DVC
DIGITAL VENTILATED CAGE

SYSTEM REQUIREMENTS

SUMMARY

DVC
DIGITAL VENTILATED CAGE

SYSTEM REQUIREMENTS

1. History - Changelog

Version	Date	Changes	Owner
22	22/02/2022	Changed layout Modified the the network configuration adding the application type communciation	IT, MKTG
23	26/10/2022	Modified browser requirements	SRV, MKTG
24	01/02/2023	Modified Server HW Specification and Server Communications table	IT, MKTG
25	20/04/2023	Added dvcrm and Electronic TopHolder rules	IT, SRV
26	08/09/2023	Added FW rules for DVC Master EVO Dunfell OS	IT, SRV
27	08/09/2023	Added FW rules for DVC Master EVO Dunfell OS	IT, SRV
28	20/03/2025	Added FW rules for DVC Server	IT, SRV
29	30/10/2025	Added details on FW rules for Cloud And requirements for DVC Server on premises Added requirements for hostname for DVC Master EVO	IT, SRV

2. Overview

The Digital Ventilated Cage (DVC®) is a unique and revolutionary home-cage monitoring system, designed for mice's standard Tecniplast IVC cage system, composed of a mix of electronic and software components that collect information directly from the home cage in the home rack.
The DVC® system has been designed for use in any animal Facility and lab, as its main component, the DVC® rack, can be easily washed and autoclaved without affecting current SOPs.

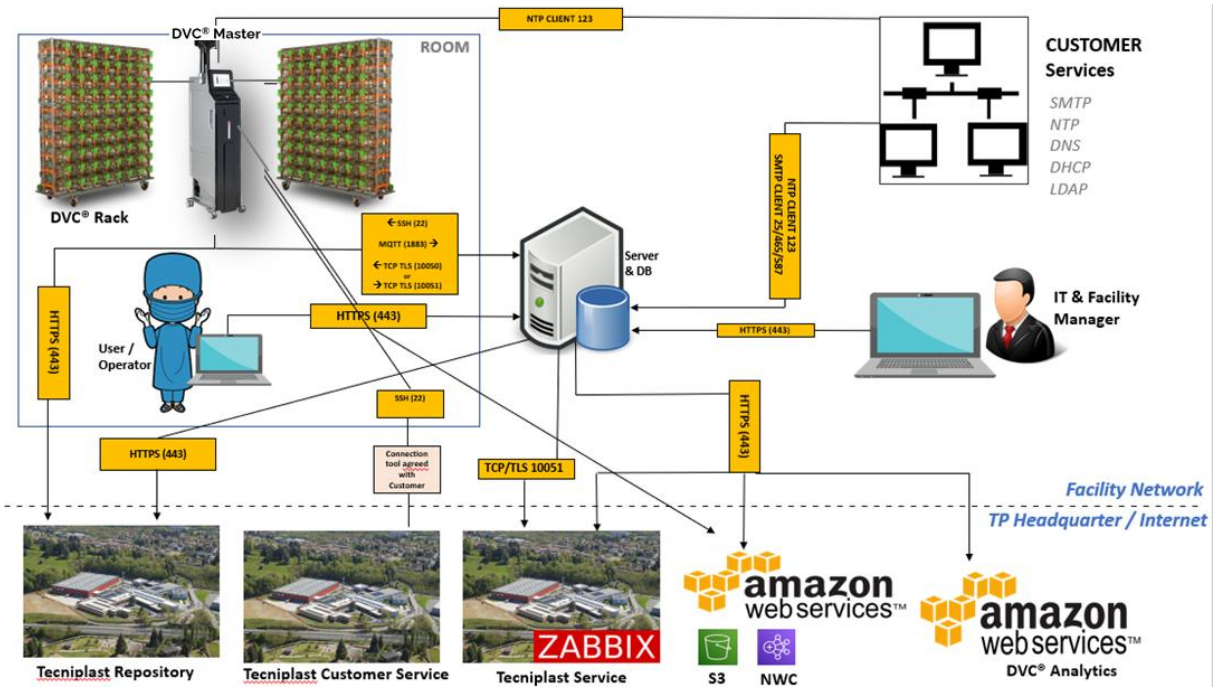
3. Deployment solutions

The DVC® System has two possible deployment solutions:

- On Premises, inside Customer Data Centre*
- In Cloud, into Tecniplast AWS infrastructure

*A deployment solution in the Customer cloud infrastructure will be considered as "On Premises" for the purpose of this document

3.1. On-Premises Deployment Solution - DVC® SYSTEM DIAGRAM



********CRITICAL********

The DVC® Server must be accessible remotely by the Tecniplast Service Team for the installation of the entire DVC® Server Applications. If this is not possible, specific and necessary travel quotations and accommodations must be invoiced.

3.2. On-Premises Deployment Solution - TECHNICAL SPECIFICATION

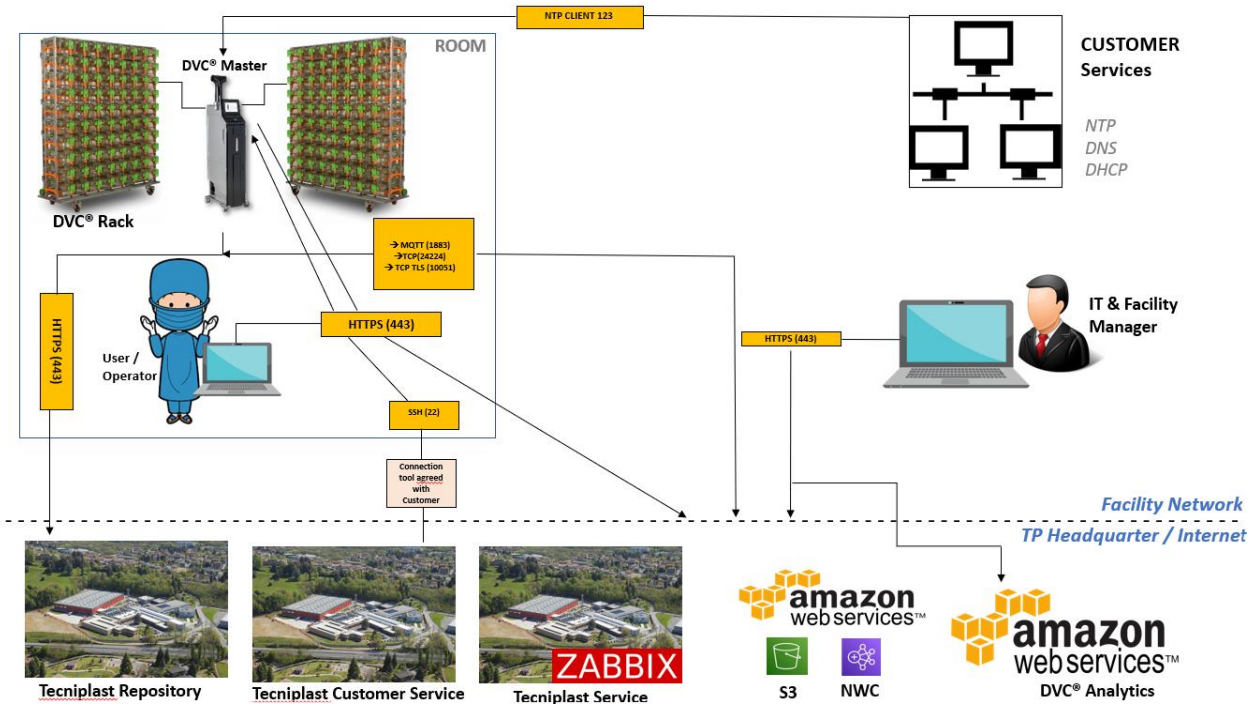
Requested hardware specifications:

	MINIMUM HARDWARE SPECIFICATIONS (less than 20 RACKS)	RECOMMENDED HARDWARE SPECIFICATIONS (more than 20 RACKS)*
N° CPU'S	8	16
RAM MEMORY	16 GB	32 GB
SWAP MEMORY*	16 GB	64 GB
HDDs (mountpoints)	1st partition 50GB (OS) 2nd partition /var/dvc/ 300GB (Data)	1st partition 50GB (OS) 2nd partition /var/dvc/ 1TB (Data)
NETWORK CARD	1 Ethernet card 1Gbps	1 Ethernet card 1 Gbps or higher
LINUX OS**	RedHat 8* Oracle Linux 8* Rocky Linux 8 RedHat 9* Oracle Linux 9* Rocky Linux 9	RedHat 8* Oracle Linux 8* Rocky Linux 8 RedHat 9* Oracle Linux 9* Rocky Linux 9

SWAP Memory*: The GB indicated is highly suggested to manage peak work situations under non-standard conditions.

****DVC System is compatible with RedHat, but the customer must provide RedHat subscriptions.**

3.3. CLOUD Deployment Solution - DVC® SYSTEM DIAGRAM



4. Server Maintenance

4.1. Server backup policy

Tecniplast performs a daily DB backup in the Server machine itself (virtual or physical). Optionally, but recommended, Tecniplast could automatically export DB backups into AWS S3 for a Disaster Recovery strategy.
The customer is responsible for backing up the entire machine.

4.2. Server Machine Updates

The customer is responsible for the security updates and patches for the Server machine. However, because the DVC® is a real-time system, it is highly recommended to alert the Tecniplast Service Team before proceeding with updates to ensure the machine's off-period is handled carefully.

5. Server Requests

5.1. Server Specifications for On-Premises solution

- SMTP credentials must be provided: SMTP server, port, authentication(if needed), SMTP sender.
- SELinux must be disabled.
- In case the 'dvc' user is provided on the login, it must have 601 ID
- 'Root' / sudo access must be provided

6. DVC® Network Communication

The DVC® system is a real-time system providing different software interface functionalities to the users and generating alarms related to the cage/animal safety; therefore, **any communication hereinbelow described has to be maintained open and stable** (**for instance, if there is a proxy in between some components or outbound to internet, be sure that the communications are allowed, and the components' IPs are placed in the whitelist**).

Moreover, **some network communications are mandatory to have the DVC® system fully operative**, while others are optional and related to the customer's preferred choices. Below in red are reported the optional network requirements. More specifically:

AMAZON WEB SERVICE – S3: is highly suggested but not mandatory. The same DVC® raw data can also be stored locally if the customer provides Tecniplast with a specific repository.

AMAZON WEB SERVICE – NWC: is probably the main feature of the DVC® system for improving animal welfare management.

AMAZON WEB SERVICE – DVC® Analytics: Not mandatory if the customer does not want to purchase this extra platform for researchers.

6.1. DVC® Server Communication (On-Premises Deployment Solution)

Source	Direction	Destination	Protocol	Port	Description
DVC® SERVER	Inbound	DVC® USER DEVICE / END-USER POINT	HTTPS	443	Web UI access
	Inbound	DVC® equipment (Master/REM)	MQTT	1883 / 8883	DVC communication
	Inbound	DVC® Master	TCP TLS	10051	ZABBIX
	Outbound	DVC® Master	TCP TLS	10050	ZABBIX
	Outbound	Customer NTP server	NTP	123	Time Sync
	Outbound	Customer DNS server	DNS	53	DNS
	Outbound	Customer SMTP server	SMTP	25/465 /587	Mail Service
	Outbound	zabbix.dvc.tecniplast.it	TCP TLS	10051	ZABBIX - TECNIPLAST SERVICE platform
	Outbound	DVC® Master	TCP TLS	5000	System Check service
	Outbound	DVC® Master	SSH	22	Maintenance
	Outbound	Operating System repository	HTTP / HTTPS	80 / 443	Repos for SW update
	Outbound	nexus.tecniplast.it	HTTPS	443	Repos for SW update
	Outbound	digitalcage-tecniplast.com	HTTPS	443	Release Note Website
	Outbound	amazonaws.com	HTTPS	443	S3, NWC
	Outbound	amazonaws.com	HTTPS	443	DVC® Analytics
	Outbound	kms.eu-west-1.amazonaws.com	HTTPS	443	DVC® SW installation
	Outbound	rm.dvc.tecniplast.it	HTTPS	443	DVC® SW installation
	Outbound	customer-dashboard.dvc.tecniplast.it	HTTPS	443	Customer Dashboard
	Outbound	prod-tp-idp-cd.auth.eu-west-1.amazoncognito.com	HTTPS	443	Customer Dashboard

6.2. DVC® MASTER communications (for both Deployment Solutions)

Cloud Solution Notes for Destinations:

DVC Server (HTTPS) = [**customername***].**dvc.tecniplast.it**
DVC Server (MQTT/TCP/TLS) = [**customername***]**-tcp.dvc.tecniplast.it**
***customername**= Provided by Tecniplast

Source	Direction	Destination	Protocol	Port	Description
DVC® MASTER	Outbound	DVC® SERVER	MQTT	1883 / 8883	DVC® Communication
	Outbound	DVC® SERVER	HTTPS	443	DVC® equipment (Electronic TopHolderEVO)
	Outbound	DVC® SERVER	TCP TLS	10051	Zabbix
	Outbound	vivatronics.tecniplast.it	HTTPS	443	Tecniplast Repos
	Outbound	vt-raw-data.s3.eu-west-1.amazonaws.com	HTTPS	443	S3 raw data
	Outbound	Customer NTP server	NTP	123	Time Sync
	Outbound	Customer DNS server	DNS	53	DNS
	Outbound	DVC® SERVER	TCP	24224	Fluentbit
	Outbound	rm.dvc.tecniplast.it	HTTPS	443	DVC® SW installation
	Outbound	kms.eu-west-1.amazonaws.com	HTTPS	443	DVC® SW installation
	Outbound	nexus.tecniplast.it	HTTPS	443	Repos for SW update

6.3. Communication specific to On-Premises Deployment Solution

Source	Direction	Destination	Protocol	Port	Description
DVC® MASTER	Inbound	DVC® SERVER	TCP TLS	10050	Zabbix
	Inbound	DVC® SERVER	SSH	22	Maintenance

Notes:

- Master Hostname must remain untouched and remain with the Serial number set already on it by default

7. End-User requirements

- Allowing outbound access to the DVC® Server on port 443 (HTTPS)
- Operating System:
  - Windows 7 or Above
  - Linux

- Browser requirements:
  - Google Chrome (Official build) – Latest version is highly suggested

- Desktop/Laptop screen resolution: 1366 x 768 or higher

8. Security and Compliance

Tecniplast ensures that the DVC® System is designed, deployed and maintained according to internationally recognized security standards and best practices. This section summarizes the main security and compliance principles applicable to both On Premises and Cloud Deployment solutions.

8.1. Information Security Management

Tecniplast S.p.A. operates under an ISO/IEC 27001-certified Information Security Management System. This certification covers the processes, infrastructures and teams involved in the development, maintenance, installation and support of the DVC® System and related digital services.
Official certification is available on request.

AWS, the cloud provider used for the DVC® cloud deployment, maintains the following certifications, among others:

- ISO/IEC 27001

- ISO/IEC 27017 (Cloud Security)

- ISO/IEC 27018 (Cloud Privacy)

- SOC 1, SOC 2, SOC 3

- GDPR-compliant data processing framework

8.2. Data Sensitivity and Classification

The DVC® System does not collect or process any personal data, identifiable researcher information, animal IDs, animal names, experiment metadata, or project-sensitive content.

The system only processes:

- DVC® raw data (sensor data)
- Cage ID
- Number of animals
- Animal sex

These data are fully de-identified and cannot be traced back to researchers, projects, or specific studies. According to most customer classification frameworks, DVC® data fall under the lowest sensitivity category (e.g., Non-sensitive / Internal or Confidential – Technical depending on customer policies).

8.3. Encryption and Data Protection

All communications between DVC® components and cloud services are encrypted using industry-standard protocols.

- Encryption in transit:
    - TLS 1.2 or higher for HTTPS, MQTT over TLS, Zabbix TLS
- Encryption at rest (Cloud Deployment):
    - All raw data stored in AWS S3 are encrypted using AES-256 with AWS KMS-managed keys
- On Premises Deployment:
    - Encryption at rest depends on customer-provided storage policies
    - DVC® System supports encrypted filesystems (LUKS) if configured by the customer

No unencrypted communication is used for external traffic.

9. TERMINOLOGY AND USAGE

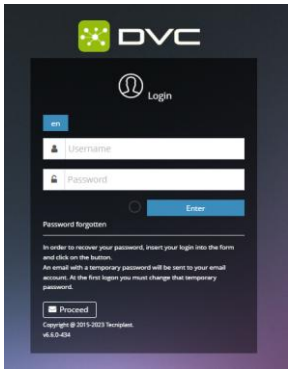
9.1.DVC® Server

The end-user must provide a physical or virtual machine with all the applications required to run the system installed.
The user provides the Server machine by following the requirements described in the corresponding section.

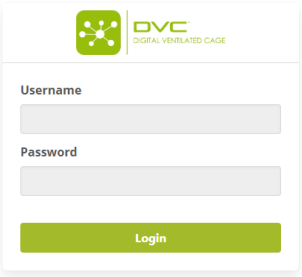
9.2. DVC® Software interfaces

Two different DVC® web applications are running on the DVC® Server.

- **DVC® workplace**: This is an administrative interface used to create user accounts, build structure, set thresholds for alarms, etc.



- **DVC® Operator**: This is the operative interface designed to support the animal caretakers while managing cages and animals directly in the animal rooms.



9.3. DVC® Master

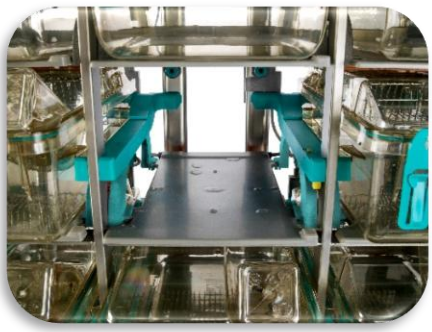
This is a physical machine usually placed over the Tecniplast Air Handling Unit. Recently, this machine has been embedded directly into the new AHU, the ZEPHYR.
It powers the DVC® Rack with its DVC® boards and exchanges data & information with them. It can manage up to 6 different DVC® racks in the Animal Rooms with the new Zephyr Version (the previous Master device only up to 4).
The DVC® Master must be hardwired to the DVC® Server, and therefore must be on the user's intranet (one straight Ethernet cable for each DVC® Master).

9.4. DVC® Reader/DVC® Electronic Top Holder

The animal caretakers use these DVC® components to interact with the Cages while they are open over the working bench in the animal rooms.
The DVC® Readers are connected wirelessly to the DVC® Master (for DVCISO customers), while the DVC® Electronic Top Holder can also be linked to the customer's wireless network, if available (WPA2 Enterprise protocol supported)

9.5. DVC® Rack

The Tecniplast ventilated rack is equipped with DVC® boards firmly attached at the Rack level. For each cage slot of the rack, there is one dedicated DVC® board.



9.6. User Device / End-User Point

To access the DVC® web applications, the user needs a device with a web browser. The browser requirements are listed in the section below.
The user's device needs to reach the DVC® Server.
It is essential to underline that the available DVC® applications are intended for desktop use (DVC® workplace) and, even more importantly, for animal room use (DVC® Operator), where a dedicated laptop for each animal caretaker, located close to the working area, is highly recommended.
For the best user interface experience, a **1366 x 768** (or higher) screen resolution is suggested.

9.7. Tecniplast Repository

This is the official Tecniplast repository for the latest software releases of all DVC® software components (DVC® Server, DVC® Master, DVC® Reader/Electronic Top Holder).
Tecniplast automated the DVC® Server upgrade by manually launching specific jobs directly in the DVC® Server located in the field, which connects to the Tecniplast repository using specific secure credentials access.

Tecniplast Repository

9.8. Tecniplast Customer Service

The tecniplast Service team might have different reasons for remotely entering the DVC® Server and DVC® Master elements. The most common reasons are installation and updates, troubleshooting and manual bug fixes if needed, and, lastly, customer care support during remote training.

The customer can provide multiple methods for the Tecniplast Service team to connect to the local DVC® system remotely. The preferred option is to allow this through a secure customer VPN connection that can be left open or opened on request. This is a customer's choice based on the desired speed of reaction.

Tecniplast Customer Service

9.9. Tecniplast Service Monitoring Platform (ZABBIX)

Tecniplast uses the Zabbix platform (https://www.zabbix.com) for DVC® application monitoring. DVC® metrics are the ones related to the performance of the system, like the status of the DVC® Server and DVC® Master RAM status, the CPUs status and so on, but also metrics related to the DVC® board functionalities, the fact that the 24/7 generated DVC® raw data are still falling in the linear working range and so on.

For the sake of clarity, no sensitive data (for instance, the name of the cage or its content or any experiment fields) is collected or monitored.

Tecniplast Service

9.10. Amazon Web Service – S3 and NWC

There are two reasons for pushing DVC® raw data to the Tecniplast cloud (Amazon Web Service - AWS). The first is to store DVC® raw data outside the Facility, directly in a dedicated AWS S3 bucket, for recovery purposes (e.g., to recover DVC® server data and support the running of the playback task for the DVC® Analytics platform). The second reason is that a specific DVC® Algorithm called Night Welfare Check (NWC) runs continuously in the cloud (to support faster updates and easier maintenance). It analyses DVC® data (DVC® raw data plus Cage ID and the number of animals) to provide daily output to

animal caretakers on the specific cage animal activity status (normal or hyper/hypoactivity detected), so they can be supported during their animal welfare check activities.

9.11. Amazon Web Service – DVC® Analytics

DVC® Analytics is the dedicated scientific cloud-based platform developed by Tecniplast for researchers to access and analyse DVC® data to improve and complement experiments with novel findings.

It runs entirely on the Tecniplast AWS cloud and is therefore accessible from anywhere with a valid internet connection.

For clarity, this platform is optional for the customer. For more information, please refer to the dedicated documentation and visit https://digitalcage-tecniplast.com/en/products/dvcr-analytics.html