



Solution Brief  
.....

2012

# Secure Monitoring in and from the Cloud

---

## Preface

The ICT landscape is evolving rapidly and Cloud-based offerings are here to stay. Organisations will increasingly use Cloud-based services to either host their applications or use Cloud facilities to fulfil tasks previously performed in house. Monitoring is one of these tasks.

Monitoring ICT systems in and from the Cloud imposes some stringent requirements in order to deal with the inherent challenges in terms of scalability, security and multi-tenant support.

SecurIT D-Man is a light-weight, secure and open-standards based monitoring system that is focussed on highly-distributed environments. It has been designed from the bottom up to integrate smoothly in customer environments that span across internet boundaries.

This White Paper describes why SecurIT D-Man is probably the best product on the market to address the specific needs of Cloud monitoring. While it is not absolutely required to be familiar with SecurIT D-Man to fully grasp the value of the product in this context, it might help to first read the generic SecurIT D-Man White Papers. The following paragraph intends to set the scene.

## About SecurIT D-Man Distributed Monitoring

Traditional monitoring systems don't fit very well with the new Cloud-based paradigm. Because they were initially designed to monitor internal processes and applications mainly from a technical point of view, they don't pay too much attention to infrastructural security and the user's perspective.

The first aspect is reflected by the heavy frameworks on which many of these systems rely. These frameworks tend to use protocols that are not supported within a Demilitarized Zone (DMZ), through firewalls or across the de facto unsafe internet.

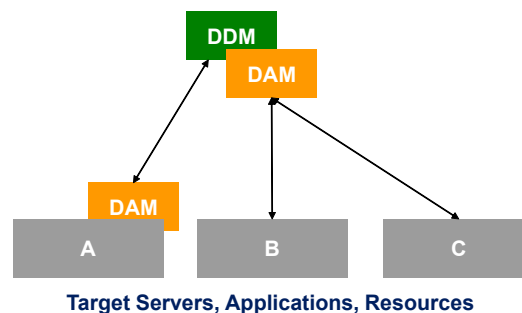
The latter aspect might result in ICT environments of which the isolated tiers are in perfect health, but where the service as a whole does not behave as expected.

SecurIT has designed and built a monitoring solution for Distributed Environments, from the ground up, with exactly these aspects in mind. It addresses both, helping IT-Administrators isolating and solving IT problems appropriately as well as end-to-end Monitoring of business applications to identify service outage before it effects end-users.

This solution was released by SecurIT under the name SecurIT D-Man in 2004. The D-Man monitoring framework consists of three main components:

- D-Man Application Manager (DAM)
- D-Man Data Manager (DDM)
- D-Man Cloud Manager (DCM)

The **D-Man Application Manager (DAM)** represents a traditional monitoring agent. It is used to gather information from any component in the infrastructure that needs to be monitored. A DAM can run on the target system or perform its monitoring functions remotely. This depends on the monitoring tasks to be provided. A DAM is responsible for monitoring any activity that is relevant to the server on which it resides. This could be local as well as remote activity.



The **D-Man Data Manager (DDM)** sits at the core of the local D-Man monitoring framework. It is responsible for collecting and analyzing the data that is gathered by all DAMs in the infrastructure and expose the results or forward them to a higher level. It is also used for the administration of the D-Man environment, either locally or on distance, e.g. from the Cloud.

The **D-Man Cloud Manager (DCM)** provides a centralized way of monitoring multiple local D-Man environments. These could be entities within a large corporation or Cloud, but can also be used to monitor multiple customer environments from the Cloud.

Please refer to the “SecurIT D-Man. Distributed monitoring for e-Business environments” Product Description for additional information on the Core D-Man Infrastructure.

## SecurIT D-Man for Cloud Monitoring

A monitoring solution must provide a number of important features in order to fulfill the specific requirements in a cloud-based environment. In this chapter we explain how D-Man uniquely addresses these needs.

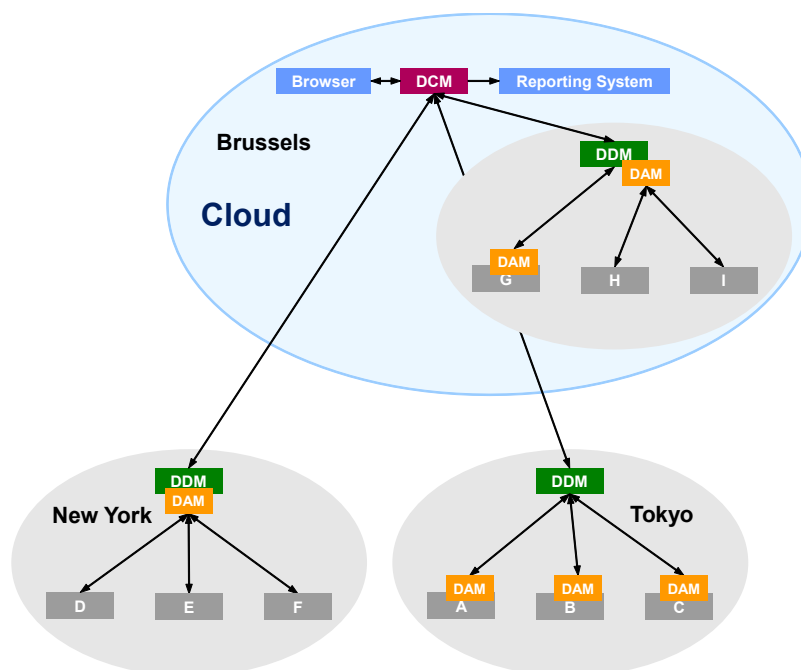
### ✓ Scalability

In federated environments like the Cloud, it is recommended to split the environment in more manageable domains. This can be handled by creating a hierarchy of DDMs and DCMs. This model, and its advantages, is described in more detail further on in this document.

In isolated or small environments, it is usually sufficient to have a single DDM to control the SecurIT D-Man system. In case there would be a requirement for high-availability of the monitoring solution as well, a second DDM could be configured for redundancy.

#### How it works

The model for deploying SecurIT D-Man in large distributed environments is best illustrated by an example. Consider a Cloud monitoring environment in Brussels with a local in-cloud customer domain and two remotely managed customer environments in New York and Tokyo.



Each location (Brussels, New York and Tokyo) hosts its own SecurIT D-Man distributed system, controlled by a local DDM software appliance with a DAM for remote monitoring (New York example), remote DAMs on the target platforms (Tokyo example) or a combination of both (Brussels example). This system operates in stand-alone mode and fully monitors the local e-Business environment. The system contains its own administration and configuration module which can be controlled from a browser in the Cloud.

At each location there is also a link to a central SecurIT D-Man DCM system that is located at the Brussels Cloud provider. This latter system operates at a Meta level. It uses exactly the same technology and components as the other systems. In other words, only its configuration is different.

The SecurIT D-Man DCM is able to extract on a regular basis event information from the SecurIT D-Man DDMs at the served locations. The mechanism used to extract this information is exactly the same as the one used to extract event information from the DAMs. The connection is established from the DCM, it runs over HTTPS and uses mutual authentication to validate the identity of the peers. Because each DDM has a local event database, occasional failures of the connections (which might run over the public internet) will not harm the system.

The DCM provides its own administration and configuration module and can be controlled from a local browser. Furthermore it is able to consolidate and correlate the events it gets from the remote systems and send them to a local reporting system. This can be achieved using SNMP or any other published interface.

In very large environments, it is possible to make the SecurIT D-Man hierarchy even deeper. In such a configuration there can be several Meta levels. Another reason for creating more levels could also be to perform more interim correlations or to spread the correlation load over different systems. DCMs can also be used for redundancy reasons and as backup systems.

## ✓ Multi-domain support

Much of the complexity associated with Cloud Monitoring is related to the fact that multiple customer domains must be monitored from the same system, whether in the Cloud or from the Cloud, with a sufficient level of segregation.

SecurIT D-Man supports both Multi-tenant and Multi-channel environments to accomplish this objective.

Multi-tenant environments are environments in which applications and services belonging to distinct parties are monitored from the same system. This situation typically occurs in cloud-based systems where different customers share the same hosting or monitoring platforms. This is also the case within a large corporation, where the responsibility for managing Test, Acceptance and Production environments may be allocated to different groups or people.

Multi-channel environments are environments where different parties are involved in dealing with the monitoring system (e.g. helpdesk, administrators, operators). This is also the case in cloud-based systems, where a clear segregation must be accomplished between people to maintain different customer environments.

Both Multi-tenant and Multi-channel environments require that the monitoring system can make a clear distinction between users and systems belonging to different parties and to make sure users can only access and manage the systems and data they are entitled to.

### SecurIT D-Man Approach

D-Man approaches this challenge by means of an attribute-based access control mechanism.

On one side all D-Man objects (e.g. agents, monitors, views, targets) are assigned attributes. On the other side users of D-Man (e.g. helpdesk, administrators, operators) are organized in profiles (similar to roles in an IdM system). These profiles group together a set of privileges whereby a privilege basically matches an attribute.

Some examples:

A “Web Server monitor” could have the following attributes:

- Customer A
- Production

This means that this monitor runs in the “Production” environment of “Customer A”.

An “LDAP monitor” could have the following attributes:

- Customer B
- Acceptance

This means that this monitor runs in the “Acceptance” environment of “Customer B”.

A user could have two profile:

- Profile 1
  - o Customer A
  - o Production
  - o Action: View events
- Profile 2
  - o Customer B
  - o Acceptance
  - o Action: Manage parameters

Looking at “Profile 1”, we can see that the user has privileges to work in the “Production” environment of “Customer A” as these privileges correspond to the attributes that are required to access the “Web Server monitor”. The user however is only allowed to “view events” generated by that monitor, as that is the only action associated with the matching profile.

Applying the same mechanism, we can also see that same user has “Manage parameters” rights for the “LDAP monitor” running in the “Acceptance” environment of “Customer B”. This would allow the user e.g. to change the IP address on which the LDAP server is listening.

Attributes and Privileges are not pre-defined by D-Man. Any D-Man administrator can choose as many values for this as required by the monitored environment. The actions however are pre-defined by D-Man as they relate to the actions users can take within D-Man. Some examples:

- Define/Remove Monitor
- Change Monitor
- Configure Monitor
- Enable/Disable Monitor
- Show event
- Acknowledge/Close event
- And many more....

### Conclusion

The attributed-based access control mechanism of D-Man allows implementing an efficient and secure distinction between systems, data and monitors in cloud based environments. Instead of having to define detailed rules for keeping this information apart, only attributes, privileges and actions have to be assigned and the D-Man authorization system will do the rest.

## ✓ Security

Obviously security is a very important aspect in cloud-based monitoring. It is common practise to apply layered security within e-Business environments by dividing the infrastructure into different Security Zones. Often, outer zones are said to provide more security than inner zones. This is however a misconception. Each of the zones provides a different level of security, protecting against the risks that this zone is vulnerable for. The idea of outer zones is to reduce the number of risks that may apply to inner zones. End-to-end security can only be guaranteed if each of these zones take full responsibility over security for its part of the e-Business infrastructure.

### Internal Security

By internal security we mean the way the system is able to protect any unauthorized access to its data or processes, while being able to transfer data between security zones with respect of common security guidelines.

Because SecurIT D-Man was designed to be deployed within sensitive e-Business environments, where security is a key concern, it is obvious that it is based on a secure core as well.

By default the communication between the D-Man components (DCM - DDM – DAM) runs over HTTPS using mutual authentication. In addition, a dynamic token is exchanged between the DDM and DAM for enhanced security. The communication between the DDM and the DAMs is always initiated by the DDM. Because the DAM may be located in a DMZ it is not recommended to open channels towards the secure Intranet. Furthermore the DDM will only fetch information from DAMs which it has configured and the DAM will only accept requests from the DDM that has configured it.

When a DAM is required on a target system, its monitors are never installed on the local disk and no local configuration is required. Configuring a DAM with its agents and monitors is always handled from the DDM.

### External Security

External security is about how the system can be managed in a secure way by administrators with the right entitlements, across different security zones.

The browser based access to administration and configuration functions runs over HTTPS and is protected by a sophisticated access control mechanism. This is illustrated by the example in the previous chapter Multi-domain Support. In this way SecurIT D-Man provides granular control on what a user is entitled to perform, like what part(s) of the total environment are accessible and what that user is able to do. Certain users can only view the results of the monitoring actions, others may be allowed to configure the components, in a granular way.

Example: segregation of duty between:

- monitor development
- monitor configuration
- monitor deployment

In a Cloud-based monitoring service set-up, all actions on the target environment can be handled from a central point in a secure way. The monitoring results are propagated by the local DDMs to the central DCM for administration purposes. If so desired, local access can be provided to certain parts with the same level of security. Configuring a remote DDM and its associated DAMs can be handled over the internet in a secure way.

## ✓ Deployment

This is a critical success factor in a cloud-based monitoring offering. Ease of deployment and swift activation of the service will contribute significantly to the success.

SecurIT D-Man has been designed to accomplish these goals from the ground up:

### Installation

The components to be installed in a target environment are the local DDM and its associated DAM(s). A DDM is delivered as a Software Appliance which can easily be installed on server or a virtual machine, without prerequisite knowledge of D-Man.

A DAM can simply be part of the same system or installed on a target system, depending on what needs to be monitored and whether that requires local access to resources or interfaces. Anyhow, installing a DAM is also very simple, since no local configuration is required.

### Configuration

All configuration actions can be performed from the Cloud in a secure and controlled way. Only users with the appropriate privileges can perform such actions through the browser interface of the DDM or DCM. Some examples of such configuration actions:

- Select the agents or monitors to run on a DAM for local or remote monitoring
- Determine the dependencies between systems via a point-and-click interface
- Distribute the agents and monitors to the DAM and activate the monitoring

In essence, there is virtually no local intervention required to get and keep the monitoring of a customer environment up and running.

## Summary

This White Paper clearly shows that through its unique and secure foundation SecurIT D-Man is a powerful monitoring solution that can easily be deployed in the Cloud for a large, distributed environment, where there is a need to have a centralised view on the status and health of the overall system and its individual parts.

## Key Features

### Multi-platform

Highly distributed environments normally consist of a heterogeneous set of platforms. SecurIT D-Man, being entirely based on Java, is available on all platforms that support a basic JVM. Among the supported platforms are AIX, HP-UX, Linux, Solaris and Windows.

### Multi-tenant and Multi-channel

SecurIT D-Man's Multi-tenant and Multi-channel features safeguard that the monitoring system can make a clear distinction between users and systems belonging to different parties and to make sure users can only access and manage the systems and data they are entitled to.

### Straightforward installation

While offered as a software appliance, SecurIT D-Man is also available as a basic compressed file that can easily be distributed and expanded to any remote target system. This allows it to be integrated within any software distribution solution.

### One-step deployment

Once deployed, D-Man is immediately operational. No interventions on the target systems are required and the system can be completely configured and controlled from a central location.

### Firewall-friendly

To be able to cross the numerous firewalls that might be in between the monitored system and the central reporting system, all internal SecurIT D-Man communication is entirely based on the HTTP and/or HTTPS protocols.

### Compliant to DMZ rules

E-Business systems contain components that reside within the DMZ zone. Because security rules dictate that connections from less secure zones to secure should be avoided as much as possible, SecurIT D-Man will never create such connections.

### Light-weight

SecurIT D-Man has no external dependencies. It requires no application server and relies completely on the embedded light-weight Jetty runtime. The SecurIT D-Man agents require less than 500K of disk space and hardly consume more than a few mega of memory.

### Secure foundation

The bigger the environment, the higher the risks are for security breaches. A system monitoring such an environment should as such not impose an extra thread. For this reason, SecurIT has translated its years of experience in securing e-Business environments into a highly secure SecurIT D-Man foundation based on SSL communication with mutually authenticated components.

### Embedded intrusion protection

To prevent malicious users from interfering with the monitoring system, the SecurIT D-Man agents never write any critical data (configuration data, events or monitor scripts) to disk. As such, the expected behaviour of the system can only be modified through the central administration console, which is protected by strong authentication.

### Redundancy

In distributed systems, the chances on unavailability increase by the size of the environment. SecurIT D-Man has been designed in such a way that the failure of any single component of the infrastructure will never cause the monitoring system to a stop or to lose any critical event data. At the monitored end-points, all SecurIT Agents are able to cache event data until it is collected

## D-Man Documentation

This paragraph provides an overview of other available D-Man White Papers and product documentation.

General purpose:

- SecurIT D-Man. Monitor Reference Guide
- SecurIT D-Man. Distributed monitoring for e-Business environments (Product Description)
- SecurIT D-Man, Distributed monitoring for Federated e-Business environments (Solution Brief)

Specific for IBM environments:

- SecurIT D-Man. Distributed monitoring for IBM Tivoli Access Manager (Solution Brief)
- SecurIT D-Man. Distributed monitoring for IBM WebSphere (Solution Brief)
- SecurIT D-Man. Distributed monitoring for IBM Tivoli Identity Manager (White Paper)  
(Not available at the moment)

\* \* \*

Copyright © 2012 SecurIT bvba. All Rights Reserved

No part of this document may be copied, translated, or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of SecurIT bvba. SecurIT has made every effort to ensure that the information in this document is accurate and complete; however, SecurIT assumes no responsibility for any errors or omissions. Information in this document is subject to change without notice.

Tivoli® is a registered trademark of Tivoli Systems Inc. in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer-Tivoli A/S.

IBM is a registered trademark of International Business Machines Corporation in the United States, other countries or both.

WebSphere is a registered trademark of International Business Machines Corporation in the United States or other countries or both.

Other product names mentioned in this paper may be trademarks or registered trademarks of their representative companies and are hereby acknowledged.