來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2011 年 11 月刊的《In The Boxing Ring》。延續自 4 月份來本月刊的格式變化，我們也有了一個新的外觀排版，這是因爲我們正繼續著手於 NBRS-5.0 發佈前的準備階段。在今年接下來的時間裡，每個月我們都將針對 NBRS-5.0 的一個話題展開探討（接下來的主要是關於 Network Box 的固件發佈的話題）。每月的提示板塊將會去除，取而代之的將是整個版面的關於現有產品 NBRS-3.0 的發佈更新的資訊。這個版頭將依然保留，主要概述本刊的新內容。

本月刊中，在第 2、3 頁，我們詳細介紹了 NBRS-5.0 的高可用性，複雜均衡和集群。Network Box 在基本網路層級上提供高可用性。然後進行擴展以提供集群和負載均衡（包括個人在 Network Boxes 集群的工作負載——採用備用的備份容量）。

高可靠性和負載均衡體現在對萬一發生的硬體故障提供持續性的服務，以及在網路層級上通過兩個或兩個以上的設備對流量負載進行擴容。集群將此功能擴展到應用層，IEEE 802.1d 通過生成樹協定方式支援它擴展爲第 2 層橋接器（包括支援透明模式部署）。

在第 4 頁，是這個月對 NBRS-3.0 的發佈的新特性和新修復的補丁的詳情。在可預見的未來幾年，我們將繼續 NBRS-3.0 的開發和提供技術支援。這一頁將讓您瞭解到我們核心產品的最新動態資訊。

您可以通過郵箱（nbhq@network-box.com）與我們總部取得聯繫，或者到我們的辦公地點親臨參觀指導。您還可以通過以下幾個對外網站對我們保持關注：

Twitter: http://twitter.com/networkbox
Facebook: http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse
LinkedIn: http://www.linkedin.com/company/network-box-corporation-limited

Mark Webb-Johnson
CTO, Network Box Corporation
2011 年 11 月

本 刊 概 要

NBRS-5.0 的高可用性，負載均衡和集群

高可用性是指當主要設備出現故障時使用其他多個硬體設備提供冗餘備份。主要設備（正常時網路流量所經過的設備）被稱爲“主機”，其他的被稱爲“備機”。 Network Box 在基本網路層級上提供高可用性。然後擴展以提供集群和負載均衡（包括個人在 Network Boxes 集群的工作負載——採用備用的備份容量）。

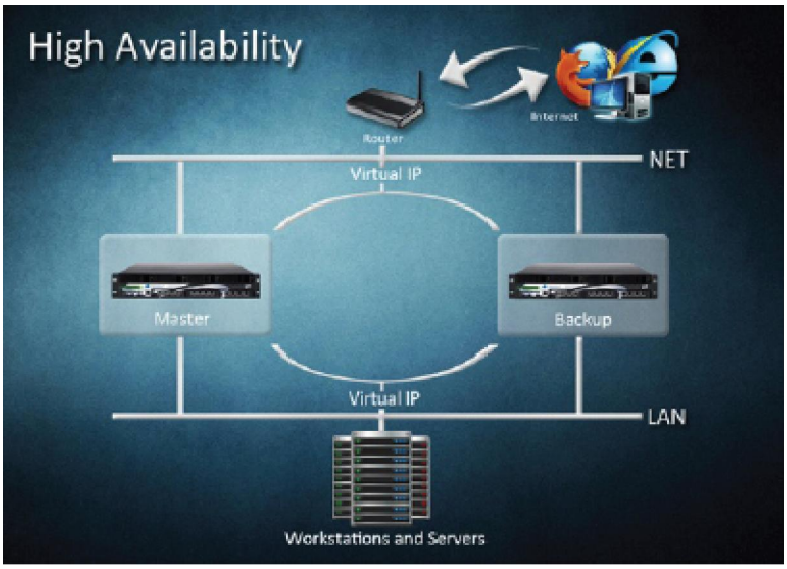
1、高可用性

Network Box NBRS-5.0 高可用性建立在 VRRP 協議行業標準的基礎上。

VRRP（Virtual Router Redundancy Protocol，虛擬路由器冗餘協議）是一個用來協商在一群主機中對一個或多個 IP 位址共用的協議，使在任何時候只有一台主機可以“持有”這些位址。協議將 Network Box 作爲一個虛擬路由器來使用，在 VRRP 群中故障路由器將角色轉移給另一個 Network Box（在這裡是指前者 Box 失效或停機維護）。VRRP 通過使用 IP 協定#112 和主播位址 224.0.0.18，在 VRRP 群中與不同的 Box 進行通信。

VRRP 監視介面和可訪問性，如果介面出現故障，介面狀態（載體，連接）顯示爲故障和主機狀態是故障的（例如：未通電或開關/電纜故障）。主機和備機不斷在它們各自之間廣播 VRRP 包，直到備機無法從主機那裡接收到 VRRP 包，在所有備機中將選舉出一個新的主機（根據優先順序）。在基本的 VRRP 協議中只允許針對單一的介面進行組的定義，而 Network Box 的 VRRP 卻將此擴展到了多個介面。基於這樣的設計，一個介面的失效將可以使故障主機的其它相關的介面的角色轉移到備機上。

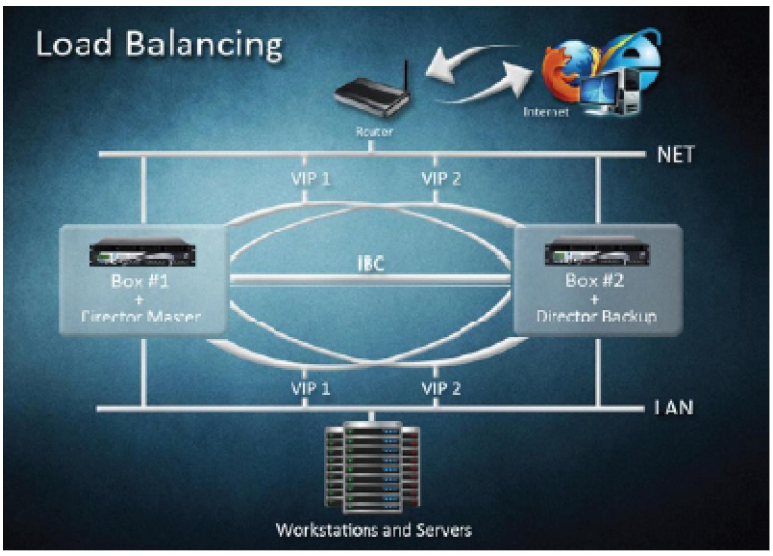
基本的 VRRP 協議是基於虛擬的 MAC 位址來進行轉移的，因此就局限於每一個 VRRP 組就是一個介面。然而，Network Box 卻是基於 IP 位址來進行轉移的（而不是 MAC 位址）。當故障發生的時候，需要通過無應答 ARP 包（及其它技術）來廣播 MAC 位址的變化，以允許多個 VRRP 組可以因此對這一相同的介面進行操作。一些網路設備可能會過濾掉這些無應答 ARP 包，這就會導致 Network Box 用於調整連接設備的 VRRP ARP 開關出現問題。若要解決這個問題，NBRS-5.0 也可以配置成使用直接廣播和其他技術去解決特定設備的這一局限性。



一個典型的高可用性配置方案需要使用兩個 Network Box，且分別需要有兩個介面（一個 NET 介面和一個 LAN 介面）。每個介面運行一個 VRRP 組，通過這兩個介面組來組成一個獨立無縫的主機/備機對。每個 Network Box 均有各自的 IP 位址（包括 LAN 和 NET），另外，一個或多個虛擬 IP 位址需要分配給 VRRP 位址集區。這樣，內部的工作站和伺服器就使用這些 VRRP 池中的位址通過具有主機角色的 Network Box 與外部進行通信。

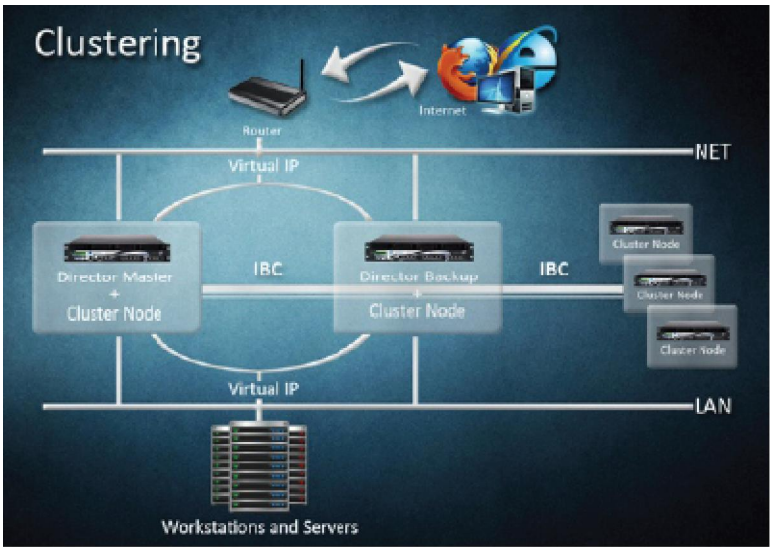
NBRS-5.0 包括一個可選的機制來同步高可用性組之間的連接跟蹤表，這樣的話，在 Box 切換角色的時候，連接就不會丟失了。但是，高層協定狀態（例如代理伺服器，虛擬私人網路絡等）是不能被同步的——因爲同步那些狀態的開銷並沒有太多的好處（鑒於要儘量減少不必要的 Box 切換次數）。

2、負載均衡



負載均衡通常與高可用性的工作方式是基本一致的，所不同的是 VRRP 組是運行於各自的介面上（box #1 是某一部分的主機，而 box #2 是另一部分的主機，它們互爲備份），爲 box 間的通信建立了 IBC（Box 間互聯）網路介面。來自工作站、伺服器、路由器的流量均被定向到指定的虛擬位址，或者由 Network Box 通過 IBC 在內部進行負載均衡（在主機中使用流量定向服務和 NAT 的方式）。在任一情況下，流量在網路層上就進行了負載均衡，所以，例如對於 SMTP 的流量，從負載均衡的角度來說，出站的 SMTP 流量可以被看做是從兩個 Box 中傳送出去的。

3、集群



除了高可用性和負載均衡（同樣在 NBRS-3.0 系統中也有提供），NBRS-5.0 介紹了一項新的技術叫做服務層集群。當負載均衡在網路層上工作時，集群就在應用層上工作（主要用於流量掃描）。

在這種架構下，服務工作進程（例如掃描，策略執行，郵件傳送等等）是在集群環境下執行的。具體地說，一個高可用性主備機對主要用於負責網路層（這裡在性能上並沒有什麼要求）的流量處理與控制，而類似掃描等服務的工作進程則放在了集群的各節點上。

各集群節點用於執行服務。它們通過內部通信來互相分享各自的服務負載水準，通常會將工作分派到當前負載水準最低的集群節點上。迴圈法分配方法對於負載均衡也是一個不錯的選擇。類似於負載均衡的配置，IBC 線路用於集群通信，與使用者網路分開（包括互聯網和局域網兩方面的網路）。兩個集群節點之間可以用對接的電纜線進行連接，或者使用冗餘的交換機（或 VLAN）來連接更大的集群內部通信網路。

4、透明模式和橋接

一個典型的高可用性配置工作於網路模型的第 3 層。從經驗上說，像 proxy-ARP（用於透明模式部署）這樣的技術沒有與高可用性或負載均衡配置一起工作。NBRS-5.0 所支援的第 2 層橋接，也可以用於透明模式部署。

Network Box NERS—5.0 第 2 層橋接支持 IEEE802.1d 生成樹協定（STP），允許在第 2 層透明網路上建立高可用性方式的部署，與同樣支援 IEEE802.1d 協議標準的交換機進行協同工作。在高可用性和負載均衡環境下所需要的透明容錯移轉和網路路由重定向，現在在 NBRS-5.0 中也可以獲得很好的支援。

總結

對於路由網路，萬一發生硬體故障，高可用性和負載均衡可使網路提供持續性服務，以及在網路層上，靈活控制通過兩個或多個設備的流量負載。集群把它擴展到應用層，IEEE802.1d 生成樹協定支援它擴展到第 2 層橋接網路（包括支援透明模式）。

2011 年 11 月 新特性

在 2011 年 11 月 1 日的星期二這一天，Network Box 將發佈這次的 Patch Tuesday 的補丁包，各區域 NOC 將會在此之後的 7 天內安排這些新的功能的發佈和更新工作。這個月的更新補丁包包括：

·各種內部 NOC 系統的功能增強；

· 合同續期階段許可狀態下 Box 的報告修正；

·最新版本的 Microsoft windows 的 NTLM 身份驗證系統、添加支援 PPTP 和網路 NTLM 系統運用 chap v2 的增強功能；

·與唯讀管理員和防火牆狀態相關的 my.network-box.com 管理介面的部分修改；

·Box Office 和支援系統的各種（主要是內部）增強功能；

在多數情況下，以上的修改並不會影響到正在運行的服務，也不需要硬體重啓。但在某些情況下（取決於具體配置），可能需要重啓設備。必要時您當地的區域 NOC 將會與您取得聯繫。

如果您還需要要關於這些的更多的資訊，請與您當地的區域 NOC 取得聯繫。他們將會進行相關的諮詢和安排。

微軟主動保護計畫（MAPP）

Network Box 成爲微軟主動保護計畫安全軟體供應商的一員已有相當長的一段時間了。微軟主動保護計畫的成員會先從微軟安全回應中心收到微軟每月的安全更新漏洞資訊。

當 MAPP 的合作夥伴提前收到漏洞資訊，他們會通過他們的軟體或設備，例如防病毒，基於網路的入侵偵測防禦系統或基於主機的入侵防禦系統向他們的客戶提供更新保護。你可以在微軟的 MAPP 網站找到更多有關 MAPP 的資訊。儘管有了這些保護，微軟建議用戶安裝安全更新，以儘快防止漏洞被利用。

網路安全猶如一場“軍備競賽”，不斷地縮短微軟安全更新發佈與漏洞被發佈這兩者之間的時間差。保持至少先行一步於駭客、惡意軟體製造者和其他網路犯罪，這是至關重要的。

MAPP 給安全軟體提供商提早獲得漏洞資訊。在這個程式之前，安全軟體供應商在公開發佈安全更新保護建立之前必須等待。通過 MAPP，安全軟體提供商可以更快地把保護特徵發佈給客戶。這是 Network Box 多年來一直在做的事情。

我們會儘快把最近發表的 Network Box MAPP 安全簽名的即時資料更新到 Network Box 安全響應網站上。這些安全簽名將會使用我們屢獲殊榮的 PUSH 更新技術推送到全球每個活躍的 Network Box 中。

2011 年 11 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	576	-7.1
特徵碼發包數	341,201	+3.8
防火牆攔截數(每 BOX)	800,877	-1.2
IDP 攔截數(每 BOX)	116,054	-0.3
垃圾郵件數(每 BOX)	17,095	+1.6
惡意軟體數(每 BOX)	503	-68.2
URL 攔截數(每 BOX)	180,156	+12.2
URL 訪問數(每 BOX)	3,919,564	+1.8

月刊工作人員

總編輯：

Mark Webb-Johnson

產品支援：

Michael Gazeley

Jason Law

Nick Jones

撰稿：

Network Box Australia

Network Box Hong Kong

Network Box UK

訂閱方式

您可以些電子郵件到：

Network Box Corporation

nbhq@network-box.com

或者寫信到以下地址：

Network Box Corporation

16th Floor, Metro Loft,

38 Kwai Hei Street,

Kwai Chung, Hong Kong

Tel: +852 2736-2078

Fax: +852 2736-2778