Lesson 14: Configuring Network Access Protection (NAP)

MOAC 70-411: Administering Windows Server 2012



WILEY

Overview

- Exam Objective 4.3: Configure Network Access Protection (NAP)
- Using Network Access Protection (NAP)

Using Network Access Protection (NAP)

Lesson 14: Configuring Network Access Protection (NAP)

© 2013 John Wiley & Sons, Inc.

Network Access Protection (NAP)

- NAP is Microsoft's software for controlling network access for computers based on the health of the host.
- NAP can be used on any computer that runs Windows and supports NAP.
- Types of computers that connect to a network:
 Desktop computers
 - Roaming laptops
 - Unmanaged home computers
 - Visiting laptops

NAP Built-In Enforcement Methods



© 2013 John Wiley & Sons, Inc.



© 2013 John Wiley & Sons, Inc.



NAP Connection Process

- 1. When the NAP client connects to a network that requires NAP, each SHA on the NAP client validates its system health and generates an SoH.
- 2. The NAP client combines the SoHs from multiple SHAs into a SSoH and sends the information to a NAP health policy server that is defined with the NAP enforcement point.
- 3. The NAP health policy server uses its installed SHVs and the health requirements policies to determine whether the NAP client meets health requirements.

NAP Connection Process

- 4. The NAP health policy server combines the SoHRs from the multiple SHVs into a System Statement of Health Response (SSoHR) and sends the SSoHR back to the NAP client through the NAP enforcement point.
- 5. If the client is compliant, the enforcement point allows the connection. If the client is noncompliant, the computer can be connected to a remediation network.
- 6. If the computer is noncompliant, the noncompliant computer can attempt to come into compliance.
- 7. If the status of the computer changes, the entire process starts over.

Installing Network Access Protection

- Because NAP is offered through NPS, the installation is similar to installing NPS (discussed in Lesson 12).
- However, you want to add HRA, which is used to issue health certificates to NAP client computers that are compliant with network health requirements.
- For HRA to function, you need to have a CA available.

Install Network Policy Server

B	Add Roles and Features Wizard	_ D X
Before You Begin Installation Type Server Selection Server Roles Features	Add Roles and Features Wizard S Select the role services to install for Network Policy and Access S Role services Network Policy Server Health Registration Authority Host Credential Authorization Protocol	DESTINATION SERVER Win2012Srv2.contoso.com Gervices Description Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection
Network Policy and Acces Role Services Confirmation Results		request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.
	< <u>P</u> revious <u>N</u> ext >	Install Cancel

Selecting the role services

Install Network Policy Server

Ъ	Add Roles and Features Wizard
Certification Author	DESTINATION SERVER WIN2012SRV.contoso.com
Installation Type	Health Registration Authority (HRA) requires that at least one Certification Authority (CA) be associated with it.
Server Selection Server Roles Features	 Use the local CA to issue health certificates for this HRA server. There is an existing CA on this computer. If you choose to use it, it will be dedicated to issuing health certificates.
Network Policy and Acces Role Services	O Use an existing remote CA. If you choose to use an existing CA it should be one dedicated to issuing health certificates.
Certification Authority Authentication Requir	 Select Select a CA later using the HRA console.
Confirmation Results	You will not be able to issue health certificates to NAP client computers until this CA is configured.
	< Previous Next > Install Cancel

Specifying the Certificate Authority

Install Network Policy Server

a	Add Roles and Features Wizard	_ 🗆 X
Authentication Re Before You Begin Installation Type Server Selection Server Roles Features Network Policy and Acces Role Services Certification Authority Authentication Requir Confirmation Results	quirements Health Registration Authority can be configured to ensure that only users domain can get health certificates. Do you want to require that users be authenticated in order to get a healt Yes, require requestors to be authenticated as members of a domain. This option is only available when the computer is joined to a domain. No, allow anonymous requests for health certificates.	DESTINATION SERVER WIN2012SRV.contoso.com authenticated to the h certificate? (recommended)
	< Previous Next >	Install Cancel

Configuring the authentication requirements

Configuring NAP Enforcement

To configure NAP:

- 1. Install and configure the server on which you will apply NAP enforcement.
- 2. Configure NPS and the NAP-related policies.
- 3. Configure the remediation servers.

DHCP Enforcement

To control network access, DHCP enforcement sets the following:

- DHCP Router option is set to 0.0.0.0 so noncompliant computers do not have a configured default gateway.
- Subnet mask is set to 255.255.255.255 so that there are no routes to the attached subnet.

Configuring NAP Enforcement for DHCP

To configure DHCP enforcement, you must:

- 1. Configure a DHCP server and create the appropriate DHCP scopes.
- 2. Install NPS on the DHCP server.
- 3. Run the NAP Wizard to configure the connection request policy, network policy, and NAP health policy. Define the remediation severs, which noncompliant clients can access.
- 4. Enable NAP for individual DHCP scopes.
- 5. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.



Opening the DHCP console

New Scope Wizard
Scope Name You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
Description:
< Back Next > Cancel

Defining the scope name

New Scope Wizard
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server Enter the range of addresses that the scope distributes. Start IP address: End IP address: Configuration settings that propagate to DHCP Client
Length: 0 📩 Subnet mask:
< Back Next > Cancel

Specifying the IP address range

New Scope Wizard
Lease Duration The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate. Set the duration for scope leases when distributed by this server. Limited to: Days: Hours: Minutes:
< Back Next > Cancel

Specifying the lease duration

	New Scope Wizard	
Router (Default Gateway) You can specify the routers,	, or default gateways, to be distributed by this scope.	Ĵ.
To add an IP address for a r	router used by clients, enter the address below.	
I <u>P</u> address:	A <u>d</u> d	
	<u>R</u> emove	
	Цр	
	D <u>o</u> wn	
1		
	< <u>B</u> ack <u>N</u> ext > Cancel	

Defining the default gateway

9		DHCP	_ D X
File Action View He	File Action View Help		
🗢 🄿 🖄 🖬 🗙 🗒	0 🗟 🚺 🛅 📮 🛱		
🖞 онср	Name		Actions
win2012srv.con win2012	Add/Remove Bindings		win2012srv.contoso.com
▶ 🖺 Scope [1	Authorize		More Actions 🔹 🕨
☐ Server O ☑ Policies ▷ ♥ Filters	Backup Restore		
þ 🖡 IPv6	All Tasks 🔹 🕨		
	View 🕨		
	Delete		
< 111	Refresh		
Authorize this server in r	Export List		
	Properties		
	Help		

Authorizing the DHCP server



Starting the Network Policy Server console

	Configure NAP	X
	Select Network Connection Method For Use with NAP	
Network con Select the netw computers. Crea network connect	nection method: ork connection method that you want to deploy on your network for NAP-capable client ated policies will work with this network connection type only. To create policies for additional ction methods, you can run the wizard again.	
Dynamic Host	Configuration Protocol (DHCP)	¥
default text or m NAP DHCP Additional rec You mu Iink bek Additior	quirements: st perform additional actions to set up NAP. View additional NAP requirements by clicking on th w.)e
	Previous Next Finish Cancel	

Selecting the network connection method

	Configure NAP	X
	Specify NAP Enforcement Servers Running [OHCP Server
RADIUS client Server, you ca	is are network access servers, not client computers. If the local computer i an skip this step and click Next.	s running DHCP
If you want to add must also server (the loca	add remote DHCP servers as RADIUS clients, click Add. All remote DHCP run NPS. Also, remote DHCP/NPS servers must forward connection requi al computer).	'servers that you ests to this NPS
Remote Acces	nts:	Add
Wireless		Edit
		Remove
		1
	Previous Next Finish	Cancel

Specifying NAP enforcement servers running DHCP server

Configure NAP X
Specify DHCP Scopes
When you specify one or more NAP-enabled scopes, NPS evaluates client health and performs authorization for client computers requesting an IP address from the designated scopes. If you do not specify any scopes, the policy applies to all NAP-enabled scopes at the selected DHCP servers. If
you specify a scope that is not NAP-enabled, you must enable NAP for the scope after completing this wizard.
To specify one or more scopes, click Add.
DHCP scopes:
Add
Edit
Remove
Previous Next Finish Cancel

Specifying the DHCP scopes to apply to NAP

Configure NAP X
Configure Machine Groups
To grant or deny access to groups of computers, add groups to Machine Groups.
If no groups are selected, this policy applies to all users.
Machine Groups:
Add
Hemove
Previous Next Finish Cancel

Specifying the computer groups that NAP will apply to

	Configure NAP	x
	Specify a NAP Remediation Server Group and	URL
Remediation Remediation se one or more rem	Server Group: rvers store software updates for NAP clients that need them. Remediation Serve rediation servers.	r Groups contain
Select a Reme	liation Server Group that you have already configured or, to create a new group,	click New Group.
<none></none>	×	New Group
http://		
	Previous Next Finish	Cancel

Specifying the NAP Remediation Server group and URL

emediation Serve	er Group)
	~	
Friendly Name		Add
		E dit
		Remove
	OK	Cancel
	Friendly Name	Friendly Name

Adding computers to the Remediation Server group

Configure NAP X			
Define NAP Health Policy			
The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.			
Name			
✓ Windows Security Health Validator			
Finable auto-remediation of client computers			
If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers. If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.			
Network access restrictions for NAP-ineligible client computers:			
Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.			
Allow full network access to NAP-ineligible client computers.			
Previous Next Finish Cancel			

Defining NAP Health Policy

Enable NAP on All DHCP Scopes

IPv4 Properties ? X					
Filters General	Eailov DNS	Failover DNS Netwo		Advanced vork Access Protection	
Network Access Protection is working on this server. You can setup the Network Access Protection settings for the DHCP server here.					
Enable on all scopes Disable on all scopes					
Full Access					
 Restricted Access Drop Client Packet 					
	OK		Cancel	Apply	

Enabling NAP for all DHCP scopes

Enable NAP on an Individual DHCP Scope

Scope [192.168.1.0] Scope1 Properties				
General DNS Network Access Protection Advanced				
Network Access Protection				
You can setup the Network Access Protection settings for this scope here.				
Network Access Protection Settings				
Enable for this scope				
Use default Network Access Protection profile Use custom profile Profile Name				
C Disable for this scope				
OK Cancel Apply				

Enabling NAP for individual DHCP scopes

Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server

٩ 🗈	APCLCFG - [NAP Client Configuration (Local Computer)]	×
File Action View Help		
😥 NAP Client Configuration (Local Comp 🛛 NA	P Client Configuration (Local Computer)	Actions
Enforcement Clients		NAP Client Configuration (Lo 🔺
Difference settings Health Registration Settings	2	Import
	9	Export
	Getting Started	View
		a Refresh
	Use these steps to create and manage the enforcement clients, specify user interface settings for the Network Access Protection	Properties
	(NAP) client, and configure settings for trusted health registration authority servers.	🕜 Help
	Create and Manage Enforcement	
	Clients	
	Enforcement Clients A Learn more about	
	enrorcement clients.	
	Emoniful land laterface Entitivate for	
	the NAP Client	
	Learn more about user	
	Juser Interface Settings - interface settings.	
	Configure Settings for Trusted Server 3	
	×	

Opening the NAP Client Configuration console

Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server

🚈 NAPCLCFG - [NAP Client Configuration (Local Computer)\Enforcement Clients]				
File Action View Help				
🗢 🄿 🗾 🖬 🚺				
👔 NAP Client Configuration (Local Comp	Enforcement Clients		Actions	
Enforcement Clients Iser Interface Settings	Name	Status	Enforcement Clients	
Health Registration Settings	DHCP Quarantine Enforcement	: Client Disabled Disabled	View 🕨	
	BD Gateway Quarantine Enfor	cement Client Disabled	Refresh	
	🐁 EAP Quarantine Enforcement (lient Disabled	👔 Help	
			DHCP Quarantine Enforceme 🔺	
			Enable	
			Refresh	
			Properties	
	S DHCP Quarantine Enforcement Client			
	ID: 75	617		
	Name: D	HCP Quarantine Enforcement Client		
	Description: Pr	ovides DHCP based enforcement for NAP		
	Version: 1.	0		
	Vendor: M	icrosoft Corporation		
	Status: Di	sabled		

Configuring the enforcement clients

Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server

DHCP Quarantine Enforcement Client Properties			
General			
Enabling the client allows Network Access Protection to be enforced from this device.			
Enable this enforcement client			
OK Cancel Apply			

Enabling enforcement client for DHCP

Configuring NAP Enforcement for VPN

- 1. Install NPS on the VPN server.
- 2. Configure the VPN server and have them use PEAP-based authentication (either PEAP-MS-CHAP v2 or PEAP-TLS).
- 3. Run the NAP Wizard to configure the connection request policy, network policy, and NAP health policy. Define the remediation severs, which noncompliant clients can access.
- 4. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.

Configure NAP for VPN Servers

	Configure NAP	x
	Select Network Connection Method For Use with NAP	
Networ Select th compute network	it connection method: ne network connection method that you want to deploy on your network for NAP-capable client rs. Created policies will work with this network connection type only. To create policies for additional connection methods, you can run the wizard again.	
Virtual F	Private Network (VPN)	¥
Policy This def default t	name: ault text is used as part of the name for each of the policies created with this wizard. You can use the ext or modify it.	
NAP VF	PN	
Additio	nal requirements: You must perform additional actions to set up NAP. View additional NAP requirements by clicking on th link below. Additional Requirements	ie
	Previous Next Finish Cancel	

Selecting the Virtual Private Network (VPN) for the Network Connection

Configure NAP for VPN Servers

Configure NAP	X		
Configure User Groups and Machine Groups			
To grant or deny access to groups of computers, add groups to Machine Groups. To grant or deny access to groups of users, add groups to User Groups. You can configure both Machine Groups and User Groups for this policy.			
If no groups are selected, this policy applies to all users. Machine Groups:			
User Groups:	Add Remove		
	Add Remove		
Previous Next Finish	n Cancel		

Specifying user and machine groups for NAP

Configure NAP for VPN Servers

Configure NAP ×				
Configure an Authentication Method				
Protected Extensible Authentication Protocol (PEAP) is the authentication method used with wireless access points and authenticating switches. To configure PEAP, you must select a server certificate on the NPS server and you must configure an authentication type.				
NPS Server Certificate				
To select a server certificate issued by your organization trusted root certification authority (CA) or a public CA that is trusted by client computers, click Choose. To view the selected certificate, click View.				
WIN2012SRV.contoso.com (Valid until 9/4/2013 6:05:39 PM)				
View Choose				
EAP types: Select EAP types to use with PEAP. The authentication type determines the kind of credentials that NPS can accept from client computers and users (either user name and password or a certificate). ✓ Secure Password (PEAP-MS-CHAP v2). This authentication type permits users to type password-based credentials during authentication. Smart Card or other certificate (EAP-TLS). This authentication type requires certificates on smart cards or in the client computer certificate store. For this authentication type you must deploy your own trusted root CA.				
Previous Next Finish Cancel				

Configuring an authentication method for NAP

- **System Health Validators (SHVs)** settings define the requirements for client computers that connect to your network.
- You configure SHVs using the Network Policy Server console.
- Windows 8 includes a Windows Security Health Validator SHA that monitors the Windows Security Center settings.
- Windows Server 2012 includes a corresponding Windows Security Health Validator SHV.



Managing the Windows SHV



Configuring Windows SHV

Configuring System Health Validators

SHV options:

- Firewall Settings
- Antivirus Settings
- Spyware Protection Settings
- Automatic Updates Settings
- Security Updates Settings



Configuring Security Updates settings

- Health policies consist of one or more system health validators and other settings that enable you to define client computer configuration requirements for the NAPcapable computers that attempt to connect to your network.
- Health policy pairs:
 NAP-compliant
 NAP-noncompliant

NAP DHCP Compliant Properties	NAP DHCP Noncompliant Properties
Settings	Settings
Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.	Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.
Select an existing template:	Select an existing template:
Policy name:	Policy name:
Client SHV checks:	Client SHV checks:
Client passes all SHV checks	Client fails one or more SHV checks
Name Setting	Name Setting
✓ Windows Security Health Validator Default Configuration ✓	Vindows Security Health Validator Default Configuration V
OK Cancel Apply	OK Cancel Apply

Viewing the health policies

	NAP DHCP Noncompliant Properties	x
Overview Conditions Cor	nstraints Settings	
Configure the conditions fo	r this network policy.	
If conditions match the cor connection request, NPS s	nection request, NPS uses this policy to authorize the connection request. If conditions do not match the kips this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	ן ר
Health Policy	NAP DHCP Noncompliant	
MS-Service class	NAP DHCP	
The Health Policies conditi	on restricts the policy to only clients that meet the health criteria specified in the health policy.	
	A <u>d</u> d <u>E</u> dit <u>R</u> emove	
	OK Cancel App	ly .

Displaying the conditions of a health policy

•	Network Policy Server		
File Action View Help			
 NPS (Local) RADIUS Clients and Servers Policies Connection Request Policies Network Policies Health Policies Network Access Protection System Health Validators Settings Error Codes Remediation Server Groups Accounting Templates Management 	Network Policies Network policies allow you to designate who is authorized connect. Policy Name	to connect to the network and	the circumstances under which they can or cannot Access Type Source
	Secure Wireless Connections Virtual Private Network (VPN) Connections NAP DHCP Compliant NAP DHCP Non NAP-Capable NAP VPN Compliant NAP VPN Noncompliant NAP VPN Non NAP-Capable Connections to Microsoft Routing and Remote Access server Connections to other access servers NAP DHCP Compliant Conditions - If the following conditions are met: Condition Value Health Policy NAP DHCP Compliant MS-Service class NAP DHCP	Enabled 1 Enabled 2 Enabled 3 Enabled 4 Enabled 5 Enabled 6 Enabled 7 Enabled 8 Enabled 393939 Enabled 1000000	Grant Access Unspecified Grant Access Remote Access Server(VPN-Dial up) Grant Access DHCP Server Grant Access DHCP Server Grant Access Remote Access Server(VPN-Dial up) Grant Access Remote Access Server(VPN-Dial up) Grant Access Remote Access Server(VPN-Dial up) Deny Access Unspecified Deny Access Unspecified
	Settings - Then the following settings are applied:		×

Displaying the network policies

NAP DHCP Noncompliant Properties
Overview Conditions Constraints Settings
Policy name: NAP DHCP Noncompliant
Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.
✓ Policy enabled
Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. <u>What is access permission?</u>
Grant access. Grant access if the connection request matches this policy.
O Deny access. Deny access if the connection request matches this policy.
✓ Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .
Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server:
DHCP Server 🗸
O Vendor specific:
OK Cancel Apply

Viewing NAP Enforcement for a network policy

NAP enforcement settings:

- NAP DHCP-compliant: Allow full network access.
- NAP DHCP-noncompliant: Allow limited access.
- NAP DHCP nonNAPcapable properties: Allow full network access.

Configuring Isolation and Remediation

- If a computer is noncompliant, it should be isolated from production network.
- When you configure NAP, you can configure either a monitor only policy or an isolation policy.

Configuring Isolation and Remediation

Remediation servers typically consist of:

- DHCP servers to provide IP configuration
- Naming servers including DNS servers and WINS servers
- Active Directory domain controllers (readonly domain controllers are recommended to minimize security risks)
- Internet proxy servers so that noncompliant NAP clients can access the Internet

Configuring Isolation and Remediation

Remediation servers typically consist of (continued):

- HRAs so that noncompliant NAP clients can obtain a health certificate for the IPsec enforcement method
- Web server that contains the troubleshooting URL server, so users can access information on compliance
- Anti-virus/anti-malware servers to retrieve updated anti-virus/anti-malware updates
- Software update servers so that clients can get Windows updates

Configuring NAP Client Settings

- You can use the Enable Security Center in the Group Policy procedure to enable Security Center on NAP-capable clients using Group Policy.
- Some NAP deployments that use Windows Security Health Validator require Security Center.
- Open the Services console to start and set the startup type to Automatic in the Network Access Protection Agent service.

Configuring NAP Client Settings

To verify a client's configuration, run the following command:

netsh nap client show state

Configuring NAP Client Settings

64 .	Administrator: C:\Windows\System32\cmd.exe	x					
C:\>netsh nap client s	how state	^					
Client state:							
Name Description Protocol version Status Restriction state Troubleshooting URL Restriction start time Extended state GroupPolicy	 Network Access Protection Client Microsoft Network Access Protection Client 1.0 Enabled Not restricted = = = Not Configured 						
Enforcement client sta	Enforcement client state:						
Id Name Description Version Lendor pame	= 79617 = DHCP Quarantine Enforcement Client = Provides DHCP based enforcement for NAP = 1.0 = Microsoft Corporation	=					
Registration date	= = = No						
Id Name Description tection Uersion Vendor name Registration date Initialized	= 79619 = IPsec Relying Party = Provides IPsec based enforcement for Network Access P = 1.0 = Microsoft Corporation = = No	10					
Id Name Description Version Vendor name Registration date Initialized	= 79621 = RD Gateway Quarantine Enforcement Client = Provides RD Gateway enforcement for NAP = 1.0 = Microsoft Corporation = No						
Id Name Description authenticated network logies. Version Vendor name Registration date Initialized	 = 79623 = EAP Quarantine Enforcement Client = Provides Network Access Protection enforcement for EA connections, such as those used with 802.1X and UPN techn = 1.0 = Microsoft Corporation = No 	P no					
0k.		~					

Using the netsh nap client show state command

Lesson Summary

- Microsoft Network Access Protection (NAP) is software for controlling networked computers based on the host's health.
- NAP includes built-in enforcement methods that define the mechanisms that NAP can use, including DHCP, Internet Protocol Security (IPsec), VPN, 802.1, and more.
- System Health Agents (SHAs) are components that report on one or more elements of the health of a NAP client.
- Each SHA creates a Statement of Health (SoH) that transmits to the NAP Agent. Each SHA generates a new Statement of Health whenever the status is updated.
- NAP Agent maintains information about the health of the NAP client computer and transmits information between the NAP enforcement clients and the SHAs.

Lesson Summary

- System Health Validators (SHVs) settings define requirements for client computers that connect to your computer.
- Health policies consist of one or more system health validators and other settings that enable you to define client computer configuration requirements for NAP-capable computers.
- Typically, you use a monitor-only policy when you first implement NAP to test the implementation so that you can verify which computers are blocked and which are granted access to the production network by viewing the security logs in the Event Viewer on the NAP server.
- A remediation server group and troubleshooting URL will be available to users if they fail the compliance check.
- For clients to use NAP, they must have Security Center enabled and have the NAP Agent service running.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.



