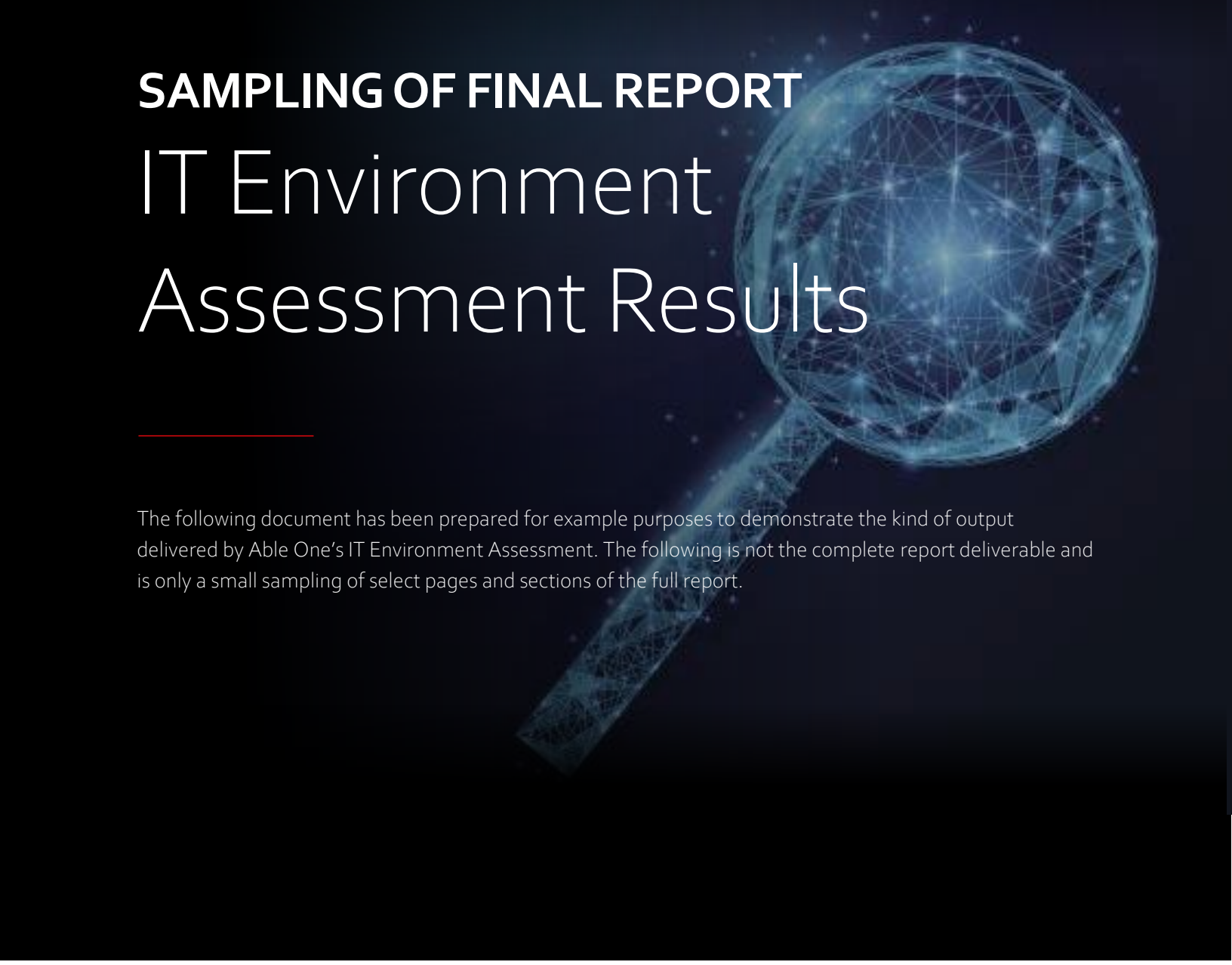
Able One

SAMPLING OF FINAL REPORT

IT Environment Assessment Results



The following document has been prepared for example purposes to demonstrate the kind of output delivered by Able One's IT Environment Assessment. The following is not the complete report deliverable and is only a small sampling of select pages and sections of the full report.

Prepared for:

EXAMPLE PURPOSES ONLY

Contents

Executive Summary (first two pages)

We recognize that minimizing disruption and its impact is a priority for Company Name. In light of the disruption from COVID-19 and the impact on resources, Company Name has decided to focus their attention on the following:

1. Company Name current IT posture versus best practices ("As is")
2. IT Disaster Recovery
3. Revisit BCP process with to determine what is "good enough" and what is necessary for a disaster recover plan and test.
4. Revisit security posture/risk management requirements to determine if updates are required in Phase 5 of our existing proposal.
5. Revisit Company Name business strategy, confirm and align "To Be" actions (ie. infrastructure, security, gaps)

As directed by Company Name, Systems Engineer Name, Able One's Senior System Engineer, performed a full manual review of the infrastructure as listed on Page 3, with a major focus on the operational status of the network, virtual infrastructure and servers.

In summary, we found that, while the overall Company Name infrastructure follows best practices of the industry, there are a number of improvements that can be implemented that will harden the environment against any downtime or interruption.

Four key findings and recommendations are as follows:

1. Network
    i. In order to minimize firm wide disruption to Company Name, it is recommended that you review and deploy a redundancy option for your switches
        - Company Equipment Name serves as a core switch of the network, providing communication between firewall and all the other edge switches.
            - It is a single point of failure and so any disruption to this core switch will result in an outage for the entire network
        - Company Equipment Name serves as a server rack switch, connecting entire server environment to the rest of the network.
            - It is a single point of failure and so any disruption to this switch will result in an outage for the entire virtual server environment.
        - Firewall servers as a single point of connectivity to the internet. Loss of firewall will lead to disruption for the entire environment.
        - All other switches also lack redundancy, and a loss of a single switch will lead to loss of access to that area of the building.

ii. Current Networking Equipment

- Networking devices are approaching or are already End of Life. It is recommended that Company Name replace all your networking hardware, and implement with redundancy in order to minimize any firm wide outages due to single points of failure as described above.

2. Servers

i. Company Name segments their infrastructure services across multiple servers. These services include domain services, file services, print services, medial workloads, etc. This type of segmentation is considered best practice in the industry:

- It reduces and balances the computing capacity among all virtual servers,
- It helps with issue resolution
- It improves maintenance capability and security

ii. Company Name should continue to segment servers and permanently delete unnecessary servers from your environment

iii. It is also recommended that you replace the end of life Windows 2008 R2 Servers as they are no longer supported by Microsoft:

- Review which if any applications are being used by the team and arrange to decommission or migrate them to new technology
- The list of servers and the applications can be found on Page 29

iv. With the recent rise in ransomware attacks, it is important to protect your environment from disruption:

- It is highly recommended that your current version Sophos antivirus be upgraded with the Intercept X component. It will protect against ransomware by preventing the attacker from encrypting your data
- It is not a matter of if but when companies will be breached. Although antivirus solutions and password protection and strength are very important, they do not replace the need for a corporate Breach Response Plan. As per our discussions regarding the upcoming IT Disaster Recovery Plan (DR) Project, it will be imperative for Company Name to revisit and prioritize your Business Continuity Plan which will take into account both the IT DR Plan and the Breach Response Plan.

3. Performance

i. No performance issues were identified in Company Name's environment. ie. There is minimal traffic and congestion

- Network Device Utilization ~ 20%, which is very much in line with best practices

ii. Storage

- Storage utilization on the V3700 is 91% which is outside of range for best practices. It is also off of warranty

Recommendations Summary (first page)

The recommendations are summarized and are sorted in priority and ease of implementation descending as per below. The detailed findings and recommendations can be found on Pages 5 – 37.

1. Network

1. Update firmware on all networking devices to the latest version
2. Review of all VPN users access
3. Implement of complex password requirements for all users
4. Review and cleanup of firewall policies
5. Replace all networking switches with newer models
6. Replace wireless access points with newer models
7. Implement redundancy on core switches
8. Implement redundant firewalls

2. Physical/Virtual Infrastructure

1. Update configuration of virtual machines to best practices
2. Purchase warranty/support for IBM v3700 SAN
3. Update vCenter Server to the latest available version
4. Update ESXi hosts to the latest available version
5. Update SAN firmware to the latest available version
6. Configure network redundancy between hosts and switches
7. Decommission IBM 3550 M4 server

3. Server and Software

1. Permanently delete unnecessary 4 servers from the environment
2. Migrate Sophos management to cloud version (with Intercept X component purchased)
3. Replace End of Life 2008 R2 servers with latest Windows 2019 server OS (see worksheet)

4. Domain Health and Configuration

1. Relocate DHCP role to domain controller

Network Overview (select sections)

The firewall (Cisco Firewall ASA 5516) is protecting the environment and providing VPN access to the infrastructure. It **represents a single point of failure in the network**, and in case of failure of any component, the **internet access** for the **entire company will be lost** until the firewall is replaced.

Best practices recommendation is to have **two redundant firewalls in automatic failover mode**, to prevent extended outage to the environment in case of hardware failure.

Switching environment is configured in "wheel and spokes" manner, which follows best practices, with few notable exceptions. In "wheel and spokes" design, "core" switches connect to firewall and all other switches, so a failure of a single "edge" switch brings down only a portion of network. Core switches in turn are typically designed with redundancy in mind, so a failure of a core switch doesn't affect the environment.

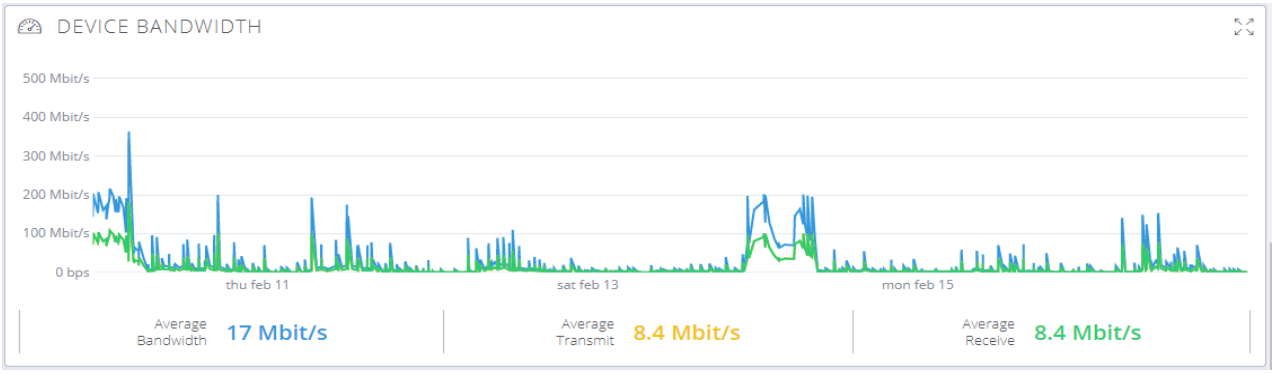
Company Equipment Name serves as a core switch of the network, providing communication between the firewall and all other edge switches. Currently, it is **a single point of failure**, and any disruption to Company Equipment Name will result in an **outage for the entire network**. It is highly recommended to have redundant core switches in stacked configuration to avoid such a scenario.

Additionally, switches Company Equipment Name and Company Equipment Name form a "daisy chain" (switches connecting to each other rather than core switch), so a failure of Company Equipment Name will cause an outage for all devices connected to Company Equipment Name as well. Due to the location of the switches, direct connection to Company Equipment Name might not be feasible. In such case, **redundancy for SW3 is recommended, both in cabling and physical chassis.**

Network Performance

FIREWALL (FW1)

Firewall is currently connected to synchronous 100 Mbit/s internet line, allowing for 100 Mbit/s upload and 100Mbit/s download speeds.

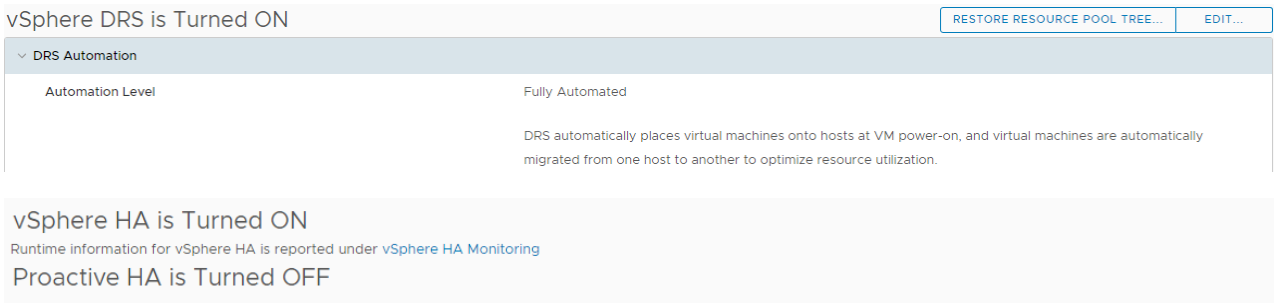


As seen from the graph above, **average speeds** throughout the week reach only 8.4 Mbit/s, with occasional spike reaching higher throughput.

Physical/Virtual Infrastructure Configuration Review (select sections)

Infrastructure Overview

The CONTOSO infrastructure is hosted on three Lenovo ThinkSystem VMWare ESXi hosts. These hosts connect to a vCenter 6.5 instance and use IBM v3700 SAN for storage. The existing configuration has **high availability (HA)** and **Distributed Resource Scheduler (DRS)** features are turned on. HA provides **automatic failover capabilities** in case of host failure. DRS provides automatic load balancing between the hosts, **minimizing load** on any one host. Both are following best practices for the environment.



In the event a physical host experiences a **hardware failure**, vCenter would automatically migrate and power up the affected virtual machines to one of the other two hosts causing **minimal impact to production**. Current infrastructure can survive failure of two hosts and still have all virtual machines running on the third host, however, performance will be negatively affected by memory utilization, as current memory requirements exceed capabilities of a single host. Two hosts can contain the entire environment **without impact to performance**.

VMware vCenter version is 6.5.0.21000 (Update 2b, build 8815520, June 28th, 2018) with the latest version available being Update 3k, build 16613358 from July 30, 2020. It is **recommended to update** vCenter server to the latest available version.

Physical Hardware

SAN (SAN-3700)

The CONTOSO ESXi hosts are utilizing standard SAN (IBM StoreWize V3700) storage implementation **for redundancy and protection** of the virtual machines.

Each host connects to the SAN via two 6Gbps direct-attached cables, creating redundancy not only between hosts but also between SAN and each individual host. Failure of any one (or specific multiple) component **will not impact** the environment. Current redundancy configuration follows best practices recommended by VMware.

The CONTOSO SAN storage pool is segmented into VMWare datastores. The screen shot below shows the existing datastores and their capacities. Datastores are following best practices in their configuration. Total amount of storage available for CONTOSO hosts is 11.18 TB with 10.2 TB (91%) of storage used.

Name	Status	Type	Datastore Cluster	Capacity	Free
v3700-SmallDatastore	Normal	VMFS 6		9.75 GB	8.34 GB
V3700DS	Normal	VMFS 5		11.18 TB	989.16 GB
VMHOST2	Normal	VMFS 6		22.25 GB	20.84 GB

V3700-SmallDatastore datastore is created to allow for High Availablity checks on datastore connectivity (HA requires at least 2 datastores to function properly).

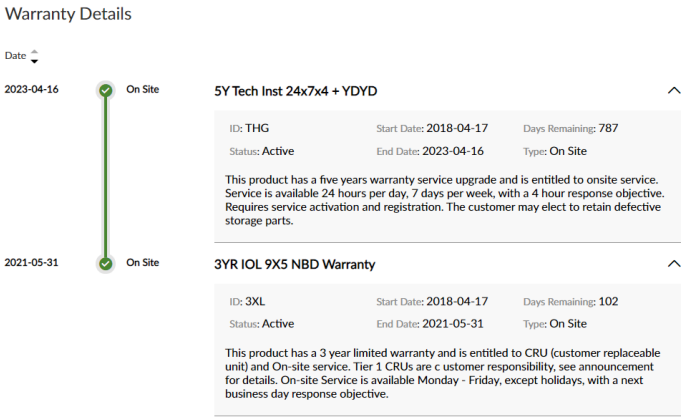
V3700DS datastore is the main storage location for CONTOSO virtual machine data.

Current SAN firmware version is 7.4.0.2, with latest available version 7.8.1.12. It is recommended that firmware is updated to the latest version.

Warranty Information

The warranty information and server service tags are identified in the images below. All three hosts are covered by active warranties until March 16th, 2023.

VM-Host-1 (S/N J10000)



StoreWize v3700 SAN

The SAN is currently not covered by a warranty. It is highly recommended to have a warranty purchased for the SAN, as failure of SAN components can lead to extensive downtime for the entire environment.