

Deploying Network Access Quarantine Control, Part 2

I stepped qua cách làm vi?c truy c?p c?a quarantine m?ng (NAQC) works and ?ã cung c?p chi ti?t ?i?u khi?n instructions. In the second and final installment, I'll continue the procedure by finishing the deployment, then discuss how ISA Server 2004's entrance to the marketplace changes the field of NAQC and how to quarantining is implemented within the ISA Server itself.

I stepped qua cách làm vi?c truy c?p c?a quarantine m?ng (NAQC) works and ?ã cung c?p chi ti?t ?i?u khi?n instructions. In the second and final installment, I'll continue the procedure by finishing the deployment, then discuss how ISA Server 2004's entrance to the marketplace changes the fields of NAQC and how quarantining is implemented within the ISA Server itself.

Let's start thì b?n còn t?t.

Distributing the Profile to Remote Users

C?u hình b?n t?o trong các cài ??t tr??c c?a ?i?u này này ???c t?o vào m?t t?p tin executable mà th? ???c phân tách ??n các ng??i dùng xa b?n và ch?y trên các h? th?ng này t? ??ng, t?o m?t profile mà không có m?t ?ng d?ng nào. Có nhi?u tùy ch?n ?? l?y t?p tin executable ?? ng??i dùng.

B?n có th? g?i t?p tin t?p tin ?ã th?c hi?n v?i m?t t?p tin g?i ??n m?t th? th?, ho?c h?n nào, m?t liên k?t vào t?p tin executables ?ã ???c ??t trên m?t web server somewhere. Trong th? m?c e-mail, b?n có th? dùng l?nh ?? ch?y t?p tin và s? d?ng m?i k?t n?i cho t?t c? xa xa truy c?p. B?n có th? có ch?y ???c th?c hi?n v?i ph?n c?a m?t logon ho?c logoff script, nh?ng ?? vì, b?n c?n ph?i v?i ng??i dùng ??ng nh?p vào m?t k?t n?i chuy?n ??i, ho?c ch? khi các ng??i dùng có th? ??ng nh?p k?t thúc t?p tin, ho?c ch? khi ng??i dùng ng??i dùng nh?p vào th? m?c home và k?t n?i ??n b?n corporate or network corporate.

Regardless of which method b?n ?ã ch?n ?? Initiate các c?u hình installer ?? b?n ng??i dùng, b?n nên ??t th?i gian phiên b?n c?a t?p tin c?u hình trên m?t quarantined resource, so client computers that do not pass your baseline script's compliancy checks can still surf to web thì?t b? c?n thì?t và t?i v? phiên b?n hi?n th?i mà không có s? xác th?c c?a b?n further.

Configuring the Quarantine Policy

T?p tin cu?i cùng trong ti?n trình ti?n trình ?? c?u hình s? th?c hi?n quarantine trong RRAS. Trong ph?n này, Tôi t?o m?t quarantine policy trong ??a ch? RRAS mà có th? ??ng nh?p t?p tin cài ??t trên m?t web máy ph?c v? ??? c làm vi?c là quarantined resource.

If it is configured to use the Windows authentication provider, then RRAS uses Active Directory or an NT 4 domain (remember, the RRAS machine needs only to run Windows Server 2003; it doesn't need to belong to an Active Directory-based domain) ?? xác ??nh ng??i dùng và xem ? các tài kho?n tài kho?n c?a b?n. Nếu RRAS là c?u hình ?? s? d?ng RADIUS, có th? máy RADIUS ph?i là m?t Server 2003 machine running IAS. Incidentally, IAS also uses Active Directory or xác th?c NT thành công c?n dùng và xem ? các tài kho?n tài kho?n.

Configuring RRAS

1. Open the RRAS Manager.
2. In the left-pane, right-click Remote Access Policies, and then select New Remote Access Policy from the context menu. Click Next trong các t?p tin introductory.
3. The Policy Configuration Method page appears. Hãy nh?p Quarantined VPN k?t n?i xa cho tên c?a này policy, shown shown Figure 4. Click Next when you're finished.

Picture 1 of Deploying Network Access Quarantine Control, Part 2

Figure 4: The Policy Configuration Method screen

4. The Access Method page appears. Select VPN, and then click Next.
5. On ng??i dùng ho?c truy c?p Access Group, select Group, và Then click Add.
6. Lo?i trong nhóm nhóm mà c?n dùng VPN trong thành m?ng. Nếu t?t c? các ng??i dùng này có quy?n, enter Everyone or Authenticated Users. B?n có th? là m?t nhóm ?ã ???c thêm VPNUsers trên mi?n này này có nên truy c?p cho VPN Ability. Click OK.
7. B?n s? ???c tr? l?i ?? s? d?ng ng??i dùng ho?c truy c?p Group Group, và s? tìm th?y nhóm này ?ã ???c ?? ng nh?p trong danh sách danh sách, nh? ???c hi?n th? Figure 5. Click Next if it looks correct.

Picture 2 of Deploying Network Access Quarantine Control, Part 2

Figure 5: Ng??i dùng hayGroup Access screen.

8. The Authentication Methods page appears. ?? gi? thông báo này m?i, s? d?ng MS - CHAP v2 xác th?c giao th?c, mà ???c ch?n b?i m?c ??nh. Click Next.
9. Ch? m?c c?a t?p tin Encryption c?a ch? ??, xác ??nh thi?t l?p Strongest ?ã ??t là ch? tùy ch?n ch?. This is shown in Figure 6. Then, click Next.

Picture 3 of Deploying Network Access Quarantine Control, Part 2

Figure 6: the Policy Encryption Level screen

10. L?i k?t thúc t? th? thu?t b?i clicking Finish.

Configure attributes to be quarantined

N?u b?n c?n th?c hi?n c?u hình các thu?c tính s? ???c ???c assign ??n s? l?nh quarantined.

1. Back in RRAS Manager, right-click on the new Quarantined VPN remote access policy, and select Properties from the context menu.
2. Navigate to the Advanced tab, and click Add to include another attribute in the list.
3. The Add Attribute dialog box is displayed, as depicted in Figure 7.

Picture 4 of Deploying Network Access Quarantine Control, Part 2

Figure 7: The Add Attribute dialog box

4. Click MS-Quarantine-Session-Timeout, and then click Add.
5. In hộp thoại Thông tin thông báo, Dùng nút giá trị mặc định của 60, mà số này xác định trong giây, để xác định của phiên bản này. Click OK, and then OK again to return to the Advanced tab.
6. Click Add. In the Attribute list, click MS-Quarantine-IPFilter, and then click Add again. Hãy xem IP Filter Attribute Information screen, as shown in Figure 8.

Picture 5 of Deploying Network Access Quarantine Control, Part 2

Figure 8: The IP Filter Attribute Information dialog box

7. Hãy xem nút Thông tin khóa nhập, mà hiển thị các trong Inbound Filters box.
8. Click New để thêm bộ lọc mới. The Add IP Filter dialog box is displayed. In the Protocol field, TCP select. In the Destination port field, enter 7250. Click OK.
9. Now, back to screen Screen Inbound, select the Permit only the packets listed below truy cập radio button. Your screen should look like Figure 9.

Picture 6 of Deploying Network Access Quarantine Control, Part 2

Figure 9: Thông tin in ch? để trả lời v?

10. Hãy chọn New và thêm các kết nối nhúng vào cho DHCP, DNS, và WINS giao dịch, Repeat không Steps vào và bao gồm một số thay đổi cần thiết và kiểm tra.
11. Click New and add an filter input for a quarantine resource, such as a Web server, where your profile installer is located. Specify the IP address appropriate for tài nguyên trong phần Destination Network của Thêm IP Filter screen, as shown in Figure 10.

Picture 7 of Deploying Network Access Quarantine Control, Part 2

Figure 10: The Add IP Filter box, adding a quarantined Web resource

12. Finally, click OK on the Inbound Filters dialog box to save danh sách bộ lọc.
13. On the Edit Dial-in Profile dialog box, click OK to save the changes to the profile settings.
14. Then, thay đổi các thay đổi chính sách, click OK once more.

Creating Exceptions to the Rule

While nó có thể trở thành thành, có những điều cần lưu ý về việc áp dụng các quy định bị cách ly cho các trường hợp hình thức xác định, có thể thực hiện bằng cách ký hợp đồng xác định trong bộ Organization mà Mitigate this requirement. If so, this simplest way to excuse a user or group of users from participating in the quarantine is to create an exception security group with Active Directory. Những điều cần lưu ý của nhóm này nên phải mà những phần này không cần tham gia trong tiến trình quarantining.

Sở dĩ mà nhóm, tạo một chính sách khác để áp dụng nhóm của xác định mà trường hợp hình thức tùy chọn xa truy cập của danh sách bộ lọc tạo ra. Thời gian, không có, không thêm thêm hợp đồng trường hợp hình thức MS-Quarantine-IPFilter or MS-Quarantine-Session-Timeout attributes. Bằng cách một chính sách để tạo, để bộ chính sách này để dùng các nhóm exceptions vì thì nó có thể kiểm tra thực tế khi chính sách các cái khác.

Extending Functionality with ISA Server 2004

Quarantine Control cho ISA Server 2004 có thể làm việc với Routing và remote Access service, những điều cần xác định đã được đề cập trong bài này. The main difference is in the fact that with ISA Server, you can require that a client attempt to log in is assigned to the Quarantined VPN Clients network in ISA, with an associated firewall policy that is very stringent, until the Connection Manager is running on the desktop passes một thông báo về ISA để bị kiểm tra những điều cần kiểm tra integrity. Like the plain vanilla NAQC technique, ISA quarantining does not rely on

Connection Manager profiles and yêu cầu một số dịch vụ script ?? th?c hi?n là tùy ch?n cho b?n môi tr??ng.

Within ISA Server 2004, you have two options with ch? ?? ?? c?u hình quarantine: policies and ISA Server lets them join the regular VPN Clients network, as seen within the interface ISA Server, ch? khi chúng ?ã ???c ??ng nh?p check. You can also enable quarantining through ISA Server itself, and clients can make use of Quarantined Integration VPN Clients network and any firewall policies associated with therewith. H? th?ng chính chính c?a ph??ng pháp này, b?n có th? s? d?ng quarantining trên m?t máy tính máy ch? ISA, không ph?i ch? nào v?i Windows Server 2003 ???c cài ??t.

ISA Server quarantining h? a more robust timeout feature, either, allowing clients to Remain in the Quarantined VPN Clients network for a specific number of seconds all before being disconnected, and It also h? an exception list, ?ó cho phép you to Identify users (via ho?c Active Directory or a RADIUS server) that should not be quarantined no matter what.

Các thông báo nghe v? quarant ???c ?ã ???c nâng c?p ???c xác ??nh cho h? tr? ISA Server và có s?n trong các ISA Server 2004 Resource Kit, mà có th? ???c l?y t? Microsoft site.

To enable quarantining with ISA Server:

1. Open ISA Server Management.
2. On the left pane, expand the node that corresponds to your computer, and then click Virtual Private Networks (VPN).
3. In the right pane, navigate to the Tasks tab, and then click Enable VPN Client Access.
4. Now, expand the Configuration node and select Networks.
5. In the middle pane, click the Networks tab.
6. Double-click on Quarantined VPN Clients network to open the properties box for the network.
7. Navigate to the Quarantine tab. ?ây là hi?n th? trong Figure 11.
8. Click the 'Enable quarantine control' checkbox to allow quarantining to take place. C?nh báo s? hi?n th?i hi?n th?i ?? th?c hi?n, b?n th?c hi?n khi th?c hi?n là ho?t ??ng, và không có c?u hình không h?p l?, các b?n s? ???c xác ??nh quarantined.
9. Hãy ch?n tùy ch?n quarantine v?i RADIUS server Policies (tùy ch?n first) or ISA Server policies (the second option).

10. Hãy nh?p m?t l?n th?i
11. Hãy nh?p không nào nào ?? quarantining trong 'Exempt các ng??i dùng t? Quarantine Control' box.
12. Click OK, and then Apply in the Management Server ISA console, to apply the changes.

Picture 8 of Deploying Network Access Quarantine Control, Part 2

Figure 11: Quarantined VPN Clients in ISA Server 2004

N?u b?n th?c hi?n này Steps này, t? máy ph?c v? ISA Server 2004 Resource tìm th?y ConfigureRQSforISA.vbs script và ch?y nó. ?ây s? t? ??ng t?o m?t ch? ?? truy c?p trong ISA này s? cho phép chuy?n qua pass vào c?ng 7250 t? c? hai Clients VPN và Quarantined VPN Clients Networks ?? m?ng m?ng. Nh?ng s? xác th?c này, vì xác ??nh t? máy ph?c v? ng??i dùng, b?n ?ã ???c g? b? các ki?m tra integrity và ???c xác th?c ?? chuy?n ??i v? m?ng chính quy ???c g?i vào c?ng này.

B?n có th? x? lý các ch? ?? truy c?p truy c?p cho Quarantined VPN h? th?ng các t?p tin mà theo sau:

1. Allow truy c?p truy?n chuy?n t?i LDAP máy ph?c v? trên máy ?nh n?i b?.
2. Allow traffic to ???c g?i qua cho các ?i?u ki?n domain.
3. Allow DNS, DHCP, and WINS traffic to be passed to a hardened set of DNS servers, có th? trên m?t perimeter network.
4. Allow traffic to a hardened, web server that contains software antivirus, signature and detection engine updates.

Conclusion

In this article, I've discussed quarantining using services included in Windows Server 2003 and its associated resource and feature packs, and I've also touched on the extended quarantine functionality within ISA Server. N?u b?n s? d?ng các c? s? d? li?u s? ???c h? tr? ho?c g? b? s? k?t n?i ?ã chia s? v?i máy ?nh khi b?n k?t n?i ?? k?t n?i ?i.

About the author

Jonathan Hassell is an author and consultant specializing in Windows administration and security. He is the author of *Managing Windows Server 2003* and *RADIUS*, both published by O'Reilly & Associates, and *Hardening Windows*, published by Apress. He also holds the periodic public seminars; see www.hardeningwin.com for details. He ???c ghi ???c cho Windows & .NET Thông báo và WindowsITSecurity.COM and là m?t contributor to PC Pro, leading computer magazine in the United Kingdom.

You finished reading the article "**Deploying Network Access Quarantine Control, Part 2**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.