ONStor Cougar 6000 Series
NAS Gateway Installation Guide

Customer Order Number: ONS-DOC-IG-6000, Rev A1
Text Part Number: 690-0024-0001A1

ONStor, Inc.
254 East Hacienda Ave.
Campbell, CA USA 95008
(408) 963-2400

Revised May 13, 2008 7:19 am
Beta Version

Contents

Chapter 1: Safety Information

This chapter contains the following sections:

Safety Information

This section details the safety considerations when installing, operating, and performing maintenance on this product.

The following sections contain the following topics:

- Heat Considerations
- Equipment Weight Considerations
- Electrostatic Discharge Considerations
- Power Cords
- Grounding
- Lithium Battery
- Optical Considerations

Choose the appropriate language:

Safety Considerations

It is recommend that you read and follow the safety considerations listed in these sections before beginning any procedure.

Warning - Failure to follow the information in the following sections can result in damage to the product, personal injury, or loss of life.

Heat Considerations

To reduce the risk of personal injury from hot surfaces, whenever you are working inside the chassis or with components that have been removed from the chassis, allow sufficient time for the components to cool before touching them.

Equipment Weight Consideration

Warning - 18 kg to 32 kg (39.7 lbs to 70.5 lbs). Two persons are required to safely lift product.

Electrostatic Discharge Considerations

Caution - This product contains electronic components that are sensitive to electrostatic discharge (ESD). To avoid damage to the product or its components, ensure that you are using an appropriate method of ESD protection prior to handling any part of the product.

Also, when removing any part of the product, ensure that you set them on an ESD safe work surface.

Power Cords

Warning - This product might have multiple power supply cords. To reduce the risk of electrical shock, disconnect all power supply cords before servicing the unit.

Grounding

This equipment is designed for connection to a grounded outlet. To avoid the risk of electrical shock or damage to the product, do not plug into any other type of outlet.

Lithium Battery

Warning - This product contains one or more lithium batteries. If the battery is misused, damaged, or incorrectly installed or replaced, the danger of explosion exists. To avoid personal injury or damage to the product, do not attempt to recharge the battery, disassemble it, or dispose of it in a fire. Ensure that you dispose of the battery properly.

Optical Considerations

This product has fiber optic connections. The optical transceivers comply with Class 1 laser requirements.

Eye Safety

Warning - To reduce the risk of personal injury, avoid pointing the NAS Gateway's laser directly into your eye.

The laser signal supported on the optical transceivers have been categorized as a Class 1 laser. Per the IEC 825-1: EN-60825-1 and FDA CDRH CFR title 21 Class 1 laser do not pose a risk under normal operating conditions.

Misuse of the laser or prolonged exposure to a human has the possibility of causing personal injury.

Consideraciones de seguridad

Le recomendamos que lea y siga las siguientes consideraciones de seguridad que aparecen en estas secciones antes de iniciar cualquier procedimiento.

Advertencia - El hecho de no cumplir con la información que se presenta en las siguientes secciones puede dar como resultado daño al producto, lesiones personales o la pérdida de la vida.

Consideraciones de calor

Para reducir el riesgo de lesiones personales debido al contacto con superficies calientes, siempre que trabaje dentro de un chasis o con componentes que hayan sido removidos del chasis, permita tiempo suficiente para que los componentes se enfríen antes de tocarlos.

Consideraciones del peso del equipo

Advertencia - 18 kg a 32 kg (39.7 lbs a 70.5 lbs). Se requieren dos personas para levantar el producto de manera segura.

Consideraciones de descargas electrostáticas

Precaución - Este producto contiene componentes electrónicos que son sensibles a descargas electrostáticas (ESD). Para evitar el daño al producto o a sus componentes, asegúrese de utilizar el método adecuado de protección ESD antes de manejar cualquier parte del producto.

Además, al quitar cualquier parte del producto, asegúrese de colocarla en una superficie de trabajo segura para ESD.

Cables de suministro de energía

Advertencia - Este producto puede tener varios cables de suministro de energía. Para reducir el riesgo de choque eléctrico, desconecte todos los cables de suministro de energía antes de dar servicio a la unidad.

Conexión a tierra

Este equipo está diseñado para su conexión a un toma corriente aterrizado. Para evitar el riesgo de choque eléctrico o daño al producto, no lo conecte a otro tipo de toma corriente.

Batería de litio

Advertencia - Este producto contiene una o más baterías de litio. Si la batería se usa en forma equivocada, se daña o se instala o reemplaza en forma incorrecta, se puede generar el riesgo de explosión. Para evitar lesiones personales o daños al producto, no intente recargar la batería, desensamblarla o disponer de ella en el fuego. Asegúrese de disponer de la batería en forma adecuada.

Consideraciones ópticas

Este producto cuenta con conexiones de fibra óptica. Los transmisores y receptores ópticos cumplen con los requisitos láser Clase 1.

Seguridad ocular

Advertencia - Para reducir el riesgo de lesiones personales, evite apuntar el láser de NAS Gateway a su ojo.

Las señales laser que soportan los transmisores y receptores ópticos son de la categoría de láser Clase 1. Conforme a la norma IEC 825-1: EN-60825-1 y FDA CDRH CFR titulo 21 el láser Clase 1 no presenta ningún riesgo bajo condiciones normales de operación.

El mal uso del láser o una exposición prolongada a un ser humano puede causar lesiones personales.

Considérations de sécurité

Nous vous recommandons de lire et d'observer les considérations de sécurité portées dans ces sections avant toute intervention.

Danger - L'inobservation des informations contenues dans les sections suivantes peut être cause d'endommagement du produit, de lésion corporelle ou de mort.

Considérations thermiques

En cas d'intervention à l'intérieur du châssis ou sur des composants qui ont été retirés du châssis, laisser les composants refroidir suffisamment avant de les toucher pour réduire le risque de lésion corporelle résultant du contact avec les surfaces chaudes.

Considération de masse de l'équipement

Danger - Masse 18-32 kg (39.7-70.5 lbs). Deux personnes sont requises pour soulever le produit en sécurité.

Considérations relatives aux décharges électrostatiques

Attention - Ce produit contient des composants électroniques sensibles aux décharges électrostatiques (DES). Pour éviter d'endommager le produit ou ses composants, veiller à utiliser une méthode de protection contre les DES avant de manipuler toute partie du produit.

De même, veiller à poser tout élément retiré du produit sur une surface de travail protégée contre les DES.

Cordons d'alimentation

Danger - Ce produit peut comporter de multiples cordons d'alimentation électrique. Pour diminuer le risque de choc électrique, débrancher tous les cordons d'alimentation électrique avant d'intervenir sur l'appareil.

Mise à la terre

Cet équipement doit être raccordé à une prise de terre. Pour éviter le risque de choc électrique ou d'endommagement du produit, ne pas le raccorder à tout autre type de prise.

Batterie au lithium

Danger - Ce produit contient une ou plusieurs batteries au lithium. Il y a risque d'explosion en cas de mauvais usage, d'endommagement, d'installation défectueuse ou de remplacement de la batterie. Pour éviter toute lésion corporelle ou endommagement du produit, ne pas tenter de recharger, démonter ou jeter la batterie au feu. Veiller à éliminer la batterie dans les règles.

Considérations optiques

Ce produit comporte des connexions à fibres optiques. Les émetteurs-récepteurs optiques sont conformes aux prescriptions laser Classe 1.

Sécurité oculaire

Danger - Éviter de pointer le laser de la passerelle NAS directement dans les yeux pour réduire le risque de lésion corporelle.

Le signal laser exploité sur les émetteurs-récepteurs optiques sont classés laser Classe 1. Selon les normes CEI 825-1: EN-60825-1 et FDA CDRH CFR title 21, le laser Classe 1 est sans risque dans les conditions normales de fonctionnement.

Le mauvais usage du laser ou l'exposition humaine prolongée présentent toutefois une possibilité de lésion corporelle.

Sicherheitsmaßnahmen

Wir empfehlen, dass Sie die in diesen Abschnitten aufgelisteten Sicherheitsmaßnahmen vor Beginn jedes Vorgangs lesen und befolgen.

Warnung - wenn Sie den Hinweisen in den folgenden Abschnitten nicht Folge leisten, kann das zur Beschädigung des Produktes, zu Personenschaden oder zu Lebensgefahr führen.

Beachtung von Hitze

Um das Risiko von Personenschaden aufgrund heißer Oberflächen zu reduzieren, achten Sie auf ausreichend Zeit, in der sich die Bauteile abkühlen können, bevor Sie sie berühren, wann immer Sie innerhalb des Gehäuses oder mit Komponenten arbeiten, die aus dem Gehäuse entfernt wurden.

Beachtung des Gerätegewichts

Warnung - 18 kg bis 32 kg (39.7 lbs bis 70.5 lbs). Zwei Personen sind erforderlich, um das Produkt sicher anzuheben.

Beachtung von elektrostatischer Entladung

Achtung - Dieses Produkt enthält elektronische Bauteile, die empfindlich auf elektrostatische Entladung (ESD) reagieren. Um eine Beschädigung des Produkts oder seiner Bauteile zu vermeiden, stellen Sie sicher, dass Sie ein entsprechendes Verfahren für den Schutz vor elektrostatischer Entladung benutzen, bevor Sie irgendeinen Teil des Produktes bedienen.

Auch wenn Sie irgendeinen Teil des Produkts entfernen, stellen Sie sicher, dass Sie die Teile auf einer Oberfläche ablegen, die gegen elektrostatische Entladung geschützt ist.

Stromkabel

Warnung - Dieses Produkt könnte mehrere Kabel zur Stromzufuhr besitzen. Um das Risiko eines elektrischen Schlags zu vermeiden, entfernen Sie vor jeder Instandhaltung des Geräts alle Stromkabel aus den Steckern.

Erdung

Dieses Gerät ist für eine Verbindung mit einem geerdeten Ausgang konstruiert. Um das Risiko eines elektrischen Schlags oder Beschädigung des Produkts zu vermeiden, stecken Sie das Gerät nicht an irgendeine andere Art von Ausgang.

Lithium Batterie

Warnung - Dieses Produkt enthält eine oder mehrere Lithium Batterien. Wenn die Batterie falsch verwendet, beschädigt oder nicht richtig eingelegt oder ersetzt wird, besteht die Gefahr einer Explosion. Um Personenschaden oder Beschädigung de Produkts zu vermeiden, versuchen Sie nicht, die Batterie wieder aufzuladen, sie auseinander zu nehmen oder sie im Feuer zu entsorgen. Stellen Sie sicher, dass Sie die Batterie richtig entsorgen.

Beachtung der Optik

Dieses Produkt besitzt Lichtleiter-Anschlüsse. Die optischen Transceiver entsprechen den Erfordernissen für Klasse 1 Laser.

Sicherheit für die Augen

Warnung - Um die Gefahr von Personenschaden zu verringern, vermeiden Sie es, den NAS Gateway Laser direkt auf Ihre Augen zu richten.

Das Lasersignal, das von den optischen Transceiver unterstützt wird, wurde als Klasse 1 Laser kategorisiert. Entsprechend dem IEC 825-1: EN-60825-1 und FDA CDRH CFR Titel 21 stellen Klasse 1 Laser keine Gefahr unter normalen Betriebsbedingungen dar.

Unsachgemäßer Gebrauch des Lasers oder längere Bestrahlung bei Menschen kann unter Umständen einen Personenschaden hervorrufen.

Precauzioni per la sicurezza

Consigliamo la lettura e l'osservanza delle precauzioni per la sicurezza elencate in questi paragrafi prima di dare inizio a qualunque procedura.

Avvertenza - L'inosservanza delle informazioni contenute nei paragrafi seguenti può danneggiare il prodotto, causare lesioni personali o il decesso.

Precauzioni da adottare nei riguardi del calore

Per ridurre il rischio di lesioni personali causate da superfici bollenti, tutte le volte che si lavora all'interno del telaio o con componenti che ne siano stati estratti, lasciarli raffreddare prima di toccarli.

Precauzioni da adottare nei riguardi del peso dell'apparecchiatura

Avvertenza - Peso variante tra 18 e 32 kg. È necessario l'intervento di due persone per sollevare il prodotto in sicurezza.

Precauzioni da adottare nei riguardi delle scariche elettrostatiche

Attenzione - Questo prodotto contiene componenti elettronici sensibili alle scariche elettrostatiche (ESD). Per evitare di danneggiare il prodotto o i suoi componenti, assicurarsi di utilizzare un'idonea protezione ESD prima di maneggiare qualunque parte del prodotto.

Inoltre, quando si rimuove qualunque parte del prodotto, assicurarsi di appoggiarla su un piano di lavoro sicuro.

Cavi di alimentazione

Avvertenza - Questo prodotto potrebbe essere corredato da cavi di alimentazione multipli. Per ridurre il rischio di essere colpiti da folgorazione, prima di procedere alla manutenzione dell'apparecchio, scollegare tutti i cavi di alimentazione.

Messa a terra

Questa apparecchiatura è progettata per essere collegata a una presa con messa a terra. Al fine di evitare il rischio di folgorazione o di danneggiamento del prodotto, non effettuare collegamenti con altri tipi di prese.

Batteria al litio

Avvertenza - Questo prodotto è corredato da una o più batterie al litio. Qualora la batteria sia stata utilizzata in modo improprio, sia danneggiata o installata o sostituita in modo scorretto, sussiste pericolo di esplosione. Al fine di evitare lesioni personali o danneggiamento del prodotto, non cercare di ricaricare la batteria, di smontarla o di smaltirla gettandola sul fuoco. Provvedere a uno smaltimento idoneo.

Considerazioni sulle connessioni ottiche

Questo prodotto dispone di collegamenti a fibre ottiche. I ricetrasmettitori ottici soddisfano i requisiti previsti per i laser di Classe 1.

Sicurezza per gli occhi

Avvertenza - Per ridurre il rischio di lesioni personali, evitare di puntare il laser del Gateway NAS direttamente negli occhi.

Il segnale laser supportato dai ricetrasmettitori ottici è stato classificato come laser di classe 1. In conformità alle norme IEC 825-1: EN-60825-1 e FDA CDRH CFR, titolo 21, i laser di Classe 1 non rappresentano un rischio in condizioni di normale funzionamento.

Un uso improprio del laser o la prolungata esposizione umana alla sua radiazione può causare lesioni personali.

安全问题

在开始任何操作步骤之前，建议您阅读并遵守相关安全事项。

警告 – 如果不遵守如下章节列出的相关信息，可能导致产品受损、人身伤害或死亡。

防热

为避免工作人员受到过热表面的伤害，如需进入机架工作或处理设备部件，则应在相关部件冷却后再触摸。

设备重量

警告 – 18 — 32 千克 （39.7-70.5 磅）产品提升操作需要两名人员。

静电放电

注意 – 本产品配有对静电放电 (ESD) 敏感的电子部件。为避免产品及其部件受损，在处理产品的任何部件之前，应确保使用合适的 ESD 保护方法。

如需拆除产品的任何部件，也要确保将其放在 ESD 安全工作表面上。

电源线

警告 – 本产品可能装有多种电源线。为减少电击风险，在对设备进行维修之前，应断开所有电源线。

接地

该设备装有接地出口接头。为避免电击风险或产品受损，请不要将其插入任何其他种类的插座上。

锂电池

警告 – 本产品配有一个或多个锂电池。如果电池使用不当、受损；或没有正确安装、更换，则可能发生爆炸。为防止发生人身伤害或产品损坏，请不要向电池充电，分解电池或将其投入火中。应采用正确地方法处理电池。

光学部件

本产品配有光纤接头。光收发器应符合一类激光要求。

眼部安全

警告 – 为减少人身伤害危险，不要将 NAS 网关发出的激光指向眼睛。

光收发器支持的激光信号被归类为一类激光。根据 IEC 825-1 的相关要求：在正常操作条件下，EN-60825-1 和 FDA CDRH CFR Title 21 一类激光不具有危害性。

不正当使用激光，或者延长激光对人体的照射时间则可能引起人身伤害。

安全に関する注意事項

製品取扱上のいかなる手順を開始する前に、以下に記した安全に関する注意事項を読み、その内容に従うことを推奨します。

警告 – 以下の各セクションに記した内容に従わなかった場合は、製品の破損、人的傷害、または死亡事故を引き起こすことがあります。

熱に関する注意

高温の機器表面による人的傷害の危険性を低減するため、シャーシ内部またはシャーシから取り外されたコンポーネントを取り扱う場合は、触れる前に、コンポーネントが冷却するまで十分な時間をおいてください。

機器の重量に関する注意

警告 – 機器の重量は 18 kg（39.7 ポンド）～ 32 kg（70.5 ポンド）です。製品の安全な持ち上げは、成人 2 人で行ってください。

静電放電に関する注意

注意 – この製品は、静電放電（ESD）に過敏な電子コンポーネントを含んでいます。製品またはコンポーネントの破損を避けるため、製品のあらゆる部品を取り扱う前に、適切な ESD 保護対策が講じられていることを確認してください。

また、製品から部品を取り外す際は、取り外した部品を必ず ESD から保護された表面に置いてください。

電源コード

警告 – この製品には、複数の電源コードが備わっている場合があります。電気ショックの危険性を低減するため、ユニットの点検や修理の前にすべての電源コードを外してください。

接地

この機器は、接地した電源コンセントに接続するように設計されています。電気ショックの危険性や製品の破損を避けるため、他のタイプの電源には接続しないでください。

リチウム電池

警告 – この製品には、1 個または複数のリチウム電池が含まれています。電池を誤って取り扱って破損させたり、不正な取り付けや交換を行ったりすると、爆発する危険性があります。人的傷害や製品の破損を避けるため、電池の再充電や分解、または火の中に投じて処分することはしないでください。電池の処分は、必ず適切に行ってください。

光学に関する注意

この製品には、光ファイバー接続が備えられています。光学送受信機は、クラス 1 のレーザー要件に準拠しています。

目の安全に関する注意

警告 – 人的傷害の危険性を低減するため、NAS Gateway のレーザーを目に直接当てないでください。

光学送受信機がサポートしているレーザー信号は、クラス 1 レーザーに分類されています。IEC 825-1: EN-60825-1 および FDA CDRH CFR タイトル 21 では、クラス 1 レーザーは、通常の操作条件下で危険性を持つことはないとされています。

レーザーを誤って取り扱ったり、人体がレーザーに継続的に晒されたりすると、人的傷害を引き起こす可能性があります。

Chapter 2: Specifications and Preinstallation

This chapter contains the following sections:

Packing List

- ONStor Cougar 6000 Series NAS Gateway
- Software Accessory Kit (qty=2)
  - Installation Guide
  - Cluster Configuration Guide
  - Software CD
  - Software License Document
  - Warranty Document
- VSCAN Software (qty=2)
- Hardware Accessory Kit
  - Cluster Cable RJ45 (qty=2)
  - RS232 Cable (qty=2)
  - Rack mount Screws
  - Wrist Strap
- Power Cord (qty=2) - Country specific
- 1U, Rack mount, Slide Rail Kit, Adjustable 22”-35”

Specifications

AC Power Requirements

Maximum	3.0A @ 120V 1.5A @ 240V

Dimensions

Height (in./cm)	3.5 in. (8.89 cm)
Width (in./cm)	17 in. (43.18 cm)
Depth (in./cm)	24.1 in. (61.21 cm)

Weight

Weight (lb/kg)	45 lbs (20.41 kg)

Environment

Operating Temperature	0 – 40 degrees C (32 - 104 degrees F)
Relative Humidity	20–80% non–condensing
Non–Operating Temperature	–20 to 60 degrees C
Relative Humidity	10–90%, non–condensing

Thermal Rating

Model 6520	938 BTU / Hr (max), 853 BTU / Hr (typical)
Model 6720	1024 BTU / Hr (max), 938 BTU / Hr (typical)

Preinstallation Tasks

This section describes the preinstallation planning and tasks that you need to perform before the actual installation takes place. In addition, this section outlines the process that comprises a basic installation.

Preinstallation Planning

Before installing and configuring the firmware and software components of the ONStor Cougar 6000 Series NAS Gateway, the preinstallation tasks listed here should be completed. Typically, the customer performs these preinstallation tasks.

Note - The ONStor Site Survey, which provides a checklist of these preinstallation tasks, should be completed and available during this installation. The survey is available as a separate document.

The customer should also have read and signed the ONStor Statement of Work.

Preinstallation covers planning and preparing the SAN network, storage subsystem, IP network, client environment, and backup/tape information. It consists of the following tasks:

- Physical site preparation includes ensuring:
  - System environment has adequate rack space
  - Redundant power available
  - HVAC requirements are met
  - Fiber raceway is in place for the new equipment
  - Cable lengths are appropriate for the NAS Gateway locations
- Installation planning:
  - Provide SAN configuration documentation, including:
    - Switch port connections
    - Host/LUN table
    - Any switch zoning requirements if tape is required
  - Provide a network diagram that includes details of the LAN/SAN switch and IP configuration pertaining to the environment
  - Schedule a downtime window to configure and install ONStor's configuration.
- Fibre Channel and SAN tasks:
  - LUN allocation: All LUNs must be pre-allocated/zeroed available in a common zone

  - Performance: To deliver the requested performance, adequate resources (such as spindle count), and appropriate policies, (such as read ahead), need to be used to create LUNs.
  - Oversubscription: If the array is a shared resource, take steps to ensure that the array will not be oversubscribed by other applications. (ONStor access to the SAN administrator is highly recommended.)
  - SAN: Four FC cables per node from the SAN in the same zone. (WWN can be provided by ONStor as needed.)
- Network setup:
  - For each node, up to four network ports are needed on the switch that connects the ONStor NAS Gateway.
  - For each switch, provide the appropriate VLANs and configure its ether channel.
  - Ensure that all Layer 3 network addresses, netmasks, and default routes are identified and allocated to the NAS Gateway.
  - Provide the IP addresses for network servers (e.g. DNS, AD, NIS, and so forth).
- Server access setup:
  - Set up access to the following servers as required: FTP server, NTP server, NIS server, SMTP server, and domain controllers.
  - Have a client running a Web browser available to run ONStor management software.
  - Provide two high-performance clients to test the performance for each protocol.
- Security setup:
  - Provide the names of the users or groups who will have cluster administrative privileges.

Chapter 3: ONStor Cougar 6000 Series NAS Gateway Hardware Installation

This chapter contains the following sections:

ONStor Cougar 6000 Series NAS Gateway Installation

Installing the ONStor Cougar 6000 Series NAS Gateway consists of two steps:

Step 1: Installing the ONStor Cougar 6000 Series NAS Gateway into the equipment rack.

There are two different rack installations that can be performed. Choose the one that applies to your environment:

- “Installing Into a 2-Post Rack” on page 3-3
- “Installing Into a 4-Post Rack” on page 3-4

Step 2: “Powering Up the ONStor Cougar 6000 Series NAS Gateway” on page 3-12.

Installing Into a 2-Post Rack

To install the ONStor Cougar 6000 Series NAS Gateway into a 2-post rack, perform the following steps:

Step 1: While positioning the NAS Gateway, ensure that the two socket outlets required to power the NAS Gateway are near the equipment and are easily accessible.

Warning - The ONStor Cougar 6000 Series NAS Gateway should not be installed in a WAN-type environment where voltage surges can enter the unit through the CAT 5 cables.

Step 2: Attach the ONStor Cougar 6000 Series NAS Gateway with four 12-24 x 5/8” screws per mounting ear. The mounting ears span two rack units (RUs). See Figure 3-1.

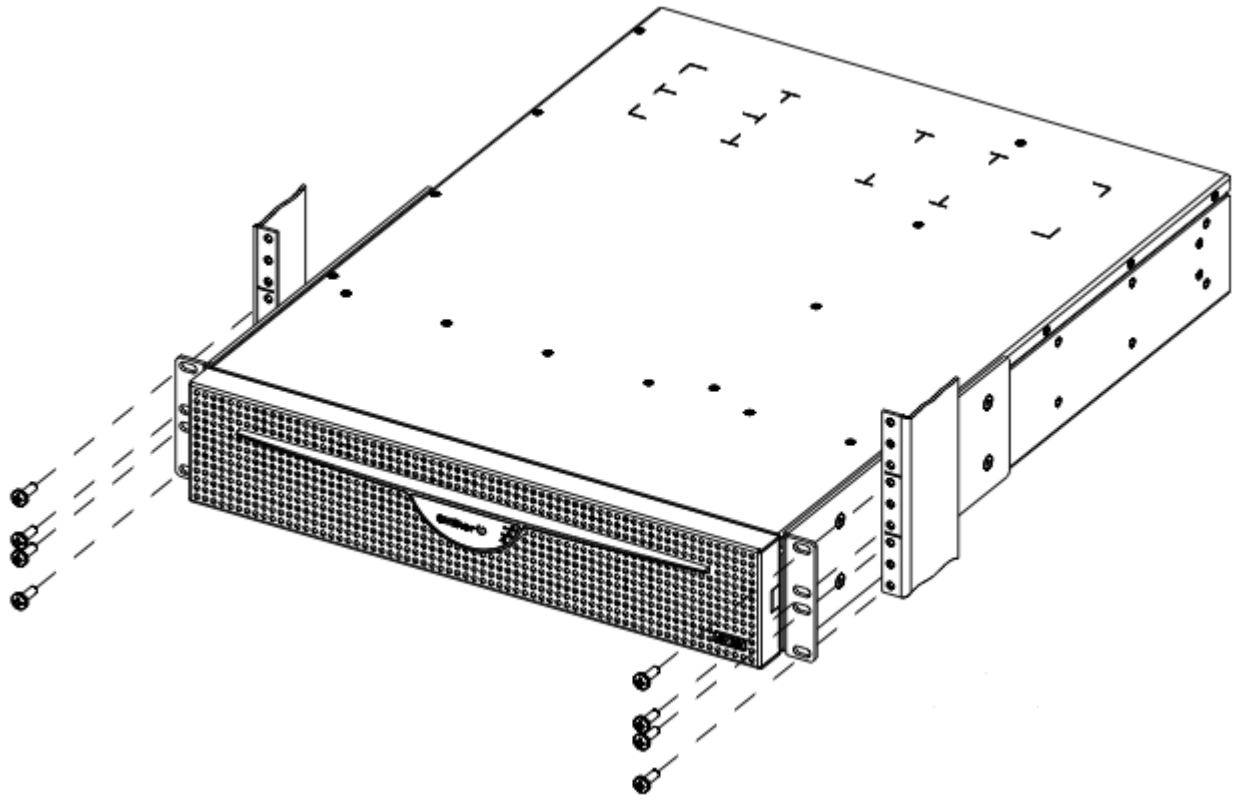


Figure 3-1 Cougar Being Attached to the Equipment Rack

Step 3: Follow the procedure for applying power. See “Powering Up the ONStor Cougar 6000 Series NAS Gateway” on page 3-12.

Installing Into a 4-Post Rack

This installation procedure documents the process for mounting an ONStor Cougar 6000 Series NAS Gateway in a four-post equipment rack, which has two posts at the front of the equipment rack and two posts at the rear. This procedure documents installing the ONStor Cougar 6000 Series NAS Gateway in either a tapped or a universal square-hole equipment rack:

- a tapped equipment rack has threaded screw holes
- a universal square-hole equipment rack has screw holes that are not threaded. In this type of equipment rack, you will need cage nuts or special screws that accompanied your equipment rack.

Required Equipment

For this procedure, you will need the following equipment:

- A #2 Phillips-head screwdriver
- Sliding rail assemblies (2)
- Stop brackets (2)
- Nut brackets (2)
- Cage nuts (8)
- Screws:
  - Ten 10-32 x 1/4” pan-head screws for attaching the sliding rails to the chassis.
  - Eight 10-32 x 5/16” pan-head screws for securing the fixed rails sleeves and cage nuts to each post.

Installing into a 4-post rack involves removing the mounting ears and replacing them with a sliding rail kit.

This task is documented in the following sections:

- “To Remove the Mounting Ears” on page 3-5
- “To Attach the Sliding Rail to the Chassis” on page 3-6
- “To Install the Fixed Rails” on page 3-8

To Remove the Mounting Ears

Step 1: Use a Phillips-head screwdriver to remove the six screws from each of the mounting ears on the chassis.

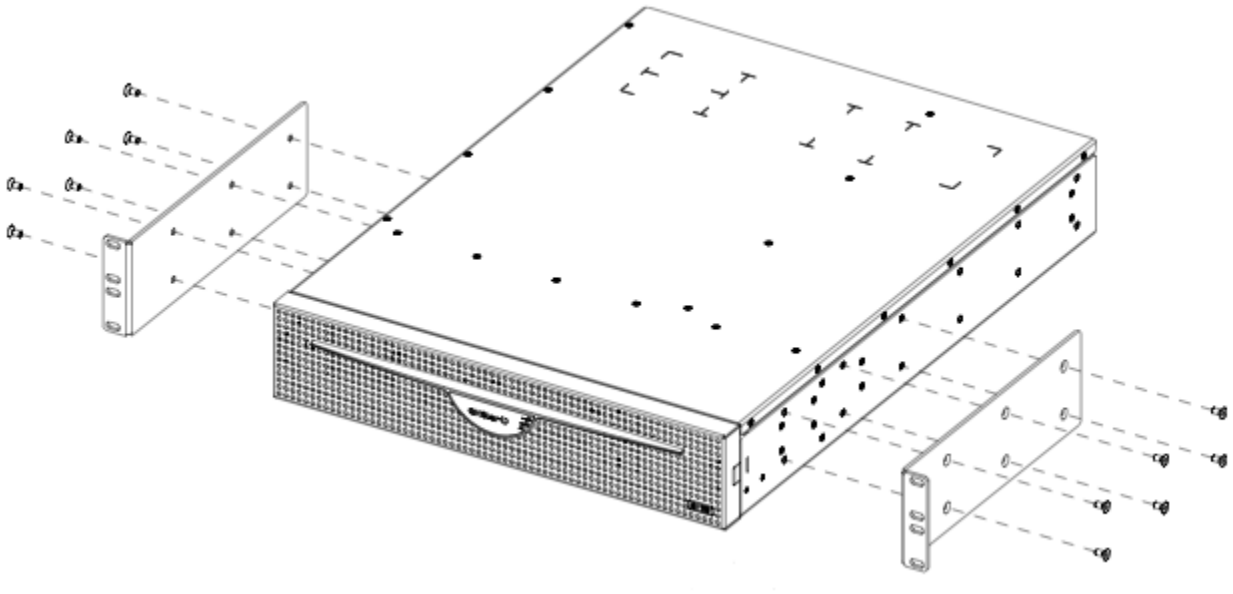


Figure 3-2 Removing Cougar Mounting Ears

Note - Retain the mounting ears. They can be used later if you need to install the ONStor Cougar 6000 Series NAS Gateway in a two-post equipment rack.

Attaching the Sliding Rails and Stop Brackets

Remove the sliding rail assembly from the product packaging. The sliding rail assembly consists of two parts:

- the sliding rails, which are installed on the sides of the ONStor Cougar 6000 Series NAS Gateway chassis.
- the fixed rails, which are installed on the inside of the equipment rack.

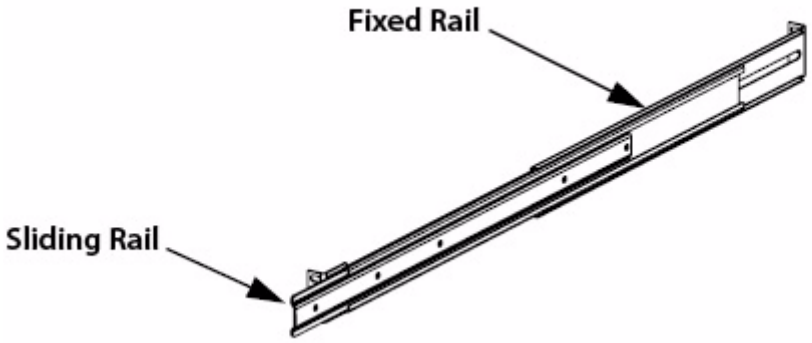


Figure 3-3 Sliding Rail Assembly

To Attach the Sliding Rail to the Chassis

Step 1: Disassemble the sliding rail assembly by grasping the sliding rail and pulling it out of the fixed rail.

Note - Each rail assembly has a release tab. The sliding rail cannot be completely removed from the fixed rail until you press the release tab.

Step 2: When the sliding rail is fully extended, press the release tab to remove the rail.

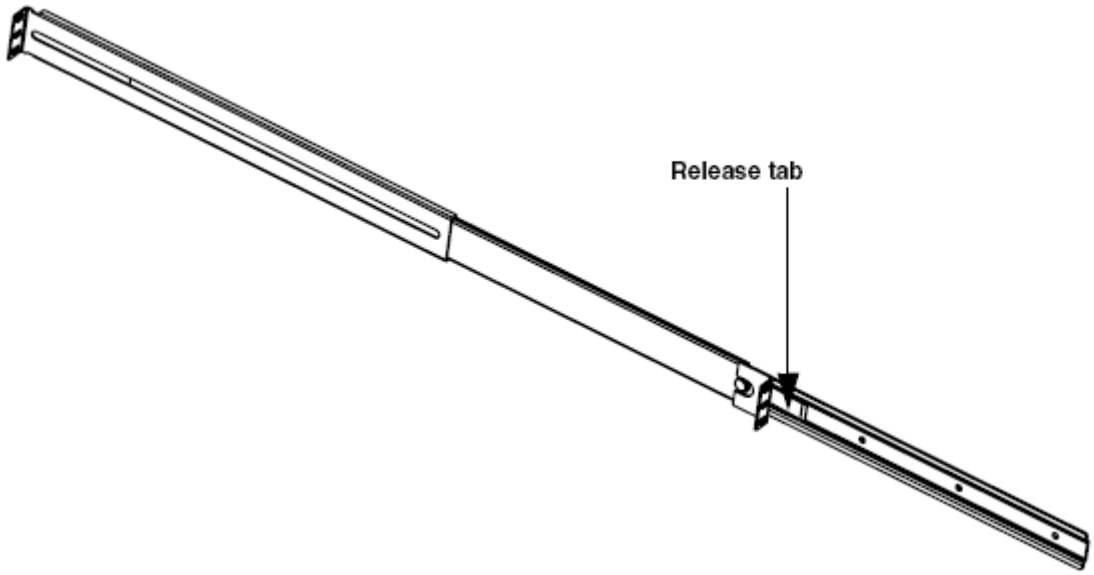


Figure 3-4 Sliding Rail With Release Tab

Step 3: With the release tab facing away from the chassis, attach the sliding rails to each side of the chassis with five 10-32 x 1/4” screws.

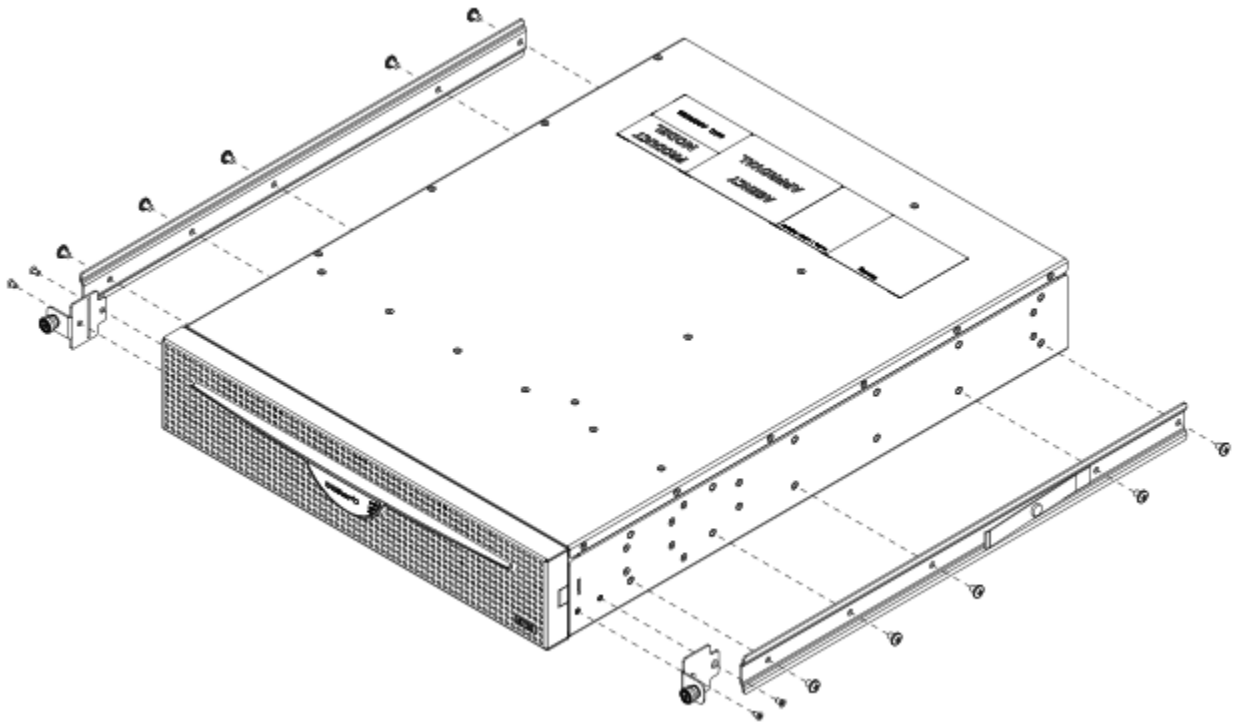


Figure 3-5 Cougar With Sliding Rails and Stop Bracket

Step 4: Attach the stop brackets to each side of the chassis with two 6-32 1/4” screws.

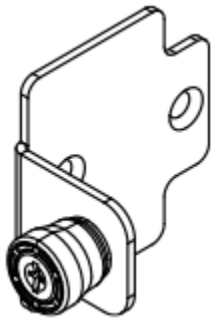


Figure 3-6 Stop Bracket

Installing the Fixed Rail in the Equipment Rack

For the ONStor Cougar 6000 Series NAS Gateway to slide easily in and out of the equipment rack, you need to install the fixed rails to the inside of the equipment rack.

To Install the Fixed Rails

Step 1: Fully extend the fixed rail, making sure that the mounting flanges are in front of the posts and facing outward.

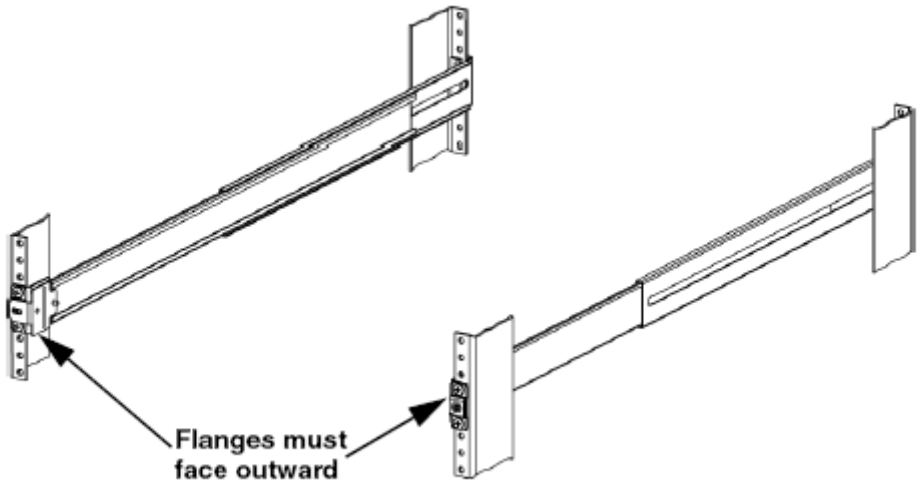


Figure 3-7 Fixed Rail Positioning

Step 2: Perform either of the following steps depending on the type of equipment rack:

- For a universal square-hole rack, place the cage nut behind the rack, align the screw holes. Insert the screws through the nut bracket, mounting flange, rack, and into the cage nut.

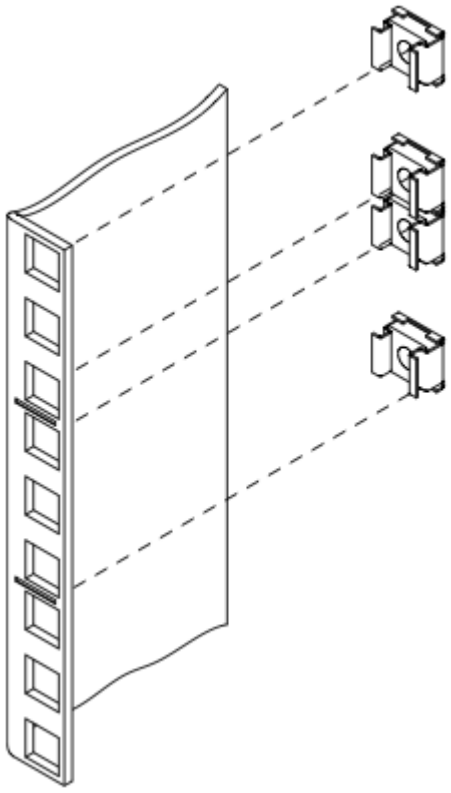


Figure 3-8 Equipment Rack and Cage Nuts

- For a tapped equipment rack, align the screw holes in all the parts, insert the screws through the nut bracket, mounting flange, and into the rack. Do not tighten the screws yet.

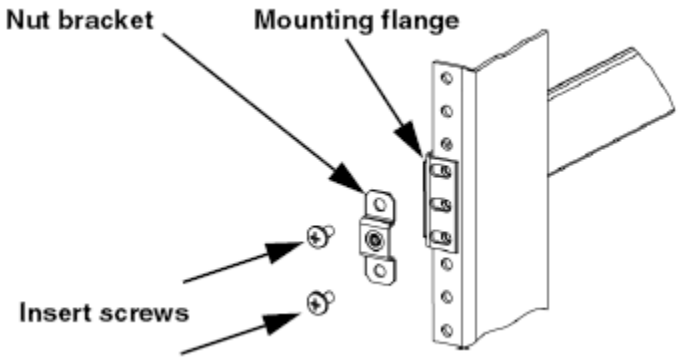


Figure 3-9 Attaching to Tapped Equipment Rack

Step 3: Repeat the appropriate steps for the rear of the equipment rack and the opposite side of the equipment rack.

Step 4: Finger tighten the screws until you begin to feel some resistance.

Note - Do not tighten the screws all the way because you might need to adjust the distance between the rails when you attempt to inset the NAS Gateway into the rack.

Installing the ONStor Cougar 6000 Series NAS Gateway into the Equipment Rack

With the sliding rails installed on both sides of the NAS Gateway and the fixed rails at the same vertical level in the equipment rack, you are ready to insert the NAS Gateway into the equipment rack.

While inserting and removing the chassis, it is a good idea to:

- Always use two people to lift the NAS Gateway
- Apply steady and constant pressure. Rapidly pulling the chassis out, or pushing it in, can cause unnecessary stress on the sliding rail assembly.
- Be aware that the sliding rail assembly has a release tab which is a safety feature that prevents you from accidentally ejecting the chassis from the equipment rack. As a result, whenever you are removing or installing the chassis, you must press the release tab to allow the sliding rail to fully slide in or out of the fixed rail.

To Install the ONStor Cougar 6000 Series NAS Gateway

Note - Because the fixed rails have not been completely tightened to the rack, you can adjust the distance inside the rack if the rails are too far apart or too narrow.

Step 1: Holding the NAS Gateway level, align the sliding rails on the NAS Gateway chassis with the fixed rails on the equipment rack.

Step 2: Gently guide the sliding rails into the fixed rails as shown in Figure 3-10.

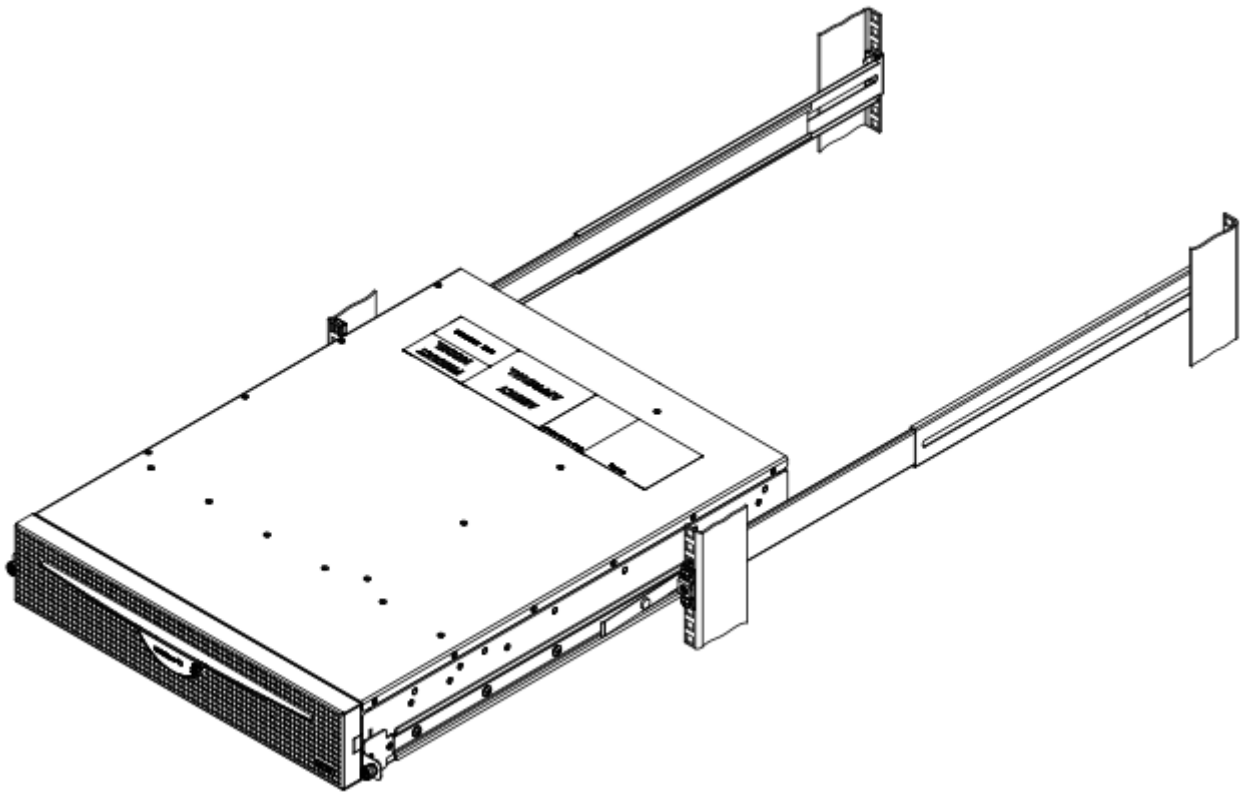


Figure 3-10 Cougar Sliding Into the Fixed Rails

Step 3: When you feel the resistance of the release tabs, simultaneously press both release tabs inward and slide the chassis the rest of the way into the equipment rack until the stop bracket contacts the nut plate, preventing the NAS Gateway from sliding further.

Step 4: Insert the stop screw into the nut bracket and hand tighten the thumb screw.

Step 5: At this point, tighten the remaining screws.

Note - Do not overtighten. You do not want to strip the screws.

Step 6: Follow the procedure for applying power. See “Powering Up the ONStor Cougar 6000 Series NAS Gateway” on page 3-12.

Powering Up the ONStor Cougar 6000 Series NAS Gateway

Step 1: Attach the two power cables to the power plugs at the rear of the ONStor Cougar 6000 Series NAS Gateway. See Figure 3-11.

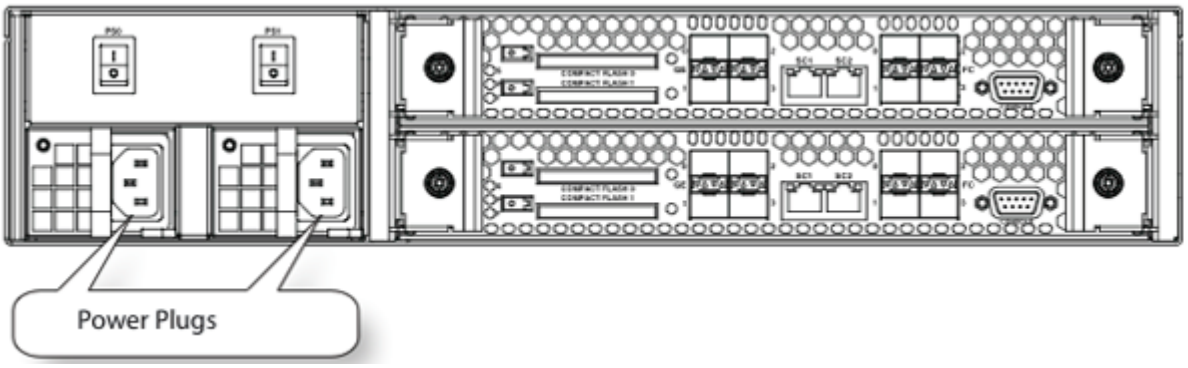


Figure 3-11 ONStor Cougar 6000 Series NAS Gateway Power Plugs

---

Note - A redundant network configuration is the preferred setup. It is recommended that you always have redundant network connections so that a single failure does not shut down the management network, which makes recovery difficult. For a two-node cluster, you should have one connection to the main network and another connection with a crossover cable. For a cluster larger than two nodes, you should have one connection to the main network and another connection with a second switch (a setup described as a hybrid network).

Step 2: After plugging the two power cables into the NAS Gateway, plug each power cord into a separate power outlet.

The NAS Gateway contains redundant load-sharing power supplies and for this reason requires two power outlets. To ensure full redundancy, you must plug the power supplies into outlets that are on different AC circuits.

Note - With the switches in the off position, the LEDs for PS0 and PS1 will blink green.

Step 3: After verifying that both connections to facility power are correct, switch on the power supplies.

The power supply activation switches, located on the rear of the NAS Gateway, are marked with an **I** (On) and **O** (Off) as shown in Figure 3-12. Press the **I** symbol to turn on the power supply (the switch should rock upwards).

The LEDs for PS0 and PS1 turn solid green. If the power units do not have AC power, the LED will turn solid amber.

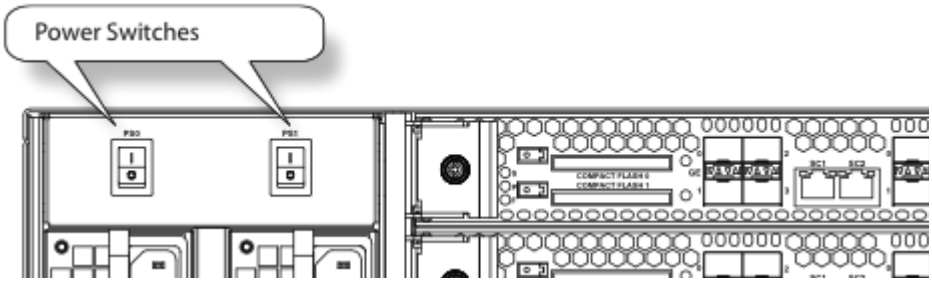


Figure 3-12 ONStor Cougar 6000 Series NAS Gateway Power Switches

---

Note - You should hear the power supplies activate when you turn them on. Also, the built-in fans start to operate at maximum speed, then slow to an operational speed. This behavior is normal.

Step 4: Check the LED lights on the front of the NAS Gateway after it completes its boot up phase.

Table 1: NAS Gateway Fascia LEDs

LED	Behavior
System	Flashing green - System booting (either NAS Blade)
	Solid green - All processors up in runtime (both NAS Blades)
	Red - Any processor has crashed (either NAS Blade)
Power Supply	Green - Both supplies OK
	Red - One supply is not up
Fan	Off - Fan modules OK.
	Red - Locked rotor with one or more fans
Logo	On when 12V present from at least one of the power supplies.

This concludes the physical hardware installation of the NAS Gateway.

Note - Contact ONStor Customer Support if your ONStor NAS Gateway is not operating properly.

Chapter 4: Hardware Overview

This chapter contains the following sections:

Overview of Hardware

This section provides more information about the ONStor Cougar 6000 Series NAS Gateway's hardware modules and chassis equipment.

System Control Components

The System Switch and Controller (SSC) contains the on-board intelligence that ensures the integrity of the ONStor Cougar 6000 Series NAS Gateway. This is essentially the "brains" of the ONStor Cougar 6000 Series NAS Gateway, and as such, plays an important role in system control, event logging, fault management, and the switching of data and metadata through the backplane. In addition, the SSC contains the boot and runtime images, the transaction journals, log files, and other system elements. The SSC provides the command line interface, and administrators can connect to it through the Console port.

File Processing Components

File Processing (FP) contains on-board processing for IP connectivity. Specifically, FP supports IP processing, network file protocols, file access protocols, and volume management, as well as providing file sharing interfaces. FP supports connection to the customer's IP network through 4 link-aggregated Gigabit Ethernet (1000BaseSX) ports. Each Gigabit Ethernet port supports an individual collision domain in an IP network.

Warning - To reduce the risk of personal injury, avoid pointing the NAS Gateway's laser directly into your eye.

The laser signal supported on the optical transceivers have been categorized as a Class 1 laser. Per the IEC 825-1: EN-60825-1 and FDA CDRH CFR title 21 Class 1 laser do not pose a risk under normal operating conditions.

Misuse of the laser or prolonged exposure to a human has the possibility of causing personal injury.

Storage Processing Components

The Storage Processing (SP) module is software that contains on board processing for storage functions. Specifically, the SP module supports fibre channel and the serial SCSI protocol that runs on top of fibre channel. The SP module provides connection to the storage network through four physical fibre channel ports that connect the ONStor Cougar 6000 Series NAS Gateway to the SAN or storage devices. Each fibre channel port supports connection into the fibre channel fabric on the storage side of the ONStor Cougar 6000 Series NAS Gateway.

Sample Topology

ONStor brings you the next generation of networked storage, the convergence of SAN and NAS, the ONStor Cougar 6000 Series NAS Gateway. The ONStor Cougar 6000 Series NAS Gateway is designed to provide next generation, high performance file services and SAN connectivity to clients in an IP network. See Figure 4-13.

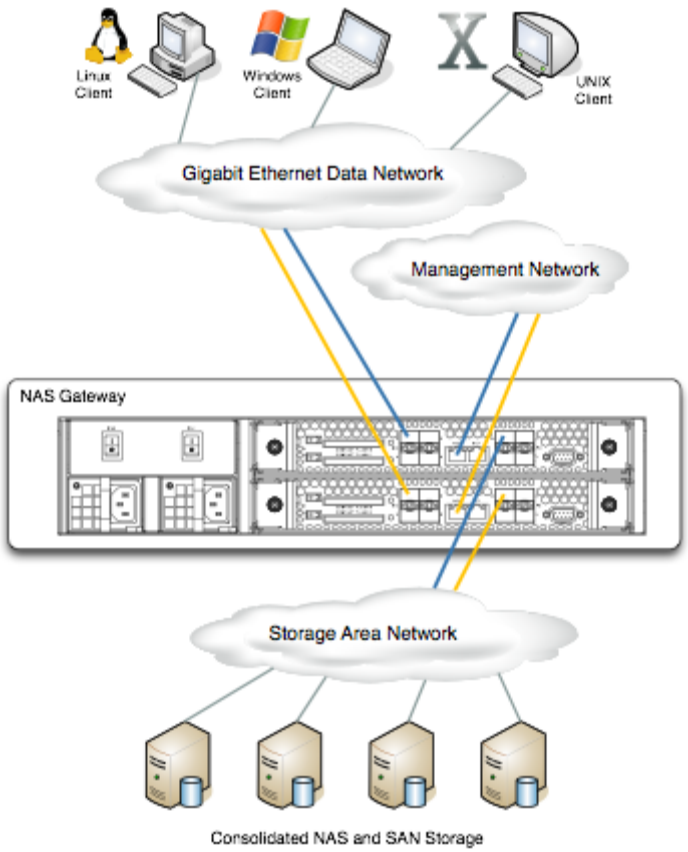


Figure 4-1 Sample Topology Containing the ONStor Cougar 6000 Series NAS Gateway

The ONStor Cougar 6000 Series NAS Gateway adds value to SAN and NAS environments in the following ways:

- By supporting massive numbers of users, files, and file systems.
- By supporting an unparalleled number of file system operations per second.
- By providing virtualized storage, which makes a SAN appear as a unified storage pool over the LAN. Because IT administrators are more familiar with an IP LAN, the ONStor Cougar 6000 Series NAS Gateway facilitates SAN administration, reducing costs and required personnel time.
- By providing high scalability and high reliability, the ONStor Cougar 6000 Series NAS Gateway offers efficient high performance service to the data center, as well as enabling the

data center to grow. Consequently, the ONStor Cougar 6000 Series NAS Gateway helps safeguard your storage investment.

- By automating storage tasks, the ONStor Cougar 6000 Series NAS Gateway offers simple management of storage. Advanced storage capacity management through the ONStor Cougar 6000 Series NAS Gateway's automated storage growth policies facilitates controlling storage regardless of the number of users, growth rates, or the amount of storage you need to manage.
- By automatically discovering the SAN storage devices when the ONStor Cougar 6000 Series NAS Gateway is connected to a SAN, the ONStor Cougar 6000 Series NAS Gateway file enables easy configuration of devices into a single easily-managed storage pool.
- By easily reducing the burden on storage administrators, the ONStor Cougar 6000 Series NAS Gateway releases administrators from tedious element-level management tasks. As a result, administrators can focus their time and effort on more productive activities that bring more benefit to your business organization.

The ONStor Cougar 6000 Series NAS Gateway also supports DAS environments, where the storage is directly-connected to the ONStor Cougar 6000 Series NAS Gateway. In this configuration, the ONStor Cougar 6000 Series NAS Gateway provides high performance file services and DAS connectivity to clients in an IP network.

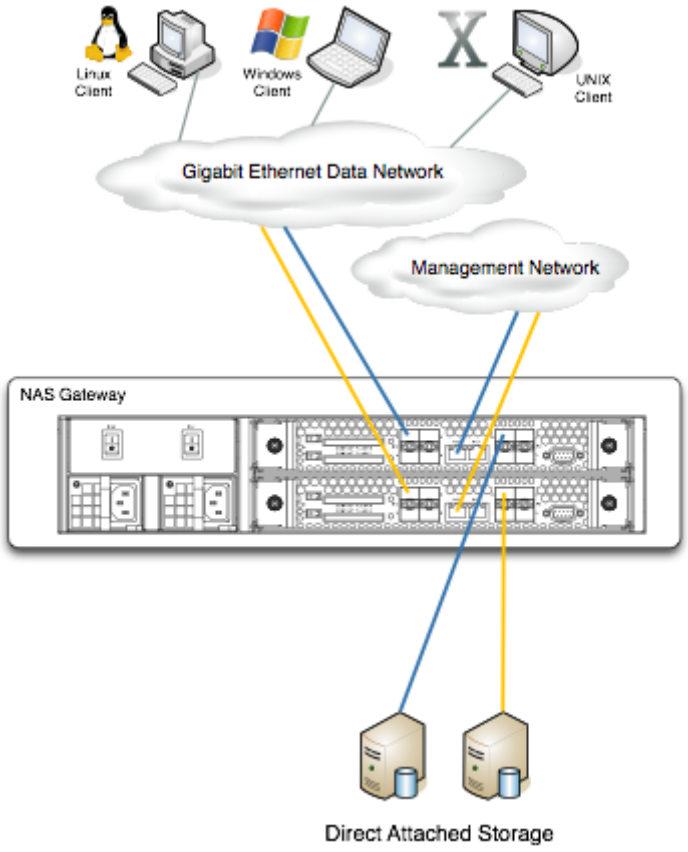


Figure 4-2 Sample DAS Environment

The ONStor Cougar 6000 Series NAS Gateway adds value to DAS environments by eliminating the need for individual fibre channel switches, thus reducing the overall costs of your storage network by simplifying the management and configuration of the SAN and NAS components of the network, as well as the benefits listed in the previous example.

Chapter 5: Software Installation

The chapter contains the following sections:

Connecting to the Management Console

The ONStor Cougar 6000 Series NAS Gateway supports a management console through direct connection or Telnet. The management console can be a PC or workstation that you will use to connect to the NAS Gateway for the purpose of configuration or management.

- To connect the management console directly to the ONStor Cougar 6000 Series NAS Gateway, connect the management console to the Console port on the ONStor Cougar 6000 Series NAS Gateway's rear panel. Direct connection is the only way to access the ONStor Cougar 6000 Series NAS Gateway at initial boot up.
- To connect the management console to the ONStor Cougar 6000 Series NAS Gateway through a Telnet session, connect the management console to the 10/100 Mbps RJ-45 port on the ONStor Cougar 6000 Series NAS Gateway with an Ethernet segment. Telnet management is available only after you have configured an IP interface.

Management Console: Terminal Server Connection

The NAS Gateway supports connecting a management console to the NAS Gateway through a terminal server. Follow this procedure to connect the management console to the NAS Gateway through a terminal server.

Step 1: Connect the terminal server to the IP network. For details about connecting your terminal server, see the documentation that accompanied your terminal server. Make sure that you can ping the terminal server from a workstation.

Step 2: Connect one of the RS-232 ports from the terminal server to the Console port on the rear of the NAS Gateway. The remaining RS-232 ports can be connected to the Console port on other NAS Gateways.

Management Console: Direct Connection

Follow this procedure to directly connect the management console to the ONStor Cougar 6000 Series NAS Gateway:

Step 1: Plug one end of the RS-232 management cable into the management console.

Step 2: Plug the other end of the RS-232 management cable into the Console port on the rear of the ONStor Cougar 6000 Series NAS Gateway. See Figure 5-15 on page 5-3.

For optimal performance, the management console should be configured with the following settings:

- Baud Rate: 57600 (56 K)
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

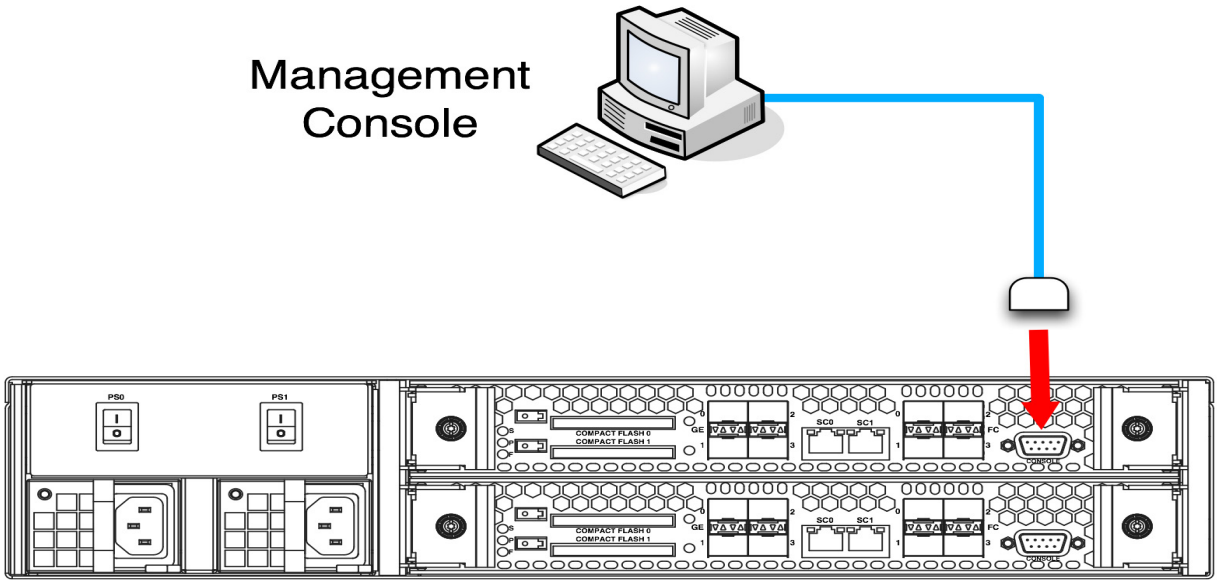


Figure 5-1 Connecting to the Management Console

Step 3: If you have not already done so, power on the ONStor Cougar 6000 Series NAS Gateway.

Note - The Initial Configuration Wizard starts once, at initial boot up. After you have completed the required input, the Initial Configuration Wizard is no longer displayed when the ONStor Cougar 6000 Series NAS Gateway boots.

Initial Configuration (NAS Gateway Startup)

When you first start up the NAS Gateway, the Initial Configuration Wizard runs automatically when you log in. The Initial Configuration Wizard is a form when accessed through a Web browser. When accessed through the Console port or SSH, the Initial Configuration Wizard is a CLI which facilitates the initial configuration of the NAS Gateway.

The Initial Configuration Wizard also starts after the **system config reset** command has been run.

When running the **system config reset** command with the **-r** option, the nfxsh shell and the WebUI will not prompt the user to enter the configuration for sc0 and sc1 IPs, default route, NTP server, DNS information, and the cluster database will be removed.

For a comprehensive list of information elements required to configure the NAS Gateway, see the *ONStor Pre Configuration Checklist*.

Connecting to the ONStor NAS Gateway

There are two ways to connect to the ONStor NAS Gateway:

- "Connecting Through the Console Port" on page 5-5
- "Connecting Though an Ethernet Cable" on page 5-5

Connecting Through the Console Port

Use a console (or serial) cable to connect your computer to the ONStor NAS Gateway. (A console cable has a DB9 end and an adapter end and it is supplied with every new NAS Gateway.)

The cable goes into the socket to the far right of the rear of the NAS Gateway. Plug the other end of the cable into a USB port on your computer.

Use a terminal emulation application such as HyperTerminal to open a TTY terminal window to connect to the NAS Gateway console through its serial port. Then, set the baud rate and serial port settings for the connection, as follows:

- Baud Rate: 57600 (56 K)
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

From the terminal window, connect to the NAS Gateway. You are now ready to use the Initial Configuration Wizard, which is the network parameter configuration tool.

When you log in as *admin*, the Initial Configuration Wizard starts automatically.

Note - When initial configuration is complete, remove the serial cable from the Console port.

Connecting Though an Ethernet Cable

An Ethernet cable can be used to connect to the NAS Gateway for the purpose of initial configuration.

DHCP Client

The DHCP IP address method assigns an IP address to the NAS Gateway through the manual allocation method. This method associates a device's MAC Address with an IP address and other network parameters. This method requires the customer to know what IP address was assigned to the NAS Gateway in the DHCP server. During Initial Configuration, you can continue to use the manually allocated IP address or change it.

Note - The MAC Address of the NAS Gateway is on the MAC Address label on the top-rear of the unit.

The DHCP client method is the default initial configuration method. If the NAS Gateway cannot get its configuration parameters from a DHCP server, the process falls back to the Default IP Address method.

Default IP Address

The Default IP Address option is available to support a unique default IP address in order to display the Web page that is used for initial configuration of the NAS Gateway.

The default IP address for sc0 is 172.18.250.250 and the default IP address for sc1 is 172.19.250.250.

The default netmask value for both sc0 and sc1 is 255.255.0.0.

To Establish an Ethernet Connection

Step 1: If you are going to use the default IP addresses, set up one of the network connections on your laptop in the 172.18.250.0 subnet if connecting to the sc0 port or 172.19.250.0 subnet if connecting to the sc1 port.

Note - The last octet of the IP address cannot be 250 since this is the one used by the default IPs.

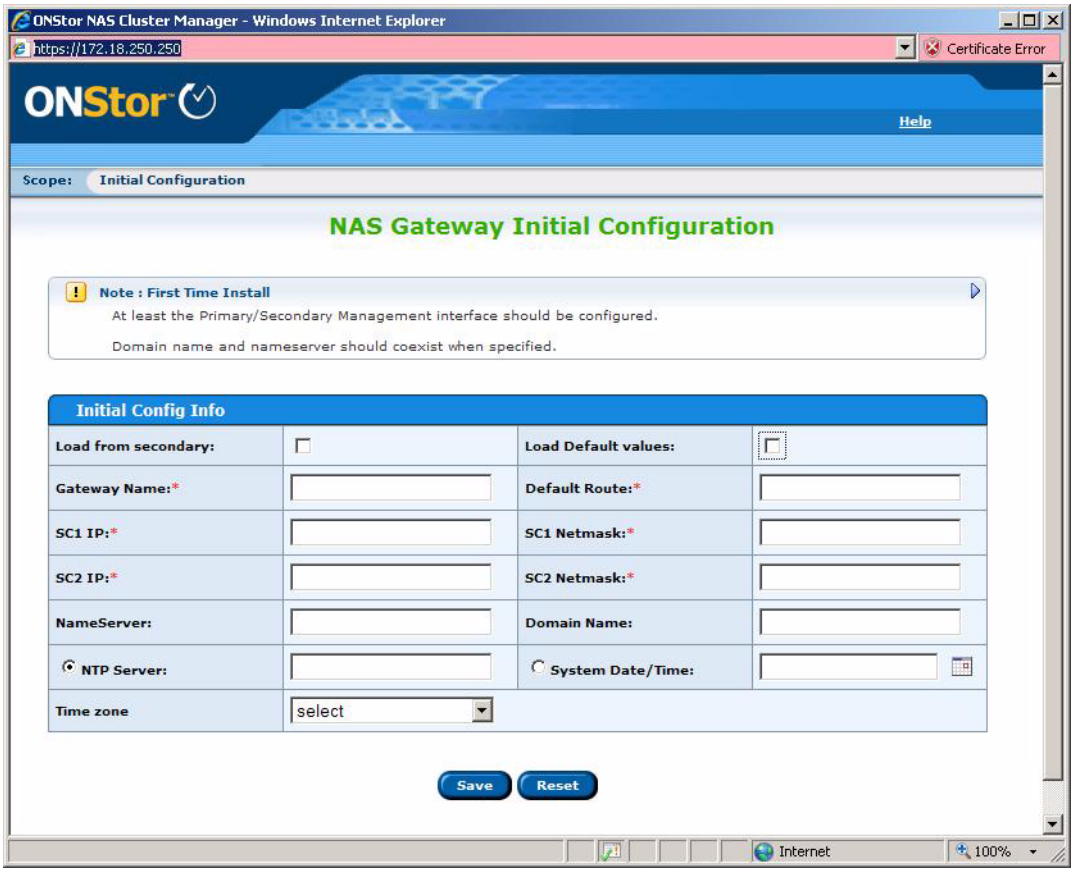
Step 2: Connect the Ethernet cable to either the sc0 or sc1 port.

Step 3: Open a browser window.

Step 4: Connect to the NAS Gateway by typing https://*IPADDRESS* into the browser and pressing **Enter**.

- If you have configured an IP address through DHCP, *IPADDRESS* is the IP address obtained from the DHCP server in the network to which you are connected.
- If you have not configured an IP address through DHCP, *IPADDRESS* is the default IP address of the Management port to which you are connected.

After you press **Enter**, the browser will be redirected to the Initial Configuration screen.



Note - When both an sc0 and sc1 interface boots using the DHCP client method, parameters obtained by using the sc1 interface override the parameters hostname, default router, NTP server, domain name, and nameserver obtained by using the sc0 interface. Only the sc0 IP and netmask are preserved.

The Initial Configuration Wizard

The Initial Configuration Wizard guides you through the initial configuration of the NAS Gateway and enables you to connect it to the network. The NAS Gateway is not configured on the network until all tasks of the Initial Configuration Wizard are completed and the parameters are committed. The NAS Gateway supports a command-line interface and a GUI that enables you to use the NAS Gateway features.

When you use the Initial Configuration Wizard, you are prompted to enter the following information:

- The hostname
- The Primary Management IP address
- The Primary Management Netmask
- The Secondary Management IP address
- The Secondary Management Netmask
- The Default Route
- The NTP Server

Note - If an NTP server is not available, you are prompted for the date and time.

- The Timezone
- The Domain Name
- The Name Server

Note - The cluster network is configured on the management IP port on the SSC. Therefore, the management IPs are set using the Initial Configuration Wizard prior to the NAS Gateway joining the cluster. The management ports are labeled sc0 and sc1 for the left and right ports, respectively.

Completing the Initial Configuration Wizard

When the Initial Configuration Wizard starts, the Initial Configuration Wizard screen is displayed as shown in Figure 5-16.

```
================================================================================

        Welcome to the Gateway Initial Configuration Wizard

This wizard allows you to quickly initialize your NAS Gateway. You'll only need to enter some
basic Networking parameters. After the initial configuration, you will able to further configure
your Gateway.

================================================================================

Do you wish to copy the configuration files from secondary flash: (y|n|q):n

================================================================================
```

Figure 5-2 Initial Configuration Wizard Welcome Screen

- If you type **Q**, the wizard closes and you return to the login prompt.
- If you type **Y**, the configuration files are copied from the standby CompactFlash card and you are returned to the login prompt.
- If you type **N**, the following screen is displayed.

```
================================================================

        Welcome to the Gateway Initial Configuration Wizard


This wizard allows you to quickly initialize your NAS Gateway. You'll only need to enter some
basic Networking parameters. After the initial configuration, you will able to further configure
your Gateway.


1. Fields marked * are mandatory.
2. Default values are displayed in square brackets. Simply hit return to use the default values.
3. Type space followed by return key to ignore default value.
4. Type # followed by return key to exit without committing the changes.
5. At least the Primary/Secondary Management interface should be configured.
6. When the NTP Server is unavailable, Date & Time can be configured.
7. Domain name and nameserver are optional. When configured, both the parameters should be
entered.
================================================================


Enter the Gateway's Hostname:* []
```

To Enter the Initial Configuration Parameter Values

Step 1: Type the parameter values as the appropriate prompt is displayed.

Additional parameter prompts are displayed when the previous parameter value is typed and you press **Enter**. Figure 5-3 shows the complete parameter window.

When all parameter values have been entered, the confirmation window is displayed.

Note - The asterisk (*) by the parameter prompt denotes a required field.

You must enter either a Primary Management IP and Netmask or a Secondary Management IP and Netmask.

```
Enter the Gateway's Hostname:* [] host
Enter the Gateway's Primary Management IP: [] 192.168.17.17
Enter the Gateway's Primary Management Netmask: [] 255.255.255.0
Enter the Gateway's Secondary Management IP: []
Enter the Gateway's Secondary Management Netmask: []
Enter the Gateway's Default Router:* [] 192.168.17.1
Enter the Gateway's NTP Server: [] 192.168.17.18
Enter the Gateway's Timezone code {Type 0 to get zone list}: [US/Pacific]
Enter the Gateway's Resolver Domain Name: [] domain-name
Enter the Gateway's Resolver Nameserver: [] 192.168.17.7
```

Figure 5-3 Initial Configuration Parameters

Step 2: If the values of the parameters are correct, type **Y** and press **Enter** to commit the changes.

- Typing **N** returns you to the parameter input window. The parameters values you previously typed are displayed and you can accept the value or override it.
- Typing **Q** returns you to the login prompt.

```
Confirmation:
        Gateway's Hostname: host
        Gateway's Primary Management IP: 192.168.17.17
        Gateway's Primary Management NetMask: 255.255.255.0
        Gateway's Secondary Management IP:
        Gateway's Secondary Management NetMask:
        Gateway's Default Router: 192.168.17.1
        Gateway's Ntp Server: 192.168.17.18
        Gateway's Timezone: US/Pacific
        Gateway's Resolver Domain Name: domain-name
        Gateway's Resolver NameServer: 192.168.17.7
--------------------------------------------------------------------------
Commit changes: (y|n|q):
```

Note - When initial configuration is complete, remove the serial cable from the console port.

Chapter 6: Basic Network Connections

This chapter contains the following sections:

Connecting the ONStor Cougar 6000 Series NAS Gateway to the IP Network and SAN

After you have installed and powered up the ONStor Cougar 6000 Series NAS Gateway, perform these steps to connect the ONStor Cougar 6000 Series NAS Gateway to the IP network and SAN.

Note - Before connecting cables, we recommend labelling the cables near both plugs so that they are easier to identify.

To Connect to the IP Network and SAN

Step 1: With one or more Gigabit Ethernet cables, connect the File Processing (FP) module, to a device in an IP network, as shown in Figure 6-1.

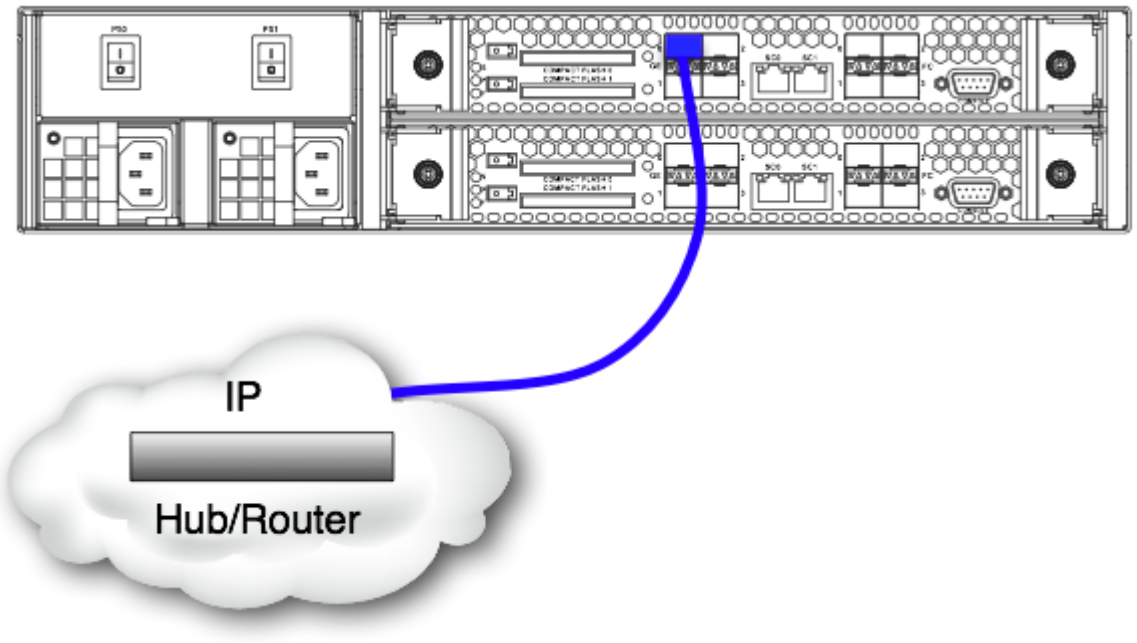


Figure 6-1 Connecting the ONStor Cougar 6000 Series NAS Gateway to the IP Network

Step 2: With a multimode fiber optic cable (not provided), connect the Storage Processing (FP) module to a Fibre Channel device in the SAN or directly to Fibre channel storage devices, as shown in Figure 6-2.

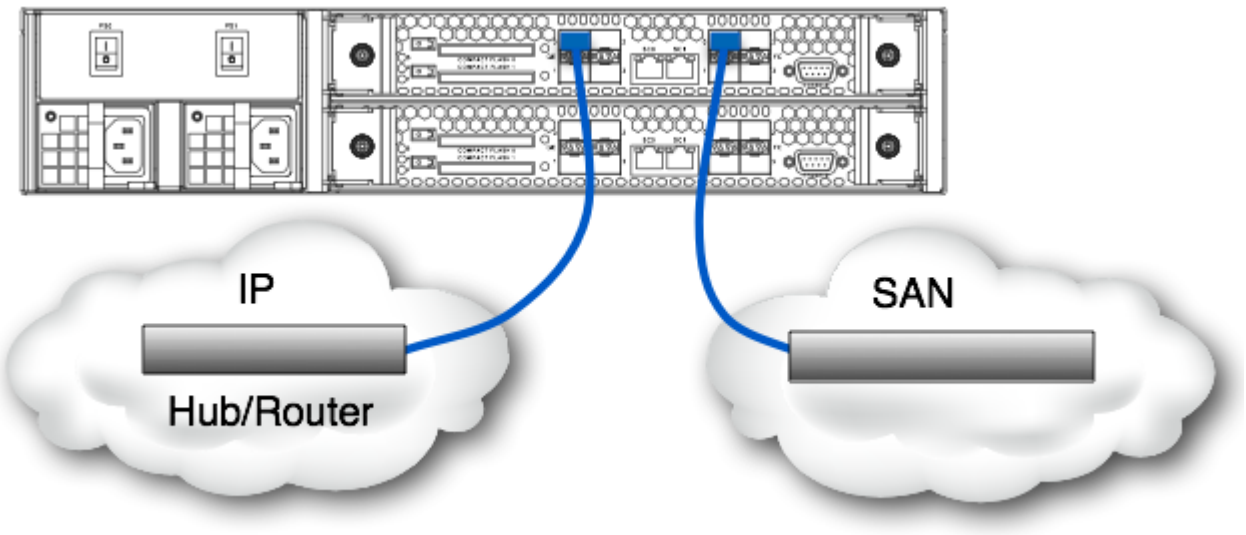


Figure 6-2 Connecting the ONStor Cougar 6000 Series NAS Gateway to the SAN

Note - Some SANs might not require all four fibre channel ports. If you are connecting only two fibre channel ports, you can optimize the fibre channel throughput by connecting any port in the first pair (ports 0 and 1), then connecting any port in the second pair (ports 2 and 3). We recommend connecting ports in the following order:

- connect link 0 first
- then connect link 2

If you need to connect additional ports:

- connect link 1
- then connect link 3

Step 3: Repeat Steps 1 and 2 for any remaining cables.

Note - Arranging cables can help keep an orderly and safe work environment and facilitate your managing the ONStor Cougar 6000 Series NAS Gateway.

Warning - The laser signal supported on the ONStor Cougar 6000 Series NAS Gateway's optical transceivers has been categorized as a Class 1 laser. Per the *IEC 825-1: 1993* and *CDRH, 21 CFR Laser Safety Requirements*, the ONStor Cougar 6000 Series NAS Gateway's laser is considered safe for casual contact with the human eye. Always operate the laser components in a manner compliant with the *IEC 825-1: 1993* and *CDRH, 21 CFR Laser Safety Requirements*. Misuse of the laser or prolonged exposure to the human eye has the possibility of causing personal injury. Even though the laser from the SF4400's optical transceivers is safe for the human eye, we strongly recommend that you keep the laser from contact with anyone's eye.

Verifying That the ONStor Cougar 6000 Series NAS Gateway is Operating

After you have connected the ONStor Cougar 6000 Series NAS Gateway to the network, observe the LEDs and other visual indicators to verify that it has booted and the system, fans, and power supplies are operating correctly:

Step 1: The system, power supply, and fan LEDs should be glowing steadily green. Figure 6-3 shows the fascia with the status LEDs.

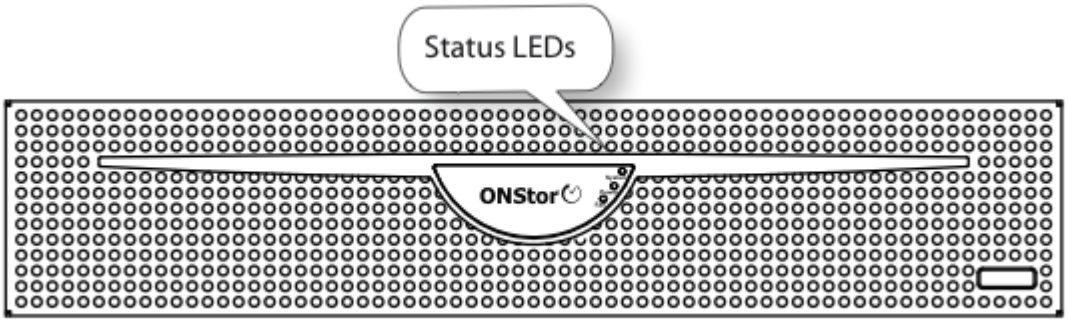


Figure 6-3 Cougar Fascia Status LEDs

Step 2: If any of the status LEDs are not green, check the LEDs on the rear of the NAS Blades. Figure 6-4 shows the NAS blade status LEDs.

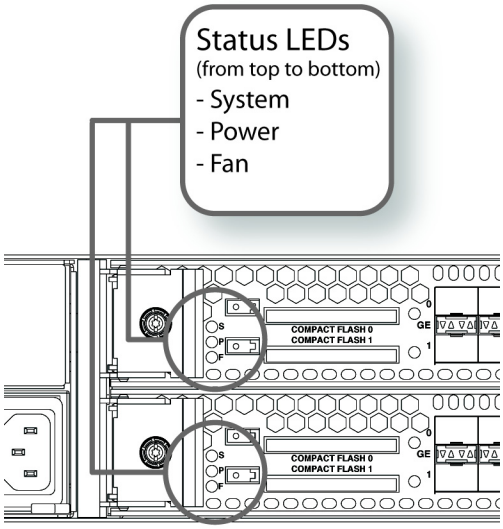


Figure 6-4 System, Power, and Fan Status LEDs on the NAS Blade

Table 6-1 describes the System, Power, and Fan LEDs and what operating states they report.

Table 6-1: NAS Blade Status LEDs

LED	Behavior
System	Flashing green - System booting
	Solid green - All processors up in runtime
	Red - Any processor has crashed
Power Supply	Green - Both supplies OK
	Red - One supply is not up
Fan	Green - All fans at normal speed
	Red - One or more fans have locked rotor or fans are at full speed due to temperature condition

Step 3: The GE and FC port LEDs (see Figure 6-5) on the NAS Blades should be glowing steadily green when operating normally. Table 6-2 describes the GE and FC LED states.

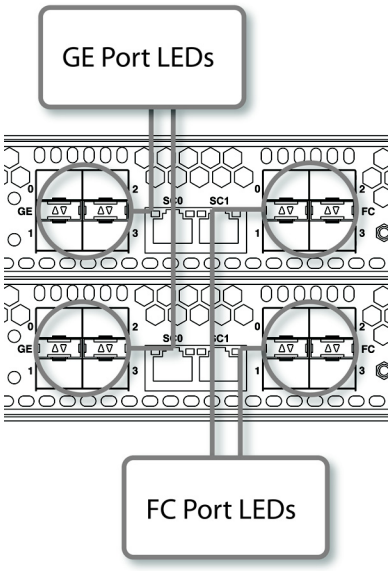


Figure 6-5 Module Status LEDs

Table 6-2: Port LED Color and Operating State

LED Name	LED color
GE Port	Steady green - Link up
	Flashing green - Activity
	Amber - Port enabled, link down
	Off - Port disabled
FC Port	Steady green - Link up
	Flashing green - Activity
	Amber - Port enabled, link down
	Off - Port disabled

Logging into the ONStor Cougar 6000 Series NAS Gateway

To configure the ONStor Cougar 6000 Series NAS Gateway for the procedures in this manual, we recommend using the default admin.

To Log In to The ONStor Cougar 6000 Series NAS Gateway

Step 1: Log in as default admin (called *admin*) with the default password (*password*). For example:

Login: admin

Password: password

Step 2: Check the ONStor Cougar 6000 Series NAS Gateway's state by running the following commands:

system show chassis

The chassis configuration should show that all modules have an operating state of *Up*.

vsvr show

interface show interface

interface show ip

system version

system version -s

lun show all

Step 3: If modules show any operating state other than *Up*, you can attempt to reboot the NAS Gateway by issuing the **system reboot** command.

Step 4: Repeat Step 2 after the module reboots.

- If the modules are in the *Up* state, run the **system show version** command, and note the system software version. The system software version string will be in a form similar to:

```
1.0.0-111303 : Wed Nov 13 16:20:49 2003
```

If the modules are still not in the *Up* state, contact ONStor Customer Support through `support@onstor.com` or the phone number listed on the inside cover of this document.

For additional set up information, consult the following documents:

- *ONStor EverON Version 4.0.0.0 System Administrator's Guide*
- *ONStor EverON Version 4.0.0.0 Command Reference*

Chapter 7: Clustering and Virtual Servers

This chapter contains the following sections:

Setting the System Time and Basic Cluster Configuration

Synchronize the system time between the NAS Blades Management Virtual Server and the network.

Set the System Time

Step 1: From each NAS Blade, set the NAS Blade's NTP client to listen for a time signal for the cluster by issuing the **system time ntp server** command. For example, to configure *Snowman* to use the time signal from the time source at 10.2.1.234, you would run the following command:

system time ntp server -a 10.2.1.234

Step 2: Verify NTP.

system time show -v

Add the NAS Blade to a Cluster

Use the following commands to add the NAS Blade to a cluster.

To Add a NAS Blade to a Cluster

Step 1: Run the following command:

cluster show cluster

Step 2: Add the NAS Blade to the cluster.

cluster add nasgateway *NASGATEWAYNAME* **-a** *IPADDR*

Step 3: Commit the change.

cluster commit

The NAS Blade you just added reboots and joins the cluster.

For additional information, see the *ONStor EverON High Availability Cluster Configuration Guide*.

Adding the NAS Blade to a Domain

For a client to be able to access the NAS Blade, the NAS Blade must be part of a domain. There are two steps to add the NAS Blade to a domain. Actually, adding it to the domain and then configuring the Domain Name Server (DNS) resolver.

To Add a NAS Blade to a Domain

Step 1: You add the NAS Blade to a domain using one of the following commands, depending on the platform. To properly complete the command, you need to know the name of the domain, the IP address for the domain controller, and the administrator login name.

On a Windows platform:

domain add windows *DOMAINNAME HOSTNAME*

For example, to add the NAS Blade to a Windows domain named *effigy* whose domain controller is at the IP address 10.2.128.141, run the following command:

domain add windows effigy 10.2.128.141

- On a UNIX platform, the command is as follows:

domain add nis *DOMAINNAME HOSTNAME*

Step 2: Add the IP address for the NAS Blade to the DNS server. This enables a client to access the NAS Blade by name rather than having to use the IP address.

Step 3: You add the IP address for the NAS Blade to the DNS server by editing the DNS resolver configuration file. (The DNS resolver configuration file contains keyword/value pairs, and you need to add the DNS server's IP address value for the *nameserver* keyword. In addition, you can add domain and search information.) Use the following command to edit the configuration file:

system dnsconfigure resolver

Enter the **nameserver** keyword and the IP address value into the file that opens, along with domain and search information.

nameserver *IP address*

Domain *domain name*

Search *list_of_domains*

For example, if the IP address of the NAS Blade is 10.3.35.1, you add the following to the file:

nameserver 10.3.35.1

The NAS Blade is now added to the domain and can be located by the DNS name server.

Step 4: Display the settings.

system dnsconfigure show

Configuration Tasks in the Management Virtual Server Context

You perform the configuration tasks in this section from within the management virtual server context rather than the global context. Once you change to this context, the commands you enter act only on the management virtual server itself.

In the management virtual server, you create two volumes (also referred to as file systems) and add references to these volumes in the DNS resolver configuration file. You also create interfaces to allow access to the server and add a route to the interfaces. The following steps take you through this process.

To Set the Management Virtual Server Context

- Set the context to the management virtual server.

  vsvr set *VIRTUALSERVER*

  You reference the management virtual server by name, which always begins with the name string "VS_MGMT" followed by a numerical ID. For example, if the management virtual server on the NAS Blade is named *VS_MGMT_512*, the command looks as follows:

  vsvr set VS_MGMT_512

  After you change to the management virtual server domain, the terminal prompt, assuming the NAS Blade is called *onstor1_lab*, is as follows:

  onstor1_lab VS_MGMT_512>

Create Volumes on the Management Virtual Server

You need to create two volumes on the management virtual server—a management volume and a core volume. Each volume must be connected to an available LUN. Both volumes have specific management uses. Therefore, customers should *not* use either of these volumes for client data storage:

Since you are working in the context of the management virtual server, you create the volumes specifying the available LUNs to which they should be connected. If necessary, before creating these volumes run the **lun show all** command to see the available (free) LUNs.

Keep in mind the following information before creating these two volumes:

- **Management volume**—A management volume is used for Network Data Management Protocol (NDMP) buffering and for backup purposes. This volume is mounted by default. The management volume also holds all system logs, including output from the **system get all** command, which tracks configuration and troubleshooting information.
  - The management volume size should be at least ten (10) GB and preferably should be twenty (20) GB.
  - While the management volume must use at least one LUN, the number of LUNs it uses does not matter.

  - Management volume use is not performance critical. Therefore, if your storage configuration includes multiple types of storage, consider using your slowest storage for the management volume.
  - Management volume availability is important.
  - The management volume, although accessible through NFS and CIFS, should never be used to store your own data files. Because it uses the management volume for administrative purposes, the NAS Blade may fill, delete, and overwrite files on the volume without notice.

- **Core volume**—The core volume's sole purpose is as a repository for the system to dump its raw memory in the event of a panic, thus preserving the raw memory for later analysis. Core dumps are automatically generated if the NAS Blade fails for some reason.
  - The core volume does not contain a readable file system and does not appear as mounted.
  - The amount of memory in the core volume's node owner dictates the volume's minimum size. If you attempt to create a core volume too small for the node, the system prints an error and does not create the core volume.

To Create the Management Volume and Core Volume

Step 1: From the management virtual server context, run the following command:

system create mgmtVolume *LUN*

For example, if you are working in the management virtual server context and there is a free LUN device called *NEXSAN_5000402001ec0590_6DCABA41*, you create the management volume as follows:

system create mgmtVolume NEXSAN_5000402001ec0590_6DCABA41

Step 2: Create the core volume. The command to create the core volume is as follows:

system create corevolume *core volume name LUN*

For example, to create a core volume called *core1* connected to the free LUN called *NEXSAN_5000402001ec0590_6DCABAA6*, you use this command:

system create corevolume core1
NEXSAN_5000402001ec0590_6DCABAA6

Step 3: You may want to verify that the two volumes were created correctly. Run the following command to see the volumes created on the management virtual server:

volume show

This command displays the following report for the *VS_MGMT_512* management virtual server:

Name	Status	Type	Current (MiB)	Hard Quota	Used	Avail	Usage	VirtualServer

vol_mgmt_512	Mounted	Standard	9408.62	No Limit	34.62	9374.01	0.37 %	VS_MGMT_512
core1	Not Mounted	Core	0.00	No Limit	0.00	0.00	0.00 %	VS_MGMT_512

You might also want to verify that the two volumes are associated to the LUNs you designated. Use the **lun show all** command. For example, the **lun show all** command displays the following information for the node *onstor1_lab*:

```
All devices known to PCC.
=========================
Device Name          Model   Raid    Size(MB)  State      Cluster         Volume
NEXSAN_5000402001
ec0590_6DCABAB2      Disk   Raid-5   9536.62   free      onstor1_lab
NEXSAN_5000402001
ec0590_6DCABA41      Disk   Raid-5   9536.62   used      onstor1_lab
vol_mgmt_512
NEXSAN_5000402001
ec0590_6DCABAA6      Disk   Raid-5   9536.62   used      onstor1_lab    core1
```

Create Interface and Route to the Management Virtual Server

Next, you need to create an interface to the management virtual server. An interface is required for client access to this server, and to any other server. The interface becomes part of the network stack for access between the client and the server.

You should create the interface to the management virtual server while you are still within the management virtual server domain context.

Step 1: To create an interface, you need to specify a port. Use the **lport show** command to see the available ports. In particular, you need to find a port whose operation status is *UP*. The **lport show** command produces a report similar to the following:

Table 7-1: Logical Port Table

Name	Admin	Operation	Mode	IPCnt	PrefPort	ActPort	Ports
fp1.0	UP	UP	single	0	N/A	fp1.0	fp1.0
fp1.1	UP	DOWN	single	0	N/A	fp1.1	fp1.1
fp1.2	UP	DOWN	single	0	N/A	fp1.2	fp1.2
fp1.3	UP	DOWN	single	0	N/A	fp1.3	fp1.3

Step 2: Create an interface to the management virtual server.

When you create the interface, you provide a name for the interface, associate it to a logical port, and assign the interface an IP address. Use the following command:

- the **-l** option lets you specify the logical port for the interface
- the **-s** option lets you specify whether the interface is enabled or disabled
- the **-a** option lets you specify the IP address

interface create *interface name* **-l** *logical port* **-s enable|disable -a** *IP address*

For example, the following command creates an interface called *mgmt* using the logical port *fp1.0* and assigns it the IP address *10.3.35.52/16*. The interface is enabled.

int create mgmt -l fp1.0 -s enable -a 10.3.35.52/16

Step 3: Add a route.

A route is associated to an interface and is the means by which the the interface is accessed. Run the following command to add a route:

route add default -g *IP address*

For example, the following command adds a route for an interface whose IP address is *10.3.30.1*:

route add default -g 10.3.30.1

Step 4: Exit the management virtual server context.

This completes the installation steps that involve the management virtual server. Use the following command to exit the management virtual server context and return to the global context:

vsvr clear

To indicate that you are in the global domain, the terminal prompt displays only the node and no longer displays the management virtual server name.

Configuration Tasks for Virtual Servers

This section covers the installation and configuration tasks for logical virtual servers, the servers that handle client data storage. These servers are referred to as *virtual servers*, but you might think of them as virtual file servers.

Create and Configure a Virtual Server for Data Storage

After completing the configuration of the management virtual server, you create and configure the virtual servers on the NAS Blade that will be used for client data storage. You create the virtual server by creating an interface for the server—assigning it an interface name, logical port, and IP address. Then, you add a route to the virtual server interface.

Step 1: Start by checking the logical virtual servers already created for the NAS Blade. Use this command to see all virtual servers on the node:

vsvr show

This command produces a report such as the following:

```
Virtual servers on nas gateway onstor1_lab
ID  State                              Name
=================================================
1    Enabled                            VS_MGMT_512
```

Note - Only the management virtual server, *VM_MGMT_512*, is defined for the node *onstor1_lab*.

Step 2: Create a logical virtual server within the node and change to that server's domain context. Run the following command:

vsvr create *virtual server name*

For example, this command creates a logical virtual server called *training* on the NAS Blade *onstor1_lab* and sets the context to that server:

vsvr create training

The steps that follow pertain to this particular virtual server and commands are given from within its context.

Step 3: Create an interface for a virtual server.

Use the following command (the **-l** option lets you specify the logical port for the interface, the **-s** option lets you indicate the interface status—either enabled or disabled—and the **-a** option lets you specify the IP address):

interface create *virtual server name* **-l** *logical port* **-s enable|disable -a** *IP address*

For example, this command creates an interface to the logical virtual server *training*.

In addition, it assigns the server the logical port *fp1.0*, enables the server, and gives it the IP address *10.4.43.35/16*.

int create training -l fp1.0 -s enable -a 10.4.43.35/16

Note - You can use the same logical port for more than one server.

Step 4: Add a route to the virtual server interface to give clients access to the interface. Run the following command:

route add default -g *IP address*

For example, the following command adds a route to the *training* virtual server interface at the IP address *10.3.35.1*:

route add default -g 10.3.35.1

Step 5: Edit the DNS resolver configuration file using the command **system dnsconfigure resolver**. Enter the *nameserver* keyword and the IP address value into the file that opens, along with domain and search information.

nameserver IP address

Domain domain name

Search list_of_domains

For example, if the IP address is 10.3.35.1, you add the following to the file:

nameserver 10.3.35.1

Add Virtual Server to Network Domain

Once a virtual server is configured, you can add it to the network domain. You may add a virtual server to a Windows Common Internet File System (CIFS) domain and/or a UNIX Network File System (NFS) domain.

Step 1: Set a domain for the virtual server. The domain may be either a Windows domain—a Domain Name Server (DNS) domain—or a UNIX Network Information Service (NIS) domain. As part of the command, you specify the domain—either *windows* or *nis*—along with the domain name and, if you are specifying a Windows domain, the administrator user name. The following command sets the domain:

vsvr set domain windows|nis *domainname adminuser*

For example, this command sets a Windows domain called *cslab* whose administrator user name is *administrator*. (You are prompted for the *administrator* password after entering this command.)

vsvr set domain windows cslab administrator

Note - For this command to work, you must previously have defined a Windows and/or a NIS domain using the command **domain add windows|nis**.

After the command completes, you can view the results using the command **vsvr show all**, which produces a report of the virtual servers on the node. Notice that, in addition to the management virtual server *VS_MGMT_512* on the *onstor1_lab* node, there is now a *TRAINING* virtual server.:

```
Virtual servers on nas gateway onstor1_lab
ID  State                              Name
================================================
1    Enabled                            VS_MGMT_512
2    Disabled                           TRAINING
```

Step 2: Enable the virtual server within the domain. When you configure a virtual server, you do so while it is disabled. By default, when a virtual server is added to a domain, it is disabled. At this point, you need to enable the virtual server. Use this command:

vsvr enable

Step 3: Create a storage area—a data storage volume—for the virtual server. Use the following command, specifying a name for the data storage volume and a LUN for the volume. (Use the **lun show all** command to see the list of free LUNs.)

volume create *volumename LUN*

For example, this command creates a volume called *training* connected to the LUN *NEXSAN_5000402001ec0590_6DCABAB2*:

volume create training NEXSAN_5000402001ec0590_6DCABAB2

Create Share Point for the Virtual Server

You need to create a share point for the virtual server volume or data storage file. A share point essentially puts the server's volume on the network and makes it accessible to clients. This action is comparable to mounting a file system (in UNIX terms) or sharing computer files or directories across a network.

After creating a share point, you must also set up the correct security permissions and privileges.

Step 1: Add the virtual server data storage volume to the CIFS network.

You need to specify the volume name, a *SHARENAME* for the volume, and the path to the volume. The *SHARENAME* is the name that is visible to clients. Run the following CIFS command:

cifs share add *VOLNAME SHARENAME PATHNAME*

For example, this command creates a share point for the *training* storage volume, gives it the name *techpub*, and specifies that the path to *techpub* is the root directory, represented by the back slash (**):

**cifs share add training techpub **

Step 2: Set the security permissions for the share point.

Add the necessary access privileges and security permissions to the share point so that clients can access it. ONStor follows the Windows security model for the node: it grants a user deemed to be an *administrator* all privileges (*admin* privileges) and all other users read-only privileges (*exec* privileges). Use this command to grant security privileges, designating either a user or a group and setting the scope of the granted privileges to the entire cluster or the virtual server: (On a UNIX system, the default security permissions for a file system are encoded as *755*. That is, a *root* user has read, write, and edit permissions and all other users have read only permissions.)

priv add {allow|deny} {user|group} *IDENTITY PRIVILEGES* **{cluster|vsvr [***VSVR_NAME***]}**

For example, the following command grants *administrator* security privileges to the user *cslab*. Furthermore, the user's privileges span the entire cluster:

priv add allow user cslab\administrator CLUSTER cluster

Step 3: At this point, the node is operational and can be accessed by Windows clients. You can verify this by using the following command:

cifs show

This command displays the storage volumes available on CIFS. For example, you might see the following output:

```
VSCAN$
IPC$
techpub
```

You can display more information on a specific volume by using the following command:

cifs show -v *VOLNAME*

For example, use the following command to see more information on the *techpub* volume, which produces a report showing the volume's share name, the volume name, and the path to the volume:

cifs show -v techpub

```
Share name: techpub
Volume: training
Path: \
```

If your setup includes providing client access to the node from a UNIX system, you must also create a Network File System (NFS) share point for the data storage volume. Follow these steps on a UNIX system:

Step 1: Create and add the share point for the volume. Use the NFS command:

nfs share add *PATHNAME* **-o** *OPTIONS*

For example, to create an NFS share point for the *training* volume and set up some access privileges, you might use the following command:

nfs share add /training -o rw=*;no_root_squash=*

The data storage volume should now be accessible to UNIX clients.

Chapter 8: EMRS and Snapshots

This chapter contains the following sections:

Configuration of Additional Utilities

You may also install additional utilities that help with troubleshooting and supporting any problems that might occur on the node. These additional utilities include:

- Event Monitoring Reporting Service (EMRS)—Monitors the node, collects information for troubleshooting, and sends email when a change event occurs to Customer Support at ONStor.
- Snapshot—Records changes made to an entire data storage volume at predefined intervals, and can be used to recover data.

Event Monitoring and Report Service

EMRS provides extensive support capabilities. Not only does it collect information useful for troubleshooting NAS Blade problems, it also automatically sends email notification messages to Customer Support at ONStor. The EMRS reporting can occur without the client's knowledge or even when the client is not aware of a problem.

Use the **autosupport** command to set up EMRS and email notification. This command has the following options:

Table 8-1: EMRS Options

clear	clear autosupport related info
email	autosupport email option
emrs	EMRS commands
generate	generate instant autosupport report
schedule	schedule for auto support report generation
show	show autosupport related info
state	modify autosupport state

When using the **autosupport** command to setup EMRS, you can enable or disable EMRS, configure EMRS for a proxy server, and enable or disable the automatic sending of EMRS data. Use the **autosupport emrs show** command to see the current EMRS configuration on a NAS Blade. It produces a report similar to the following:

```
Virtual servers on nas gateway onstor1_lab
ID  State                              Name
================================================
1    Enabled                            VS_MGMT_512
2    Enabled                            TRAINING
```

For additional information, see the *ONStor EverON Version 4.0.0.0 Command Reference*.

Snapshots

Snapshots is a utility that is useful for recovering data that is mistakenly deleted. The utility takes an initial picture of the entire data storage volume. Then, according to a schedule you define, the utility takes another picture of the entire data storage volume and saves the delta between the two pictures. Therefore, it keeps a running track of data storage changes to file systems made between successive snapshots of the volume.

By default, snapshots are enabled on a new volume, but can be disabled. The snapshots schedule is approximately every four hours, but this, too, can be modified.

Use the **snapshot** command to setup this utility.

To see how the utility is currently defined for a volume, use this command:

snapshot show *VOLNAME* **{schedule | list | usage}**

For example, the command **snapshot show vol_mgmt_512 schedule** displays the following report:

```
** snapshot scheduling currently disabled for this volume **
  schedule
  ========
   0  2  8 @8 12 16 20
```

For more information, see the snapshot section of the *ONStor EverON Version 4.0.0.0 Command Reference*.

Appendix A: Approvals and Certifications

The appendix contains the following sections:

Approvals and Certifications

This section details the regulatory notices, agency approvals, and certifications for the ONStor Cougar 6000 Series NAS Gateway family of NAS Gateway products. ONStor declares that its models of ONStor Cougar 6000 Series NAS Gateway comply with the following sections.

Compliances

ONStor NAS Gateway products comply with the standards of:

- European Union Evaluation
- ETL/cETL Listing for North America
- FCC Declaration of Conformity, United States
- Voluntary Control Council for Interference (VCCI), Japan
- Australian Communications Authority (ACA) Compliance

European Union Evaluation

The ONStor family of NAS Gateway products complies with the European Union standards shown in Table B-5.

Table 9: European Union Standards

Designation Standard	Standard
CENELEC EN 55022:1998	Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment.
CENELEC EN 55024:1998	Information Technology Equipment - Immunity Characteristics Limits and Methods of Measurement CISPR 24:1997, Modified.
CENELEC EN 60950-1	Safety of Information Technology Equipment, Including Electrical Business Equipment.
EN 61000-3-2:2000 (IEC 1000-3-2)	Electromagnetic compatibility (EMC). Limits for harmonic current emissions (equipment input current up to and including 16 A per phase)
EN 61000-3-3:2001 (IEC 1000-3-3)	Electromagnetic compatibility (EMC). Limits for harmonic current emissions (equipment input current up to and including 16 A per phase)

The Commonwealth of Europe (CE) mark affixed to each model of ONStor Cougar 6000 Series NAS Gateway indicates its compliance with the listed standards and the EMC Directive and the Low Voltage Directive of the European Union. Figure B-22 shows the CE mark.

Figure 1 CE mark

Caution - The ONStor Cougar 6000 Series NAS Gateway is a Class A product and might cause radio interference in a domestic environment. If such interference occurs, the user may be required to take adequate measures.

ETL/cETL Listing for North America

The ONStor 6000 family of NAS Gateway products complies with the Canadian standards shown in Table B-6.

Table 10: United States and Canadian Safety Standards

Designation	Standard
ANSI/UL 60950-1	UL Standard for Safety for Information Technology Equipment, Part 1
CAN/CSA C22.2 No. 60950-1	Safety of Information Technology Equipment, Including: Electrical Business Equipment First Edition.

The Edison Test Laboratories (ETL/cETL) mark affixed to each ONStor Cougar 6000 Series NAS Gateway unit indicates its compliance with the listed standards. Figure B-23 shows the ETL/ cETL mark.

Figure 2 ETL Mark

FCC Declaration of Conformity, United States

The ONStor 6000 family of NAS Gateway products complies with the United States of America's Federal Communications Commissions (FCC) Part 15 standards shown in Table B-7.

Table 11: FCC Conformity Standards

Designation	Standard
FCC Part 15, Class A	Radio Frequency Devices: • 15.107 Conducted Limits • 15.109 Radiated Emissions Limits

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Warning - Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The Federal Communications Commissions (FCC) mark affixed to each ONStor Cougar 6000 Series NAS Gateway unit indicates its compliance with the listed standards. Figure B-24 shows the FCC mark.

Figure 3 FCC mark

Voluntary Control Council for Interference (VCCI), Japan

The ONStor Cougar 6000 Series NAS Gateway products complies with the VCCI emission certification in Japan shown in Table B-8.The Voluntary Control Council for Interference (VCCI) mark affixed to each ONStor Cougar 6000 Series NAS Gateway unit indicates its compliance with the listed standards. Figure B-25 shows the VCCI mark.

Table 12: VCCI Standard for Japan

Designation	Standard
VCCI V-3/2000.04	Emission limits and methods for ITE-Class A.

Figure 4 VCCI Mark

Australian Communications Authority (ACA) Compliance

The ONStor 6000 family of NAS Gateway products complies with the Australian Communications Authority's (ACA) EMI requirements shown in Table B-9.

Table 13: Australian Communications Authority EMI Requirements

Designation	Standard
AS/NZS 3548:1995	Limits and Methods of Radio Disturbance Characteristics of Information Technology Equipment.
AS/NZS 3260:1993	Approval and Test Specification - Safety of Information Technology Equipment, including: • Electrical business equipment, incorporating - Amendment 1 - Amendment 2 - Amendment 3

The C-tick or RCM Mark affixed to each ONStor Cougar 6000 Series NAS Gateway unit indicates its compliance with the listed standards. Figure B-26 shows the C-tick mark.

Figure 5 ACA C-tick mark

CB Scheme Certificate

The ONStor Cougar 6000 Series NAS Gateway products comply with the applicable requirements of the International Standards shown in Table B-10.

Table 14: CB Scheme Certificate

Designation	Standard
IEC 60950-1	Information Technology Equipment, Part 1