為預設值,然後按一下Properties頁籤。系統將顯示Novell Login對話方 塊的樣例。各個頁籤控制對對話方塊功能區域的訪問。例如,「身份證明」頁籤僅包含「使用 者名稱」欄位。不允許密碼欄位包含預設值。
- 6. 取消選中位於頁籤上方的Save profile after successful login覈取方塊。註:如果希望「使用者 名稱」欄位的內容顯示為空白,請刪除該欄位的內容
- 7. 按一下NDS頁籤,然後選中Active Authenticator覈取方塊。
- 8. 從下拉選單中,為樹、上下文和伺服器選擇所需的選項。思科安全服務客戶端使用這些值來查 詢上下文資訊。通常,您可以為無情登入配置樹和伺服器,或者配置所有三個欄位(如果您知 道上下文)。如果您希望該欄位顯示為空白,則必須從下拉選單選擇空白欄位。不能在欄位內 容上退格。
- 9. 按一下**LDAP Contexless Login**頁籤,並驗證Enable LDAP Treless Login和Enable LDAP Contexless Login覈取方塊是否未選中。

Novell Client Configuration	? ×	
DSCAT Contextless Login	Update Agent	
Default Capture Proto	col Preferences	
Service Location Advanced Settings Ad	vanced Menu Settings	
Client Location Profiles	Advanced Login	
LDAF Contextiess Login Single Sign-on	DHCP Settings	
Enable LDAP Treeless Login		
Enable LDAP Contextless Login		
Enable LUAP Context Search Scope		
MTG	Add 1	
MIG	And	
	Delete	
	Properties	
Servers		
	Add	
192.168.1.60	Delete	
	Properties	
	1 ispongeen.	
	UB Down	
Settings		
OK Cancel		

:由於LDAP無上下文登入在Novell客戶端中禁用且通過Cisco Secure Services客戶端受支援

,因此無法單獨設定此映像中顯示的各個引數。

LDAP Contextless Login Settings		? ×
Settings		
Parameters: Alow Wildcards in Searches Display Context Display E-mail Address Display Full Name Display Given Name Display Sumame Display Sumame Display Telephone Number Display Unique ID Search on E-mail Address Search on Full Name Search on Given Name	<u>S</u> etting: Off	
Description Set this value to On to allow wildcard so the search attributes in LDAP Services	earches for a during login	any of 🔺
	ОК	Cancel

10. 按一下**DSCAT Contexless Login**頁籤,並驗證是否未選中Enable覈取方塊。

Novell Client Configuration ? 🗙			
Default Capture	Protocol Preferences		
Service Location Advanced Settings	Advanced Menu Settings		
Client Location Profiles	Advanced Login		
LDAP Contextless Login Single S	ign-on DHCP Settings		
DSCAT Contextless Login	Update Agent		
Enable			
■ Wildcard Searching Allowed			
2 A Sepreh Timorut (see)			
2 Search (Inteout (sec.)			
For improved performance specify the	e Tree and distinguished		
Catalog name's.			
Ties: Daraioà.			
Add Reg	nove Replace		
	OK Cancel		

11. 按一下**OK**儲存更改並退出Novell Client應用程式。

這些更改將在下次登入時顯示在Novell Login對話方塊中。此影象提供Novell Login對話方塊的示例。

🔀 Novell I	Login
Novel	l₀ Client™ for Windows* N
<u>U</u> ser Name <u>P</u> assword:	
NDS S	cript Dial-up NMAS
<u>I</u> ree:	MTG Trees
<u>C</u> ontext:	Contexts
Server:	NOVELL1 Servers SecretStore' Novella
. And the second se	
	OK Cancel Advanced <<

注意:在802.1X環境可用且身份驗證建立之前,Novell Login對話方塊中的某些功能不可用。例如 ,如果沒有網路連線,樹、上下文和伺服器按鈕將無法正常工作。

您可以將思科安全服務客戶端配置為允許802.1X在Novell之前對使用者進行身份驗證。在Network Profile對話方塊中,選中Automatically established User Connection和Before User Account。此外 ,驗證「自動建立機器連線」覈取方塊是否未選中。

思科安全服務客戶端配置

本節介紹要與Novell客戶端一起使用的關鍵思科安全服務客戶端設定。無論登入時是否指定上下文 ,思科安全服務客戶端的配置設定都保持不變。有關適用於您網路的其他配置設定,請參閱Cisco安 全服務客戶端幫助系統。

• 在Network Profile對話方塊中,選中Automatically established User connection覈取方塊和 Before user account (僅支援智慧卡/密碼) 覈取方塊。

🐵 Network Profile				
Network Name: Office Available to all users (public profile)				
 Automatically establish Machine connection Automatically establish User connection Before user account (supports smartcard/password only) 				
Network Configuration Summary:				
Authentication: PEAP;				
Credentials: Use Single Sign On.				
۳۶ Modify				
Access Devices				
Access / SSID Mode Notes				
MDChidden (hidden) WPA2 Enterprise MDCis#1 WPA2 Enterprise				
Add Modify Configuration Remove Help QK Cancel				

• 在Network Authentication對話方塊中,選中Authentication Methods區域中的所需選項,然後 按一下**Use Single Sign on Credentials**單選按鈕。

Network Authentication	<u>×</u>
Network: Office	
Authentication Methods: Tum Off Tum On Use Usemame as Identity Use 'Anonymous' as Identity Protocol EAP-MD5 EAP-MSCHAPv2 EAP-TLS 	User Credentials: Use Machine Credentials Use Single Sign on Credentials Request when needed Remember forever Remember for this session Remember for 5 minutes
☐ FAST ☐ GTC ✔ Configure	
Help	OK Cancel

<u>相關資訊</u>

• <u>技術支援與文件 - Cisco Systems</u>