

# OTHER

*Revised 4/28/2008*

**/training/etc**

*The Art of Knowledge.*

**This Page Intentionally Left Blank**

**Configuration Management****Networking/Security**

Building and Operating Snort.....	1
Snort Rules.....	2
Sourcefire 3D Solution.....	3
Building and Testing Secure Web Applications.....	4
SOA, Web Services, and XML Security.....	5
Secure Coding for Java EE.....	6
Network+ Certification.....	7
Security+ Certification.....	8
CISSP.....	9

**ITIL**

ITIL Foundations Certification v3.....	10
--	----

**NetApp**

Data ONTAP CIFS Administration (CIFS).....	11
Data ONTAP SAN Administration (SAN).....	12
Data ONTAP Fundamentals.....	13
Data ONTAP NFS Administration (NFS).....	14
Data Protection and Retention (DPR).....	15
MS Exchange on NetApp Storage Systems (MSEXC).....	16
Microsoft Clustering with SnapDrive (MSCLU).....	17
NCDA Boot Camp.....	18
Advanced NCDA Boot Camp (ANCDAB).....	19
Data ONTAP GX Fundamentals (DOTGX).....	20
Microsoft SQL Server 2005 on NetApp Storage Systems (MSSQL).....	21
Fundamentals of Performance Analysis (FPA).....	22

This Page Intentionally Left Blank

---

**Course Description:** This two-day class is for those who want to learn how to build a Snort IDS/IPS from scratch using many of the open source tools and plug-ins available to help manage, tune and deliver feedback on suspicious activity in your networks. Hands-on labs with fully documented instructions help students construct solid, secure Snort installations and understand the inner workings of the premier open source IDS/IPS available today. Students will also learn how to fine tune and configure Snort in addition to creating custom rules and learning techniques for optimizing rules.

**Who Should Attend:** Network Administrators, security administrators, security consultants and others that are responsible for deploying open source Intrusion Detection sensors in their organizations.

**Prerequisites:** This course assumes that students have a technical understanding of TCP/IP networking and network architecture. Proficiency with Linux and UNIX text editing tools (vi editor) is suggested, not required.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Build a Snort IDS/IPS from scratch
- Construct solid, secure Snort installations
- Understand the inner workings of the premier open source IDS/IPS available today.
- Fine tune and configure Snort

## Course Outline:

Introduction to Snort

Snort Architecture

Snort Sensor Deployment

Snort Installation

Snort Configuration and Operation

Snort Rules Primer

Snort Preprocessor Operation

Snort Tuning

Snort Output Processing

**Course Description:** This two-day class provides an in-depth look at Snort rules and Snort rules language syntax. Snort is the most widely used open source Intrusion Detection product. Learning how to take advantage of the power behind Snort rules can help security administrators write and configure highly effective rules. This class features extensive hands-on rules development and testing to reinforce the theoretical concepts that are presented.

**Who Should Attend:** Network Administrators, security administrators, security consultants and those that are responsible for deploying open source Intrusion Detection sensors in their organizations.

**Prerequisites:** This course assumes that students have a technical understanding of TCP/IP networking and network architecture. Proficiency with Linux and UNIX text editing tools (vi editor) is suggested, not required.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Write and configure highly effective rules
- Understand Snort rules and Snort rules language syntax

## Course Outline:

Introduction

Rule management

Variables

Anatomy of a Snort rule

Good rule writing practices

Using advanced rule syntax

Using PCRE in Snort Rules

Testing rules

Tuning rules

Rule & Preprocessor Profiling

**Course Description:** This three-day class covers the features and functionality of Sourcefire's 3D System including RNA, Intrusion Sensors, Defense Center and an overview of the Snort rules language. Users of Sourcefire products will learn to customize rules, troubleshoot, and write optimized rules with high performance while providing the highest levels of security.

**Who Should Attend:** Network administrators, security administrators, security consultants and others that are responsible for deploying and supporting Sourcefire's products are a must for this class.

**Prerequisites:** This course assumes that students have a technical understanding of TCP/IP networking and network architecture.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Customize rules
- Understand the Snort rules language

**Course Outline:**

Introduction

IDS/IPS &amp; RNA Technology Overview

Policy Management: Intrusion Sensor, RNA, and Compliance

Event Analysis &amp; Reporting

End-Point Intelligence

Flow Data Analysis

Nessus Scans

Rules and Rule Optimization

Rule Option Overview

Advanced Rule Options: Byte\_Test/Byte\_Jump &amp; PCRE

Rule Writing Best Practices and Troubleshooting

IDS/IPS &amp; RNA Technology Overview

3D Sensor Deployment and Network Architecture

Sourcefire 3D System Overview &amp; Product Installation

Basic Interface Navigation

Sensor Configuration and Management with the Defense Center

Configuring Interface Sets and Engine Instances

System Administration and Maintenance and Policy

**Course Description:** The course starts with a module that demonstrates just how insecure most web applications are. It demonstrates how hackers are able to attack web applications, and what common vulnerabilities they exploit. The next modules detail specific security areas, discussing the foundational principles and best practices, and review code examples of design patterns for solutions.

**Who Should Attend:** This course is for software and web application developers; Software, QA, and Security Testers; System and security administrators; Security engineers and managers; and individuals responsible for software requirements definition, procurement, or negotiations.

**Prerequisites:** Students should have basic IT skills, including using Windows and a browser. Students should have some exposure to web software and come ready to test. Minimal programming experience is required.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- employ the security features involved with using HTTP (e.g., headers, cookies, SSL);
- apply application security design principles;
- identify and explain common web application security threats and implement mitigation techniques;
- handle credentials securely while providing the full range of authentication support functions, including login, change password, forgot password, remember password, logout, re-authentication, and timeouts;
- implement access control rules for the user interface, business logic, and data layers;
- recognize potential input validation issues, particularly injection and Cross-site Scripting (XSS) problems, and implement appropriate input validation mechanisms for user input and other sources of input;
- understand the dangers of command injection and techniques for avoiding the introduction of this type vulnerability;
- implement a consistent error (exception) handling and logging approach for an entire web application;

**Course Outline:**

Authentication

Session Management

Access Control

Parameter Use

Cross Site Scripting

Buffer Overflows

Input Validation

Command Injection

SQL Injection

Using Databases Securely

Error Handling

Cryptography

Using Services Securely

Unnecessary and Malicious Code

Thread Safety

Denial of Service

Privacy and Legislative Compliance

Accountability and Logging

Caching, Pooling, and Reuse

Code Quality

Establishing Application Security Policy

Integrating Security into Your SDLC

**Course Description:** The movement towards Web Services and Service Oriented architecture (SOA) paradigms requires new security paradigms to deal with new risks posed by these architectures. This session takes a pragmatic approach towards identifying Web Services security risks and selecting and applying countermeasures to the application, code, web servers, databases, application, and identity servers and related software.

Many enterprises are currently developing new Web Services and/or adding and acquiring Web Services functionality into existing applications -- now is the time to build security into the system!

**Who Should Attend:** This course is for those people who want to understand the real risks in SOA, WebServices, and XML.

**Prerequisites:** Students should have a basic understanding of SOA, web services, and XML. In addition, students will benefit more from the course if they have completed a basic course in web application security.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Architect security services in Web Services and SOA
- Understand how an attacker looks at Web Services

**Course Outline:**

Web Services attack patterns

Common XML attack patterns

Data and XML security using WS-Security, SAML, XML Encryption and XML Digital Signature

Identifying services and federation with SAML and Liberty

Hardening Web Services servers

Input validation for Web Services

Integrating Web Services securely with backend resources and applications using WS-Trust

Secure Exception handling in Web Services

Understanding the impact of Web 2.0 technologies like Ajax, and REST on distributed systems security

**Course Description:** This course extends the Building and Testing Secure Web Applications course by adding a significant amount of Java specific content and exercises. Everything in the two-day version of the course is covered in this course. In addition, all language-specific content such as code examples, spot the bug exercises, and server specific recommendations have been translated to Java EE and its associated standard servers.

Three multistage hands-on Java programming labs have been added to this course. In these labs, the student not only finds flaws in a sample Java application, but then actually fixes the code using a Java IDE. They complete the lab stages by retesting to prove that they have fixed the target vulnerability for that stage.

**Who Should Attend:** This course is for JEE programmers and developers who want to provide secure coding for Java EE applications.

**Prerequisites:** Students should have experience with the design and implementation of Java EE applications. Familiarity with Eclipse is a plus but is not required.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- employ the security features involved with using HTTP (e.g., headers, cookies, SSL);
- apply application security design principles;
- identify and explain common web application security threats (e.g., cross-site scripting, SQL injection, denial of service attacks, "Man-in-the-middle" attacks, etc.) and implement mitigation techniques;
- handle credentials securely while providing the full range of authentication support functions, including login, change password, forgot password, remember password, logout, re-authentication, and timeouts;
- implement access control rules for the user interface, business logic, and data layers;
- recognize potential input validation issues, particularly injection and Cross-site Scripting (XSS) problems, and implement appropriate input validation mechanisms for user input and other sources of input;
- understand the dangers of command injection and techniques for avoiding the introduction of this type vulnerability;

## Course Outline:

Modules on XML and Web Services Security, including additional Web Services hands-on security testing labs

Numerous Spot the Bug Exercises are added where students are challenged to find real life security flaws in carefully constructed code samples

More in-depth discussion of topics from the 2-day course, including additional examples, code snippets, design patterns, and configuration recommendations

**Course Description:** Network+ Certification is a five-day class that prepares students to take the Network+ exam. Furthermore, the Network+ Certification can be the first step in achieving a Windows MCSE or CNE Certification.

**Who Should Attend:** This course is geared toward technicians with 18 to 24 months of experience in the IT industry who wish to earn their Network+ certification.

**Prerequisites:** An introductory course in a Windows operating system, or equivalent skills and knowledge, is required. CompTIA A+ certification, or the equivalent skills and knowledge, is helpful but not required.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Identify the basic components of network theory.
- Identify the major network communications methods.
- Identify network data delivery methods.
- List and describe network media and hardware components.
- Identify the major types of network implementations.
- Identify the components of a TCP/IP network implementation.
- List the major services deployed on TCP/IP networks.
- Identify characteristics of a variety of network protocols.
- Identify the components of a LAN implementation.
- Identify the components of a WAN implementation.
- Identify major issues and technologies in network security.
- Identify the components of a remote network implementation.
- Identify major issues and technologies in disaster recovery.
- Identify major data storage technologies and implementations.
- Identify the primary network operating systems.

### Course Outline:

#### Network Theory

Networking Terminology  
Network Building Blocks  
Standard Network Models  
Network Topologies  
Network Categories

#### Network Communications Methods

Transmission Methods  
Media Access Methods  
Signaling Methods

#### Network Data Delivery

Data Addressing and Delivery  
Network Connection Mechanisms  
Reliable Delivery Techniques

#### Network Media and Hardware

Bounded Network Media  
Unbounded Network Media  
Noise Control  
Network Connectivity Devices

#### Network Implementations

The OSI Model  
Client Network Resource Access  
Ethernet Networks  
Token Ring Networks  
Fiber Distributed Data Interface (FDDI) Networks  
Wireless Technologies and Standards

#### Networking with TCP/IP

Families of Protocols  
The TCP/IP Protocol  
Default IP Addresses  
Custom IP Addresses  
The TCP/IP Protocol Suite

#### TCP/IP Services

IP Address Assignment Methods  
Host Name Resolution  
NetBIOS Name Resolution  
TCP/IP Utilities  
TCP/IP Upper-layer Services  
TCP/IP Interoperability Services

#### Other Network Protocols

The NetBEUI Protocol  
The IPX/SPX Protocol  
The AppleTalk Protocol  
The IP Version 6 (IPv6) Protocol

#### Local Area Network (LAN) Infrastructure

Bridges and Switches

IP Routing Topology  
Static IP Routing  
Dynamic IP Routing  
Controlling Data Movement with Filters and VLANs

#### Wide Area Network (WAN) Infrastructure

WAN Switching Technologies  
WAN Transmission Technologies  
WAN Connectivity Methods  
Voice Over Data Systems

#### Network Security

Network Threats  
Virus Protection  
Local Security  
Network Authentication Methods  
Data Encryption  
Internet Security

#### Remote Networking

Remote Network Architectures  
Terminal Services Implementations  
Remote Access Networking Implementations  
Virtual Private Networking (VPN)

#### Disaster Recovery

Planning for Disaster Recovery  
Data Backup  
Fault Tolerance Methods

#### Network Data Storage

Enterprise Data Storage Techniques  
Clustering  
Network Attached Storage (NAS)  
Storage Area Network (SAN) Implementations

#### Network Operating Systems

Microsoft Operating Systems  
Novell NetWare  
UNIX and Linux Operating Systems  
Macintosh Networking

#### Network Troubleshooting

Troubleshooting Models  
TCP/IP Troubleshooting Utilities  
Hardware Troubleshooting Tools  
System Monitoring Tools  
Network Baselining

**Course Description:** Security+™ A CompTIA Certification is the primary course you will need to take if your job responsibilities include securing network services, network devices, and network traffic. It is also the main course you will take to prepare for the CompTIA Security+ examination (exam number SY0-101). In this course, you'll build on your knowledge and professional experience with computer hardware, operating systems, and networks as you acquire the specific skills required to implement basic security services on any type of computer network.

**Who Should Attend:** This course is targeted toward an Information Technology (IT) professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as NetWare, Macintosh, UNIX/Linux, and OS/2, who wants to: further a career in IT by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ Certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

**Prerequisites:** Students should have CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP. Although not required, students might find it helpful to obtain foundational information from introductory operating system administration courses.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Identify security threats.
- Harden internal systems and services.
- Harden internetwork devices and services.
- Secure network communications.
- Manage a PKI.
- Manage certificates.

### Course Outline:

#### Identifying Security Threats

Identify Social Engineering Attacks  
Classify Software Attacks  
Identify Hardware Attacks

#### Hardening Internal Systems and Services

Harden Base Operating Systems  
Harden Directory Services  
Harden DHCP Servers  
Harden Network File and Print Servers

#### Hardening Internetwork Devices and Services

Harden Internetwork Connection Devices  
Harden DNS and BIND Servers  
Harden Web Servers  
Harden FTP Servers  
Harden Network News Transport Protocol (NNTP) Servers  
Harden Email Servers  
Harden Conferencing and Messaging Servers

#### Securing Network Communications

Secure Network Traffic Using IP Security (IPSec)  
Secure Wireless Traffic  
Secure Client Internet Access  
Secure the Remote Access Channel

#### Managing Public Key Infrastructure (PKI)

Install a Certificate Authority (CA) Hierarchy  
Harden a Certificate Authority  
Back Up Certificate Authorities  
Restore a Certificate Authority

#### Managing Certificates

Enroll Certificates for Entities  
Secure Network Traffic Using Certificates  
Renew Certificates  
Revoke Certificates  
Back Up Certificates and Private Keys  
Restore Certificates and Private Keys

#### Enforcing Organizational Security Policy

Enforce Corporate Security Policy Compliance  
Enforce Legal Compliance  
Enforce Physical Security Compliance  
Educate Users

#### Monitoring the Security Infrastructure

Scan for Vulnerabilities  
Monitor for Intruders  
Set Up a Honeypot  
Respond to Security Incidents

**Course Description:** This course trains students in all areas of the security Common Body of Knowledge. They will learn security policy development, secure software development procedures, network vulnerabilities, attack types and corresponding countermeasures, cryptography concepts and their uses, disaster recovery plans and procedures, risk analysis, crucial laws and regulations, forensics basics, computer crime investigation procedures, physical security, and more.

**Who Should Attend:** Students who wish to pass the CISSP certification exam will benefit from this class.

**Prerequisites:** There are no prerequisites for this course, although having taken other security courses is extremely helpful.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Confidently meet the challenge of CISSP certification exam

### Course Outline:

#### Access Control Systems and Methodologies

Access control concepts, methodologies, and implementation  
 Access controls: detective, corrective, and preventative  
 Access control techniques in centralized and decentralized environments  
 Access control risks, vulnerabilities, and exposures

#### Security Architecture and Models

Secure operating system principles, concepts, mechanisms, controls, and standards  
 Secure architecture design, modeling, and protection  
 Security models: confidentiality, integrity, and information flow  
 Government and commercial security requirements  
 Common criteria, ITSEC, TCSEC, IETF, IPSEC  
 Technical platforms  
 System security preventative, detective, and corrective measures

#### Disaster Recovery and Business Continuity Planning

Business continuity planning, business impact analysis, recovery strategies, recovery plan development, and implementation  
 Disaster recovery planning, implementation, and restoration  
 Compare and contrast disaster recovery and business continuity

#### Security Management Practices

Organizational security roles  
 Identification of information assets  
 Security management planning  
 Security policy development; use of guidelines, standards, and procedures  
 Security awareness training  
 Data classification and marking  
 Employment agreements and practices  
 Risk management tools and techniques

#### Law, Investigation, and Ethics

Computer crime detection methods  
 Applicable computer crime, security, and privacy laws  
 Evidence gathering and preservation methods  
 Computer crime investigation methods and techniques  
 Civil, criminal, and investigative law  
 Intellectual property law  
 ISC2 and IAB ethics application

#### Physical Security

Prevention, detection, and correction of physical hazards  
 Secure site design, configuration, and selection elements  
 Access control and protection methods for facility, information, equipment, and personnel

#### Operations Security

Resource protection mechanisms and techniques  
 Operation security principles, techniques, and mechanisms; principles of good practice and limitation of abuses  
 Operations security preventative, detective, and corrective measures  
 Information attacks  
 Access Control Subversion

#### Cryptography

Cryptographic concepts, methods, and practices  
 Construction of algorithms  
 Attacks on cryptosystems  
 Ancient cryptography and modern methods  
 Public and private key algorithms and uses  
 Key distribution and key management  
 Digital signature construction and use

Methods of attack, strength of function

#### Telecommunications and Network Security

Overview of communications and network security  
 Voice communications, data communications, local area, wide area, and remote access  
 Internet/Intranet/Extranet, firewalls, routers, and network protocols  
 Telecommunication and network security preventative, detective, and corrective measures  
 System development process and security controls  
 System development life cycle, change controls, application controls, and system and application integrity  
 Database structure, concepts, design techniques, and security implications  
 Object oriented programming  
 Data warehousing and data mining

#### Review and Q&A Session

Review concepts introduced in previous sessions  
 Answer specific questions or concerns regarding CISSP preparation material

#### Testing-Taking Tips and Study Techniques

Tips for additional preparation for the CISSP exam  
 Additional resources  
 Techniques for scoring well on the exam

**Course Description:** This course provides IT Managers and Practitioners with a practical understanding of IT Service Management, the underpinning core ITIL Service Delivery and Service Support Processes and implementation guidance. It describes a set of processes involved in developing an IT framework and features both lecture and interactive hands-on learning experience throughout the course. This results in a thorough grounding in the basic theory of ITSM, which can be used to take the Foundation Certificate in IT Service Management, or to participate in ITSM projects at any level. The ITIL Foundations Certification Exam is administered at the end of the course.

**Who Should Attend:** IT Management, Business Unit Managers, IT Services Managers, Supplier Managers, Consultants and those responsible for the support and implementation of Information Technology will benefit from this course.

**Prerequisites:** Familiarity with IT Services is recommended.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Identify the Key ITIL processes
- Identify the Benefits of implementing each ITIL process in an organization
- Identify the Basic concepts related to each ITIL process
- Identify the Activities and roles involved in each process
- Identify the Relationship of each ITIL process to other processes

### Course Outline:

Introduction to ITSM/ ITIL

Configuration Management - with Exercise

Service Desk

Incident Management

Problem Management

Change Management - with Case Study

Release Management

"I am the Incident" Exercise

Service Level Management - with Exercise

Availability Management - with Case Study

Capacity Management - with Case Study

IT Service Continuity Management

Security Management

Financial Management

Wrap Up / Review of Sample Exam

Exam Preparation Module

ITIL Foundation Exam

**Course Description:** This course teaches Data ONTAP CIFS Administration (CIFS).

**Who Should Attend:** This course is for network professionals who need to perform in-depth support, administrative functions, and performance management for CIFS protocol on a NetApp storage appliance running the Data ONTAP operating system.

**Prerequisites:** Students should have taken Data ONTAP Fundamentals.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Explain and identify common components of the Common Internet File System (CIFS)
- Create, configure, and manage CIFS shares, groups, and permissions
- Implement auto home share on the filer/DC
- Describe and implement event and file auditing procedures
- Describe On Access Virus Scanning and configuration for sample implementation
- Appraise an organization's quota requirements and design an appropriate configuration
- Apply basic concepts for moving and restoring ACLs
- Measure and graph CIFS performance using smb\_hist and sysstat commands
- Review & identify potential performance issues given Storage Appliance statistics
- Check network-related performance statistics and identify possible courses of action
- Collect data to assist with troubleshooting hardware, operating systems, and applications

### Course Outline:

Explain and identify common components of the Common Internet File System (CIFS)

Create, configure, and manage CIFS shares, groups, and permissions

Implement auto home share on the filer/DC

Describe and implement event and file auditing procedures

Describe On Access Virus Scanning and configuration for sample implementation

Appraise an organization's quota requirements and design an appropriate configuration

Apply basic concepts for moving and restoring ACLs

Measure and graph CIFS performance using smb\_hist and sysstat commands

Review & identify potential performance issues given Storage Appliance statistics

Check network-related performance statistics and identify possible courses of action

Collect data to assist with troubleshooting hardware, operating systems, and applications

Investigate, identify, troubleshoot, and implement solutions in a CIFS environment

**Course Description:** In this course, students will learn Data ONTAP SAN Administration (SAN).

**Who Should Attend:** This course is for network professionals who perform in-depth support, administrative functions, and performance management for FCP for SCSI or iSCSI for TCP/IP protocol on a NetApp storage appliance running the Data ONTAP operating system.

**Prerequisites:** Students should have taken Data ONTAP Fundamentals.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Identify concepts, commands and procedures for using the UNIX operating system as part of creating and mounting file systems using UFS LUNs on a NetApp storage appliance
- Identify concepts, commands and procedures for using Windows operating system as part of creating and accessing LUNs on a NetApp storage appliance
- Configure the appropriate cmode for an FCP for SCSI environment
- Locate documentation and identify systems and procedures for booting a host from a LUN
- Create and manage LUNs with SnapDrive for Windows
- Perform administration tasks for LUNs on a NetApp storage appliance
- Diagram and describe the implementation of a LUN on a NetApp storage appliance

### Course Outline:

Identifying concepts, commands and procedures for using the UNIX operating system

Creating and mounting file systems using UFS LUNs on a NetApp storage appliance

Identifying concepts, commands and procedures for using Windows operating system

Creating and accessing LUNs on a NetApp storage appliance

Configuring the appropriate cmode for an FCP for SCSI environment

Locating documentation and identifying systems and procedures for booting a host from a LUN

Creating and managing LUNs with SnapDrive for Windows

Performing administration tasks for LUNs on a NetApp storage appliance

Diagramming and describing the implementation of a LUN on a NetApp storage appliance

Configuring a simple SAN using a Brocade SilkWorm 2Gbps switch with a clustered NetApp storage appliance and SUN Solaris or Microsoft Windows 2000

Verifying HBA drivers and firmware for FCP for SCSI and iSCSI for TCP/IP protocols

Managing and viewing HBAs and LUNs using a SUN or Windows host

Using the sio\_ntap utility as well as NetApp storage appliance commands to gather data for performance and problem analysis

Collecting data to assist with troubleshooting hardware, operating systems and applications

Identify problem isolation problems

**Course Description:** This course teaches students the fundamentals of Data ONTAP.

**Who Should Attend:** This course is for Network Professionals who perform basic support and administrative functions on a NetApp storage appliance running the Data ONTAP operating system.

**Prerequisites:** Students should have taken Introduction to NetApp Products Web Based Training, have basic knowledge of client/server and networking terminology and management including TCP/IP, and have a background in one of the following: UNIX, Windows, or SAN system.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Explain the primary function of a storage appliance
- Use a storage appliance console to access and execute commands
- Determine a storage appliance's system configuration
- Manage a storage appliance's configuration files from an adminhost
- Setup aggregates and volumes and set volume specific options
- Identify the physical interfaces used by a storage appliance
- Configure physical interface parameters on a storage appliance
- Configure the virtual interfaces (VLANs and VIFs)
- Export a storage appliance's volumes to a host
- Mount the exported file system from a host

### Course Outline:

Primary function of a storage appliance

Using a storage appliance console to access and execute commands

Storage appliance's system configuration

Storage appliance's configuration files from an adminhost

Setup aggregates and volumes and set volume specific options

Physical interfaces used by a storage appliance

Physical interface parameters on a storage appliance

Virtual interfaces (VLANs and VIFs)

Storage appliance's volumes to a host

Upgrading Data ONTAP via NFS, CIFS or HTTP

Joining a storage appliance into a Windows 2000 domain using CIFS

Qtrees

Filers and new file systems

Licenses

System files

Set the Snapshot schedule on a storage appliance

Restore a deleted file from the .snapshot directory

Create the /etc/quotas file

Restrict disk space using quotas

Backup a volume using a storage appliance's native dump command

Backup a qtree using a storage appliance's native dump command

Restoring a volume

Restoring a qtree

NDMP services on a storage appliance

Volume and aggregate copy on a storage appliance

The admin privilege commands

statit command

Storage Appliance's optional settings

**Course Description:** This course will teach students how to perform in-depth support, administrative functions, and performance management for the NFS protocol on a NetApp® storage appliance running the Data ONTAP operating system.

**Who Should Attend:** This course is for Network Professionals.

**Prerequisites:** Students should have taken the Data ONTAP Fundamentals course.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Explain the storage appliance NFS concept and components.
- Describe the configuration requirements for NFS.
- State the rules for exporting resources to hosts, subnets, and netgroups.
- Explain the /etc/exports access options and how they relate to mount permissions.
- Analyze NFS performance using sysstat and nfsstat commands.
- Check network-related performance statistics and identify possible courses of action.
- Collect data to assist with troubleshooting hardware, operating system, and applications.

### Course Outline:

Storage appliance NFS concept and components

Configuration requirements for NFS

Rules for exporting resources to hosts, subnets, and netgroups

/etc/exports access options and mount permissions

NFS performance using sysstat and nfsstat commands

Network-related performance statistics and possible courses of action

Collecting data to assist with troubleshooting hardware, operating system, and applications

Problem resolution techniques in a storage appliance environment

Storage appliance hardware  
Data ONTAP operating system  
Networking interfaces  
NFS configuration files and options  
RAID and RAID-DP volumes

**Course Description:** This instructor-led course will teach students how to manage mission critical data in the enterprise. Basic NDMP skills for data archive are presented. A mixture of lecture and hands-on activities teach concepts and techniques needed to effectively use these solutions.

**Who Should Attend:** This course is for administrators and support personnel who will use the SnapMirror®, SnapRestore®, SnapVault™, OSSV™, SnapLock™, and LockVault™ to manage mission critical data.

**Prerequisites:** Students should have taken the Data ONTAP Fundamentals course.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Explain the concept of Information Lifecycle Management (ILM).
- Set up and maintain snapshots.
- Plan and perform data recovery using SnapRestore.
- Configure and administer Asynchronous and Synchronous SnapMirror.
- Configure and administer SnapVault.
- Configure and administer OSSV.
- List best practices and perform troubleshooting of SnapMirror, SnapVault and OSSV.
- Use NDMP to archive data.

### Course Outline:

Overview and Components

Snapshot Review

SnapRestore

SnapMirror

SnapVault

OSSV

Best Practices and Troubleshooting

NDMP Fundamentals

SnapLock

**Course Description:** This solution-based course focuses on the optimization of Microsoft Exchange in a NetApp storage environment. This course takes students through the entire systems integration process of architecture planning, data migration, backup and restore, disaster recovery, and troubleshooting.

**Who Should Attend:** Windows and Exchange administrators will benefit from this course.

**Prerequisites:** Students should have taken the following courses: Data Protection Solutions (DPS), Implementing and Managing Microsoft Exchange Server 2003, and Troubleshooting Microsoft® Exchange Server 2003.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Understand optimization of Microsoft Exchange in a NetApp storage environment.

**Course Outline:**

Solution Overview

MS Exchange Storage Internals

Architecture, Planning, Provisioning

Implementation and Migration

Backup and Restore using SnapManager

Disaster Recovery Scenarios

Troubleshooting

**Course Description:** This intermediate level, hands-on course introduces students to clustering Microsoft servers with SnapDrive. This course also introduces students to implementing MS Exchange and MS SQL on a MS Cluster

**Who Should Attend:** Windows, Exchange and SQL Server administrators will benefit from this course.

**Prerequisites:** Students should have take High Availability (HA) Boot Camp.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Illustrate how MS Clustering works and discuss its benefits.
- Establish MS Cluster with a SnapDrive-created iSCSI Quorum disk.
- Demonstrate, maintain, and troubleshoot a MS Cluster.
- Install MS Exchange on a MS Cluster.
- Demonstrate, maintain, and troubleshoot MS Exchange on a MS Cluster.
- Install MS SQL on a MS Cluster.

**Course Outline:**

MS Clustering Overview and filer CFO Review

Establish MS Cluster

Setup MS Exchange on MS Cluster

Setup MS SQL on MS Cluster

**Course Description:** This 10-day intensive, hands-on boot camp will prepare students for the four required NetApp exams to achieve NCDA certification. Students will be provided with all four test vouchers as well as one extra voucher per exam, as needed.

**Who Should Attend:** Network Professionals seeking NACP or NACE Certification should attend. This course is also valuable for those who need to perform in-depth support, administrative functions, and performance management for CIFS protocol, FCP for SCSI or iSCSI for TCP/IP protocol, NFS, or DPS protocol on a NetApp® storage appliance running the Data ONTAP operating system.

**Prerequisites:** Students should have taken Data ONTAP Fundamentals.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Create, configure, and manage CIFS shares, groups, and permissions
- Implement auto home share on the filer/DC
- Describe and implement event and file auditing procedures
- Describe On Access Virus Scanning and configuration for sample implementation
- Appraise an organization's quota requirements and design an appropriate configuration
- Apply basic concepts for moving and restoring ACLs
- Measure and graph CIFS performance using smb\_hist and sysstat commands
- Review & identify potential performance issues given Storage Appliance statistics
- Check network-related performance statistics and identify possible courses of action
- Collect data to assist with troubleshooting hardware, operating systems, and applications

### Course Outline:

CIFS shares, groups, and permissions

Auto home share on the filer/DC

Event and file auditing procedures

On Access Virus Scanning and configuration

Quota requirements and design an appropriate configuration

Basic concepts for moving and restoring ACLs

Measuring and graphing CIFS performance using smb\_hist and sysstat commands

Potential performance issues given Storage Appliance statistics

Network-related performance statistics and identify possible courses of action

Troubleshooting hardware, operating systems, and applications

Solutions in a CIFS environment

Configuration requirements for NFS

Rules for exporting resources to hosts, subnets, and netgroups

/etc/exports access options and how they relate to mount permissions

NFS performance using sysstat and nfsstat commands

Network-related performance statistics and identify possible courses of action

Problem resolution techniques in a storage appliance environment

Performance characteristics with NetApp data protection solutions

Data protection problems

**Course Description:** This 5-day intensive, hands-on advanced boot camp will prepare you for all required NetApp exams to achieve the NCDA certification, assuming you have met the prerequisites. You will be provided with two test vouchers to use to sit the two exams required for the NCDA certification. Should you not pass an exam, we will provide you with one extra voucher to retake an exam.

**Who Should Attend:** Network Professionals seeking the NCDA certification. This course is also valuable for those who need to perform in-depth support, administrative functions, and performance management for environments using any of the following enterprise storage solutions: CIFS, NFS, FCP, iSCSI protocols on a NetApp storage appliance running the Data ONTAP operating system.

**Prerequisites:** Students should have taken the Data ONTAP Fundamentals course.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Describe the different server environments
- Identify the appropriate server environment for your storage system
- Configure the CIFS environment on a storage system
- Administer a storage system in a CIFS environment
- Explain how to troubleshoot basic CIFS problems
- Explain NFS protocol overview, NFS versions, and NFS Implementation criteria
- Configure and administer client and server in an NFS environment
- State the rules for exporting resources to hosts, subnets, and netgroups
- Explain the /etc/ exports access options and how they relate to mount permissions
- Analyze NFS performance using sysstat, nfsstat, and other commands

### Course Outline:

Server environments	High Availability and Network Appliance solutions
Configuring the CIFS environment on a storage system	SyncMirror aggregate
Administering a storage system in a CIFS environment	Best practices when deploying active-active configurations
Troubleshooting basic CIFS problems	MetroCluster
NFS protocol overview, NFS versions, and NFS Implementation criteria	SyncMirror
Configuring and administering client and server in an NFS environment	
Rules for exporting resources	
/etc/ exports access options	
Analyzing NFS performance	
Collecting and analyzing data	
Characteristics of a SAN environment	
Components of FC and IP SANs	
Size planning requirements for LUNs	
Creating and managing LUNs on a storage controller	
FC and IP SAN multipathing options	
Troubleshooting common SAN issues	
Information Lifecycle Management (ILM)	
Snapshots	
Data recovery using SnapRestore	
Asynchronous and Synchronous SnapMirror	
SnapVault	
Configuring and administering OSSV	
Best practices	
Troubleshooting of SnapMirror, SnapVault and OSSV	
Using NDMP to archive data	
SnapLock and LockVault	

**Course Description:** The Data ONTAP GX Fundamentals course is a comprehensive, though not exhaustive, learning object designed to teach the basics of Data ONTAP GX.

At the end of this course, the student will know the evolution of Data ONTAP GX, dating back to the 1980s, understand the benefits of this product, be able to explain the architecture and functionality of the product, and be able to install, configure, manage, and troubleshoot Data ONTAP GX clusters

**Who Should Attend:** This instructor led course is for customers who perform basic support and administrative functions on a NetApp® storage system running the Data ONTAP GX operating system software.

**Prerequisites:** Students should have taken Data ONTAP Fundamentals (DOTF) or Data ONTAP Overview.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Describe the major principles associated with Data ONTAP GX
- Describe how an N-blade and a D-blade interact with each other
- Describe how a replicated database (RDB) application communicates among the members in its ring
- Describe the difference between an mroot volume and a virtual server root volume
- Create a cluster made up of multiple nodes
- Create an aggregate
- Create two virtual servers, two additional volumes in each, and two three-volume name spaces
- Configure an active-active relationship between a pair of nodes
- Configure network interfaces for a virtual server
- Create an NFS export and a CIFS share

### Course Outline:

Major principles associated with Data ONTAP GX

N-blade and a D-blade interactions

Replicated database (RDB) application communication

Difference between an mroot volume and a virtual server root volume

Clusters made up of multiple nodes

Aggregates

Virtual servers, additional volumes, and two three-volume name spaces

Active-active relationships between pairs of nodes

Network interfaces for a virtual server

NFS export and CIFS share

Moving a volume from one node to another

SnapShot policy for a volume

Load sharing (LS) mirrors

Disaster recovery (DR) mirrors

Promoting a mirror to be a read-write volume

Diagnosing a VLDB crash and recovering from it

Upgrading the CFE (firmware) on a node

Upgrading the Data ONTAP GX software on two nodes with no down time

**Course Description:** This solution-based course focuses on the optimization of Microsoft SQL Server 2005 in a NetApp storage environment. This course takes students through the entire systems integration process of architecture planning, data migration, backup and restore, disaster recovery, and troubleshooting.

**Who Should Attend:** Network Professionals who need to have a working understanding of Microsoft SQL Server 2005 on a NetApp Storage System will benefit from this course.

**Prerequisites:** Students should have taken Data ONTAP Fundamentals, Data Protection and Retention, and Data ONTAP SAN Administration. They must have at least one of the following: Microsoft Course 2072, Microsoft exam 70-228, or one year Microsoft SQL Server 2005 experience.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Describe the benefits of running SQL Server 2005 on a NetApp Storage System
- Perform SQL Server 2005 storage planning, implementation, and administration
- Architect a high performance, highly available, consolidated SQL Server solution on a NetApp Storage System
- Deploy SQL Server 2005 on a NetApp Storage System
- Describe the SQL Server 2005 backup and restore process using SnapManager
- Determine the correct NetApp Storage Controller model, volume size, and LUN size to support the solution
- Back up and verify a SQL Server 2005 database using SnapManager.
- Restore data using SnapManager

### Course Outline:

Roles and functionality of the various components in a SQL Server 2005 solution

Various dependencies of each component in a SQL Server 2005 Solution

Storage solutions

Installing multiple instances of Microsoft SQL Server

Configuring an IP SAN

Configuring the Storage Controller and Windows host for Microsoft SQL Server

Installing SnapDrive

Installing SnapManager for SQL Server

Creating and managing qtrees and LUNs

Performing and testing a database migration

Performing full database backups

Performing a concurrent backup of multiple databases

Transaction log backups

Local and remote database verification

Backup management groups in backup and verification

Deleting backup Snapshot copies

SnapManager

Restoring a database to an alternate location

Creating, configuring, and testing a backup schedule

Common faults in SnapDrive and SnapManager for SQL Server and Microsoft SQL Server

Implementing NetApp supported and recommended Disaster Recovery methods

Integration of secondary storage as a D/R technique

Backup archiving

Roles of NetApp CFO and Microsoft MSCS in a High Availability configuration

**Course Description:** The Fundamentals of Performance Analysis course provides students with the knowledge and skills to perform data collection and analysis on NetApp storage systems. The student learns how to interpret the data and apply performance changes based on their analysis. The student will use data for tuning, monitoring, and other performance related areas.

**Who Should Attend:** This class is for students who want to perform data collection and analysis on NetApp storage systems.

**Prerequisites:** Students must have taken Introduction to NetApp products and Data ONTAP Fundamentals and have three months of experience with NetApp hardware and software products. It is recommended, but not required, that students have taken NetApp Hardware Fundamentals and FAS3000 Series Hardware Maintenance courses.

**Benefits of Attendance:** Upon completion of this course, students will be able to:

- Recognize performance terminology and basic methodology
- Describe how Data ONTAP reads and writes data to disks
- Diagram how data flows through Data ONTAP components
- Use knowledge about how data flows through the network and protocol layers of Data ONTAP to monitor and analyze storage system performance
- Use Data ONTAP tools and NetApp provided scripts to identify networking disk I/O, Fibre Channel loop saturation and CPU bottlenecks
- Use the reallocation command to optimize disk performance
- Utilize both client and storage system tools to monitor and analyze a performance problem

### Course Outline:

NetApp Technology Overview

Software Architecture

Performance Monitoring and Analysis

Implementing Growth Management Techniques for Performance

Performance Tuning and Best Practices