白皮書

選擇 Infoblox 應用 DDI 的原因

是時候從 *BIND* 和 *Microsoft* 移轉

目錄

打造 InfoRanks 的原因 3
不穩定的來源 4
InfoRanks 的實施 6
估計的排名 7
等級的信任間隔 8
區間範圍內的變異分析 9
系統分析 10
InfoRanks 與單一排名的範例 10
不穩定的例子 11
參考資料 12

在許多組織中，可提供可靠連結和存取互聯網的核心服務都仰賴免費和近乎免費的產品。 雖然價格可能相當誘人，但這些產品通常將帶來功能限制和管理效率低下的隱性成本。 在規劃目前網路中不可避免的成長和變化時，必須考量「免費」的自然限制以及核心服務如何將網路提升到全新水準。

DNS、DHCP 和 IPAM：簡史

最初，DNS 是一種存取網站和應用程式的便捷方法，而 DHCP 幾乎聞所未聞。 通常由十分了解的人來管理，並仰賴「免費」系統，例如 BIND/DHCPD 和 Microsoft DNS/DHCP。 有時，電子試算表是維護基本協議服務的根基（即 DNS 和 DHCP）。 這些系統通常透過由一小群專家維護的「自家打造」工具集來拓展。 當這些專家轉調至其他職務或組織時，便阻礙了營運和計劃決策。

IP 位址管理 (IPAM) 是後來的增強功能，有時與管理 DNS 和 DHCP 的人員中斷連線。 分配資源和定義網路的團隊並不是管理和定義名稱和位址的人員。

在整體 IT 策略中，這些系統的業務影響或可靠性常常被忽視，並且與哪個群組（營運、系統或網路）負責其維護也很少有一致的規則。 直至最近，組合 DNS、DHCP 和 IPAM（「DDI」）的概念才被採用。

現代網路中的 DDI

隨著過去 20 年對網路和流動性的驚人增長和仰賴，以及行動裝置使用的爆炸性增長，DNS 現在有望成為「萬靈丹」解決方案。

存取身份驗證、資料庫和其他後端資源的迫切需求，IPv6、物聯網以及幾乎所有其他技術現在都將網路核心焦點聚焦於 DDI 。 這增加了對極端可靠性、整合性和問責制的額外要求。 這些要送從未被充分考量為原始設計模型的環節之一。

雖然免費或開源解決方案能夠提供必要的服務，但它們可能需要大量的維運時間，並且缺乏目前現代網路中被視為「企業級」的穩健性。

企業也正在轉向更自動化的環境，特別是在雲端和虛擬空間之中。 然而，如果這些現有解決方案想要適應預期的自動化等級，則需要更高程度的客製化。 隨著 IPv6 越來越普及，透過電話讀取 IP 位址的機制早已一去不復返，困難度將進一步增加。 為了正確管理日益複雜的環境，必須採用可支援、可擴展、集中管理的 DDI 解決方案。

簡而言之，如果 DDI 服務停止運作，或變更需要太長時間才能實施，業務功能將受到負面影響，最終導致生產力和利潤損失。

C 級優先順序

KPMG 最近的一份報告列出了 CIO 的下列五大執行策略重點：

- 加速上市速度
- 營運數位化
- 轉向資料驅動
- 建立公眾信任
- 實施革新技術

在 DDI 領域，這些措施可能發展成為「保護業務」等倡議。
「提升營運速度」或「保護公司的聲譽」。

而在重新設計 DDI 基礎架構解決這類倡議時，不需要將太多努力花費在串連點之上，並發現傳統解決方案與現代整合解決方案的限制。

只有當您充分保護並減輕對資料的所有可能攻擊媒介，企業才能達到完全安全。 而 DNS 現在是 78% 的應用程式層級攻擊 (DDoS) 和 91% 的惡意軟體分發、命令與管控和資料的主要管道外洩。

只有當網路核心使用能夠處理基礎架構合規與保護、惡意軟體緩解以及整合式威脅管控和營運模式的系統，才能維護公司聲譽，以及向更資料驅動營運的進展。

而且，只有當 DDI 自動化到能夠支援雲端基礎架構所需的迅速和變化增長時，才能達成營運速度成長。

達成次世代資料中心承諾的路途可能相當艱鉅。 傳統的 DNS 基礎架構和在電子試算表中管理 IP 位址無法提供工作負載配置的效率、可見性或自動化：使得 IT 部門只能透過手動、耗時的流程部署核心網路服務。 真正的資料中心轉型不僅只是儲存和運算自動化，組織還需要網路自動化來達成敏捷、集中管理和極具擴展性的資料中心。

您需要清楚掌握所有裝置的位置、用途、正在與誰交流、長期下來如何變化，以及應該運用手頭有限資源聚焦的目標。

理想的系統

在當今環境中的 DDI 必須符合許多重要標準：

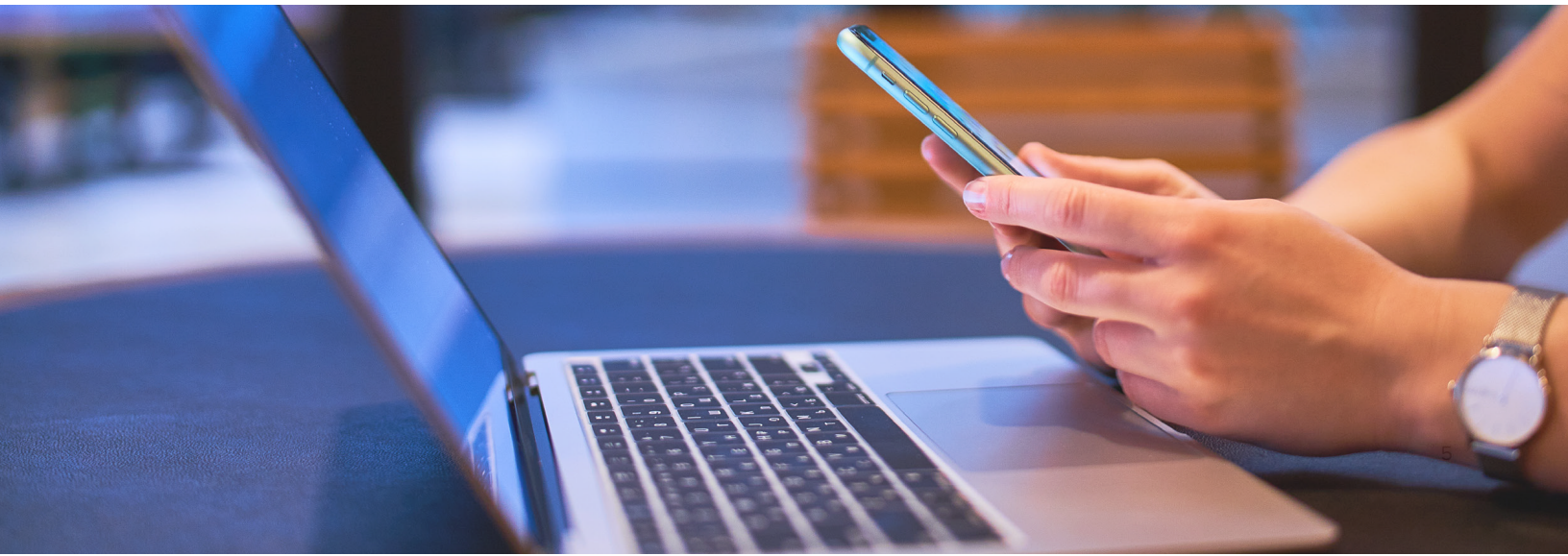
- 可靠的正常運行時間
- 變更容易
- 即時端點和拓撲可見性
- 整合至自動化系統
- 冗餘和/或迅速復原時間

因此，理想的系統應該是集中管理的，需要最少的資源來維護，並且易於部署和擴展。 亦應具備穩定性 、安全性並支援各種不同的需求。這些可能是高階管理員 、網站 / 桌面支援 、自動化任務、網路規劃和安全取證。

對於規劃和取證而言，「單一事實來源」便是關鍵。 提供單一地點的系統必須尋找任何裝置或網路訊息，而不是搜尋多個可能衝突或不同步的系統。

這將延伸到歷史增長模式、DNS 使用情況 & 趨勢的可見性，DHCP 租用和裝置歷史記錄。所有這些都是能夠迅速回應安全事件、排解網路問題和一般容量規劃的關鍵。

理想的解決方案還能夠與作為更大生態系統環節之一的其他系統進行互動，並動態地互相交流以便交換資訊。 自動化在目前是必須具備的。



這方面的例子包括：

- 對已標記為潛在惡意的 DNS 記錄的查詢，DNS 能夠透過回應原則區域「擷取」此記錄。 接著，能夠將該匹配傳送到裝置掃描程式，自動掃描相關系統尋找可能的問題，並在必要時發出警報，並隔離所述系統。
- DHCP 租用日誌能夠傳送到第三方日誌記錄系統，以便追蹤使用趨勢與事件的相關性
- 針對新建立的虛擬機器 IP 指派與回收的自動化系統，能夠將部署時間從數小時或數天縮短為幾分鐘。
- 標記惡意端點的端點安全系統能夠自動將此資訊推播到安全性原則中，防止使用者端聯絡所述端點。

當然，這些只是系統之間的自動化互動可以帶來輕鬆更改、即時端點和拓撲可見性以及與自動化系統整合的眾多範例中的幾個而已。

Infoblox 的優勢

舊式系統無法擴展

儘管 BIND 已成為 DNS 和 Internet 的業界標準，但它卻需要高水準的知識和技能才能正確實施和操作。 正確執行簡單任務涉及多個手動步驟（例如：當新增 / 修改 / 刪除記錄時，區域的序號必須遞增）。 在實施更複雜的配置和功能（例如 DNSSEC）時，存在某些陷阱，可能導致效能不可預測，甚至可能導致 DNS 完全中斷。

此外，雖然 BIND 支援 DNS，但它不提供達成效能監控和管理目標的整合報告，並且不提供與 IP 位址管理的整合，這將導致原生 DNS 記錄與 IPAM 中可能出現的內容之間存在差異。 BIND 的開發從未考量到自動化，因此並不包含用於簡單自動化 DNS 記錄變更的強大 API，這是聚焦 DDI 系統提供的功能。

整合 IPAM 與 DNS

將 IPAM 與 DNS 整合對於維持兩個系統的準確性和同步相當重要。 在網路上部署新裝置時，將先指派 IP 位址，接著通常會立即要求將主機新增至 DNS。 透過整合 DNS 和 IPAM，此流程轉化成單一步驟 - 同時建立 DNS 記錄與 IP 分配。 這不僅提升效率，且還減少了錯誤的可能性，因為數據不會被轉錄或轉發。隨著 IPv6 的不斷普及，對 IPAM 與 DNS 整合的需求只會不斷增加。

欲進一步提升 DNS 和 IPAM 的精準度，能新增探索元件。 將探索元件整合至 IPAM 中，將其從幾乎完全仰賴人工行動的系統轉換為「權威 IPAM」，該系統能夠讓網路管理員和安全營運商隨時查看網路上的內容。 與報告解決方案結合使用時，能夠長期追蹤 IP 位址的歷史記錄，這對於正確分析安全事件相當重要。

使用 Infoblox DDI，您擁有現代化的 DNS 服務系統，能夠透過下列方式解決許多相關問題：

- 將 DNS、DHCP、IP 位址管理和其他核心網路服務整合至單一平台中，並透過共用控制台進行管理
- 透過混合、公共、虛擬與私有雲端環境的整合功能，跨不同基礎架構集中編排 DDI 功能
- 存取豐富的整合報告和分析功能，進行容量規劃、資產管理、合規管控和審計
- 透過 RESTful API 與 Infoblox Grid 連結，與其他 IT 系統無縫整合，提升 IT 效率和自動化

Infoblox for DNS 對比 Microsoft DNS

在選擇與 Microsoft Active Directory 一同使用的 DNS 解決方案時，許多管理員只是簡單地選擇「Windows Server 隨附的內容」。 但是，使用非 Microsoft DNS 是有原因的。

- **安全**：組織需要為其外部 DNS 提供最佳解決方案，以應對遭受網路攻擊的情況。 可以使用第三方 DNS 解決方案，這些解決方案是從頭開始設計和建置的，並考慮了安全性。 組織的內部 DNS 結構同樣容易受到惡意威脅、惡意軟體、網路釣魚和資料外洩的影響。
- **可見性和單一檢視**：大多數組織都擁有異質的技術組合，精準的一站式可見性對於高效的合規性和管控相當重要。
- **營運效率**：透過利用自動化和工作流程而不是手動電子表格管理來優化營運支出。
- **智慧服務**：根據 DNS 的整合流量管控、網路負載平衡和服務監控為組織賦予巨大價值。 Microsoft IPAM 中的差距導致網路拓撲的目前狀態與 Microsoft Active Directory (AD) 中包含的資訊之間不一致。 這可能將導致使用者身份驗證和文件可用性等基本服務徹底中斷。

Infoblox IPAM 還能夠與 Microsoft AD 網站和服務無縫整合，並為 AD 和網路管理員彌補這一差距。 此外，Infoblox 跨越 Microsoft 樹系，並將整個 Microsoft 環境帶入整合管理的 GUI，提供前所未有的可見性、營運效率和服務正常運行時間。

如需詳細資訊，請參閱群組原則 MVP Jeremy Moskowitz 撰寫的「Microsoft 與非 Microsoft DNS：事實與虛構」。

Infoblox 與其他產品和生態系統整合

Infoblox 也提供與領先安全和管理技術的無縫整合。 我們透過開放 API 達成智慧自動化，並支援跨雲端和內部部署環境的工作負載。 我們的產品包括情境感知安全、進階威脅情資和生態系統整合。

作為更大安全生態系統的環節之一，Infoblox 還支援 REST 和 PERL API，例如以及根據事件的外站 API，能夠與安全基礎架構中的其他系統互動，在新增至 IPAM 時新增網路進行掃描、觸發裝置掃描及 / 或隔離 ·若終端裝置傳送與 RPZ 規則相符的查詢 (包括 Threat Insight) 等等。 此外，Infoblox 還與 Cisco ISE、McAfee 等 20 多間公司整合，且數量仍在持續增加。

結論

您應該做些什麼

「免費」系統，例如 BIND/DHCPD、Microsoft DNS/DHCP 和電子試算表，並不能完全符合現代網路的需求。 花時間檢查您的核心弱點並製定一項計劃，遷移至整合 IPAM 系統。

定義您現有的工作流程和 IPAM 流程，並檢視能夠改善的面向：

- 可靠的正常運行時間
- 變更容易
- 即時端點和拓撲可見性
- 整合至自動化系統
- 冗餘和/或迅速復原時間

Infoblox 也擁有良好的業績記錄，是市場先驅，擁有超過 50% 的市場份額與超過 8,000 名客戶，我們擁有大量資源能夠協助您做出這項決策：https://www.infoblox.com/resources/?category=Whitepaprs

後續步驟

請聯絡您的 Infoblox 業務團隊討論建議的部署架構。

企業總部
2390 Mission College Blvd, Ste。 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com