**TECHNICAL BRIEF** 



# **KOLLECTIVE FOR SCCM**

**Technical Overview** 

# SUMMARY AND BENEFITS

The Kollective Enterprise Content Delivery Network (ECDN) enables enterprises to distribute large content such as video and software packages to every employee device without impacting the network, and without additional investment in physical infrastructure or servers. The Kollective ECDN has a low level integration with SCCM, such that the Kollective ECDN can be used as an alternative to the traditional server based mechanism for package and update distribution.

Through its cloud-based architecture, network efficiencies, ability to self-optimise, and work completely in the background to other network traffic, the Kollective solution provides the following additional benefits to the organisation and desktop management teams:

- Faster updates to desktop, ability to get out emergency updates quickly = increased protection
- Massively reduced operational overhead. Ease of achieving full automation with Windows as a Service updates.
- No additional hardware or serves required, reduction in distribution points by up to 99%
- Reduction in SCCM Total Cost of Ownership
- Analytics and measurability of delivery



Figure 1: The Traditional Model



CONTENT DELIVERED CONTENT DELIVERED ARCHITECTURE ARCHITECTURE DEER-TO-PEER ARCHITECTURE NO HARDWARE REQUIRED NO HARDWARE REQUIRED

Figure 2: The Kollective Model

**Figure 1:** With this model, each endpoint will download the package from the nearest distribution point server. With the size and frequency brought by Windows 10 WaaS, this needs to be done at each location to avoid excessive load on the WAN links. And so the traditional approach is not only expensive, both short term and long term, but imposes a significant maintenance and operational overhead on the enterprise.

**Figure 2:** With the Kollective approach, there are no distribution point servers required. The Kollective agent collectively creates a single virtual distribution point spanning all nodes such that content such as updates are sent only ever once over a WAN link, but equally important, making the solution highly resilient with very low operational overhead.

The Kollective ECDN solution brings several benefits to the Enterprise's configuration management processes:

- No additional hardware required, reduction in distribution points by up to 99%
- Reduced operational and maintenance cost of SCCM. Easier to achieve full automation.
- Reduction in SCCM Total Cost of
  Ownership
- Faster updates to desktop, ability to get out emergency updates quickly
   = increased protection
- Analytics and measurability of delivery
- Brings cloud based benefits to a traditionally on-prem system

This document provides a technical overview of the Kollective for SCCM solution, and aimed at providing an initial overview of the solution to architects and engineers around the solution. Further technical details are provided by ECDN specific datasheets and user manuals.

# THE KOLLECTIVE SCCM USE CASE

# Supporting the continuous Windows 10 WaaS lifecycle

Once workstations have been upgraded to Windows 10, there is a requirement to support an ongoing lifecycle of updates, as per Windows as a Service (WaaS) requirements. There is no longer the option for administrators to selectively choose which patches to deploy. Every month, a "quality update", around 1GB in size, needs to be deployed to each workstation. Biannually, spring and fall, a feature update of around 4GB needs to be deployed to each workstation.

To achieve this massive feat (an example company with 100,000 endpoints will need to distribute 1.2 petabytes of additional content across their network each year), organisations need to take into consideration the infrastructure required to support it. In most current environments, this infrastructure is largely inadequate. Organisations also need to consider the operational requirements and should be to striving for full automation of the process.

The Kollective solution seamlessly supports the demands of WaaS, by delivering the updates to the endpoints, without any additional physical infrastructure, without any impact on the corporate network and with minimal operational overhead. As the Kollective solution acts as a single "virtual distribution point", and self-orchestrates to ensure containment and efficiency, an automated ringed approach can easily be achieved without special considerations for location, network capacity or server capacity.

#### **Package and Application Deployment**

The Kollective solution supports content delivery of all application and package deployments. This is done on an on-demand basis, without need to pre-seed content in advance, and is beneficial to specialist rarely used applications installed through the catalogue, to the standard build applications that need to be installed and regularly updated to all workstations. Applications such as O365 suite, themselves have monthly quality and biannual feature updates, and so too need to be deployed in an automated continuous manner.

#### **Desktop Security**

For desktops, and ultimately the organisations within which they run, to remain secure, it is essential to remain up-to-date with the latest patches and updates. The Wannacry attack of 2017 exploited a known vulnerability, and compromised organisations that were behind in the updates, most famously Equifax, who were 49 days behind in updates<sup>¬</sup>Can we cite a reference?

Security patches, from Microsoft or other applications, typically require fast distribution in response to an identified vulnerability. Often, patches are required for zero-day attacks, meaning the identified vulnerability has been weaponized and incorporated into malware being targeted at end users. To thwart a potential or active zero-day attack, remediation patching must be delivered efficiently at highest velocity.

The Kollective ECDN provides the infrastructure to support continuous and immediate deployment of updates and security patches across the entire organisation.

#### HIGH LEVEL OVERVIEW

The following diagram illustrates the high-level architecture of the Kollective for SCCM Solution.

The Kollective SCCM is an addon component to the Kollective ECDN solution to provide the interfacing and delivery optimisation to SCCM.

Kollective uses the Alternate Content Provider (ACP) interface, supported natively by SCCM. The SCCM ACP is a set of API calls and modifies the function of Data Transfer Services, allowing an additional provider other than BITS to be invoked to retrieve ConfigMgr content.



Figure 3: High Level Architecture

**Figure 3:** The Kollective ECDN consists of two components, the backend Kollective Delivery Management System (DMS) located in the cloud, and an agent on each endpoint in the organization. The Kollective Agent provides edge delivery, intelligence and an interface to the Kollective ECDN. The DMS provides the central management and control of the ECDN, and together with the agent, provides the smart routing and caching of content.

#### This integration has three components:

- Kollective Publisher installed on a Primary Site server and is responsible for publishing content to the Kollective SD ECDN.
- Kollective Agent background service, installed on end user's machines and is responsible for acquiring content from the ECDN. If an existing Kollective customer, this may already be installed.
- Kollective Bridge installed on the end user's machine and functions as the SCCM Alternate Content Provider (ACP). The Kollective Bridge interacts with both the SCCM client and the Kollective Agent.

The publisher module is installed on all SCCM Site Servers from where updates and packages are to be deployed. The module enables ACP delivery through the Kollective ECDN. The administrator can select whether to publish all content through Kollective via the ACP (recommended), or to allow the administrator to enable ACP-mode delivery on a content-by-content basis. The publisher module automatically queues, and syndicates the content through Kollective Delivery Management System.

The Kollective Agent is a background service on the endpoint that provides the intelligent peer to peer delivery to the device. The Kollective SCCM Bridge provides the interface between the Kollective agent and the SCCM client. The Bridge supports the ACP interface, allowing the SCCM client to invoke Kollective for file delivery.

The request for the content through the ACP is made by the SCCM client, and adheres to scheduling and collection rules configured for the particular package/update. Once requested, the Kollective agent retrieves the files of the package, and cached by the Kollective agent. The files are copied by the Bridge to the SCCM cache store. At this point, the role of the Kollective solution is complete, apart from assisting other endpoints that request the same files in the future. The SCCM client initiates the install of the package or update.

The Kollective agent self manages its cache, removing old, unrequested cache if one of the configurable disk capacity thresholds are reached, or if the package is removed from SCCM.

### DATA FLOW

The following diagram illustrates the data flow of the Kollective solution:



- 1. Upon receiving software distribution policy, the SCCM client via Execmgr requests content.
- The Content Access Service (maintains the local package cache) submits the job to the Content Transfer Manager. The Content Transfer Manager (CTM) is responsible for scheduling Background Intelligent Transfer Service (BITS), Server Message Block (SMB) or Alternate Content Provider (ACP) to download or to access SMS packages.
- If the content has been enabled Alternate Content Provider (ACP) delivery and the ACP has been registered on the client, the Content Transfer Manager (CTM) invokes ACP to use Kollective for Software Distribution (SCCM).
- With the Bridge and Kollective installed, the ACP invokes the agent to receive download the files via the Kollective ECDN. If the ACP fails, the SCCM client will fallback to using the distribution point for BITS download.

- 5. Once received, a hard-link is created within the SCCM cache, so not to cache the same file twice using unnecesary disk space.
- Once the content is delivered to the local SCCM cache, control is passed to SCCM client. At this point, the role of the Kollective ECDN in the installation process is complete.
- 7. The Content Access Service (CAS) processes the content and checks ConfigMgr hash.
- Execmgr executes the command (installs the software) and returns the result.
- 9. All the processes and actions detailed above are imperceptible to end users by design.

#### **KOLLECTIVE ECDN**

#### **Distributed Cache**

In general, an agent requesting delivery will attempt to get different fragments of a content item in parallel from as many nodes in the network as it can find, subject to software-defined topology boundaries (connection limits and bandwidth caps) and then bond the bandwidths of the available nodes to speed up delivery.

Each node rotates through its prioritized sources, making multiple concurrent connections, discarding poor sources, and re-engaging source discovery as needed, all under the control of software-defined formation policies, such as LAN-focusing, topology boundary rules, throttling rules, and so on. Requesting nodes choose random blocks to download so they can cross-serve one-another to reduce load on origin servers and WAN links.

As soon as a fragment is received, it can be served. An agent does not need to download a full content item before it can serve that content to other nodes. And so there is not a storm of downloads of the same content item over the WAN if multiple nodes request at the same time.

As each block is received, the block is cached to persistent cache store. If the download is interrupted, say through a restart, the content item will resume.

The following diagram illustrates the distributed cache in action.



#### SCCM Benefits:

- In cases of monthly patch deployment, all nodes effectively want the same portions of the content at the same time. The Kollective distributed cache model allows that only a single content item, albeit load-balanced between multiple receiving endpoints, is downloaded over the WAN links.
- If a file download is interrupted, say through a restart or loss of connectivity, the agent will resume when connectivity restored.

#### **Optimal Source Selection**

Unlike traditional distribution models, the Kollective system is aware of the network topology and delivers only one copy of a digital media asset to each office, regardless of the number of users, endpoints and subnets at that location. Topology information is managed by a central service that maintains a virtual network map of all the available peers and arranges communications between peers that are close to each other.

This approach means that Kollective is not limited to sourcing content from peers that are only on the same subnet. Rather, the agent requests for files are provided with a prioritized list of peers that are at the same location and have all or parts of the content available.



#### **SCCM Benefits:**

- Automated out of the box. No need to manually configure boundary or AD groups to contain traffic and reduce WAN traffic.
- Topology agnostic and unlimited scalability
- Does not require use of broadcasts, which have limited scalability, are not supported across all networks and do not work across subnets.



**Traditional throttling** 



**Kollective Dynamic Throttling** 

### **Dynamic Throttling**

Patch deployments with SCCM are often throttled to reduce bandwidth and scheduled for off hours maintenance windows during, both factors, can impact patching SLAs and allow breaches to propagate. Furthermore, throttling does not prevent congestion caused by SCCM traffic. During peak periods the SCCM traffic, despite being throttled will still compete with regular user traffic and cause congestion. The above diagram shows that the throttled SCCM traffic is wasteful to unused bandwidth during nonpeak traffic periods but may still cause congestion during peak traffic. The download of the files takes considerably longer than it needs to.

Kollective's core delivery protocol (KDP) is designed to limit packet loss on its connections. It uses available WAN bandwidth and dynamically throttles itself down when it detects congestion. This behaviour enables KDP to tap unused bandwidth while yielding to other traffic by using flow control mechanics that are deferential to TCP. By using dynamic rather than static bandwidth management, Kollective removes the need to manually pre-calculate a restrictive throttle based on the number of endpoints or based on peak usage for a given link.

The KDP measures and benchmarks the packet round-trip and dynamically throttles the download speed. It makes download traffic deferential to all other network traffic, effectively making the download soak up idle bandwidth. Kollective SD ECDN agents detect user activity and politely throttle CPU and bandwidth use, so as not to interfere with foreground tasks on the device.

For SCCM, this means faster downloads and ultimately faster deployment of applications and updates to all endpoints, whilst never being the cause of congestion in the presence of other traffic on the network.

#### Granular control and configurability

One of the ECDN objectives is to avoid the need for extensive configuration, such as is the case when creating boundary groups. With Kollective, the out of the box experience provides the automation and adaptability needed not to require excessive boundary groups. However, the agent's behaviour is centrally configurable through a policy used by the agent, mostly done globally, but with ability to tune on a per location basis. An example would be to configure users connected by VPN to receive only and not to serve other users.

# **KOLLECTIVE MULTI-LAYER SECURITY**



# MULTI-LAYER SECURITY

Content data is ingested into the Kollective SD ECDN using HTTPS upload. Upon ingest, the content data will be virusscanned and encrypted, and in all cases, has a set of datablock cryptographic digests created that will be used later during delivery to validate content as it arrives at a receiver.

In the use case for Kollective for Software Distribution (SCCM) there exists a two-level delivery validation using both Kollective block signatures and the native SCCM crypto hashes. Should either validation be compromised, the content is discarded, insuring no malicious content can be injected into the network or end points.

The Kollective SD ECDN is a fully-managed ECDN, meaning all content published is authenticated and secure.

A site server authorized to publish connects to the SD ECDN through the API and can then perform tasks, such as:

- Creating a logical content item that can be associated with one or more physical files.
- Adding descriptive metadata or portal-specific structure.
- Setting up access controls, Kollective has a sophisticated content security system that integrates with the enterprise's own identity services.

Content items are assigned a unique location independent identifier that can be embedded in the Kollective SD ECDN URLs.

In the use case for Kollective for Software Distribution (SCCM) there exists a two-level delivery validation using both Kollective block signatures and the native SCCM crypto hashes. Should either validation be compromised, the content is discarded, insuring no malicious content can be injected into the network or end points.

### SYSTEM REQUIREMENTS

#### Windows Server Versions:

- Windows Server 2016
- Windows Server 2012 R2

#### System Center Configuration Manager Versions:

- Configuration Manager Current Branch
- Configuration Manager 2012 R2

## **KEY BENEFITS**

- Accelerate software distribution while reducing global distribution points
- Minimize network bandwidth impact from Windows as a Service update cadence
- Enhance endpoint security by deploying patches
  immediately upon availability



# **INTERESTED IN A FREE DEMO?**

SETUP DEMO