Bureau du vérificateur général

V.9. Active Directory Security

TABLE OF CONTENTS

V.9. ACTIVE DIRECTORY SECURITY

1. INTRODUCTION

Background

Information technology (IT) has become vital to ensuring efficient operational management in the Ville de Montréal (the city), as it has in the administrations of most major cities throughout North America and Europe. IT must provide elected officials, employees and the public with access to relevant information on a timely basis.

The vast majority of city employees need access to a secure computer system to carry out their day-to-day duties with a desktop computer, a laptop or a mobile workstation connected to the city's IT networks.

To effectively manage these networks and the access to the data they contain, the Service des technologies de l'information (STI) and the borough IT divisions have set up centralized Windows-compatible identity and authentication services within their computer and server networks. These centralized services are provided by Microsoft Active Directory (AD).

Role and Features of Active Directory

Every server and workstation in a Windows environment has functioned as a stand-alone unit since the Windows architecture was decentralized. Microsoft AD is the technology underlying the Windows operating system. It serves as a central repository, commonly referred to as a directory service, for centralized user and security management.

AD can manage objects no matter where they are and no matter what the network protocol used, thus making it possible to manage workstations and remote users in a fully centralized way. AD organizes the directory into sections to meet the needs of any organization—from those with only a few objects to manage to those that handle millions.

More specifically, AD uses Windows operating system to provide centralized identity and authentication services to the city's computer networks. As a directory service, AD indexes all elements of a network or networks, including user accounts, workstations, servers, printers and

so forth. All AD-related information and settings are stored in a centralized proprietary database that resides on the domain controllers. This information and settings form the AD structure, which is composed of a hierarchical organization of objects.

A domain controller is a server that stores a copy of the AD directory. It ensures changes made to the directory are propagated, users are authenticated and logged in and searches can be performed in the directory. A domain can have one or several domain controllers. Each domain controller can receive or replicate changes made in any of its counterparts. Domain controller security is vital. If the security of the domain controller is compromised, overall AD security is at risk.

Windows security depends on AD. *Windows security* includes the security of workstations, users, servers, data and networks that run on the Windows operating system. If AD security is compromised, all other related security measures are in danger of collapsing as well.

The effectiveness of AD security lies in the configuration settings defined during initial setup and the maintenance of these settings throughout AD's life cycle. These settings are stored in group policy objects (GPOs), which are applied when the computer starts up and when users log on. GPOs are used to maintain an adequate level of system and data security, but they also reduce potential risk due to users by restricting their activities (e.g., locking the control panel, restricting access to select folders, disabling certain executable files).

Developed to provide high performance and security, AD allows system administrators to control access to and use of shared data and resources through distribution, duplication, partitioning and access restriction functions.

2. AUDIT SCOPE

The purpose of our audit was to evaluate the controls means ensuring Active Directory security.

The objectives of this audit were:

- Evaluate the efficiency and effectiveness of the controls ensuring the secure setup and management of AD
- Provide an independent evaluation of AD security settings

The audit process resulted from our analysis of the dangers related to AD security and circumstances specific to the city. Our method and audit criteria were designed to adhere to best

industry practices. We developed the audit program after consulting several relevant publications.

We performed our audit tests in the presence of the STI's AD administrators and the AD administrators from the boroughs created from the former suburban municipalities. We interviewed these individuals and also used Microsoft AD administrative tools.

There are several ADs in place within the city. Following our risk analysis, we focused our audit on seven ADs. Given the sensitive nature of ADs, we prefer to keep this list confidential.

The AD security audit concentrated on the management and configuration controls for:

- AD management
- AD perimeter security
- Logical security of domain controllers
- Configuration settings for domains and domain controllers
- AD policies and procedures

The following elements were excluded from our audit:

- Configuration of non–domain controller servers
- Configuration of workstations
- User identity and access management
- Domain name system (DNS) management
- Physical server security
- Application security management
- Database access
- Password management.

3. FINDINGS, RECOMMENDATIONS AND ACTION PLANS

In this section, we will list the main observations made about all the ADs. However, given the criticality of the ADs where we identified weaknesses, we have chosen to keep the audit details and results specific to each AD confidential. Confidential audit reports were remitted to the authorities responsible for each AD. They subsequently reviewed the findings and the proposed recommendations specific to them.

3.1. MULTIPLE ACTIVE DIRECTORIES

3.1.A. Background and Findings

FINDING

Our audit revealed that there are several ADs being used within the city.

The former suburban municipalities that became boroughs following the municipal mergers on January 1, 2002 are still running their own copies of Active Directory, the same ones that were installed long before the mergers occurred.

This situation was justified at the time of the mergers, as these boroughs were using their own management and operational applications and the STI did not support these applications.

However, the context has since changed. The STI now provides integrated solutions that are used by all boroughs (e.g., SIMON, Ludik), which means the boroughs' "orphan" applications will become obsolete in the very near future.

By maintaining several ADs among its business units, the city is exposing itself to the following dangers and potential impacts:

- Problems in maintaining a consistent level of security for all ADs. Security for ADs that the STI does not oversee may not comply with the city's security and operational requirements. In the event of a security breach, the boroughs' Windows environments could be compromised, and this risk could also extend to the city's Windows environment, given the relationship of trust between the city's AD and some borough ADs.
- Development and implementation of more complex contingency plans, and the corresponding higher costs, because of the need to produce operational continuity plans for each AD instead of developing one that is city wide. This could prevent boroughs from resuming operations promptly in the wake of a disaster.
- Increase in infrastructure costs, including additional software licence costs, because of the greater number of domain controllers (each AD must have at least two domain controllers to run properly).

3.1.B. Recommendations

We believe that a single, city-wide Active Directory should be set up. We recommend that the Direction générale:

- **Perform a cost-benefit analysis and an impact analysis on implementing a single Active Directory.**
- **Have IT business units play an active part in the analysis and the project.**
- **Provide a sufficiently powerful architecture with enough capacity; for example, some telecommunications links will have to be replaced to accommodate higher bandwidths.**
- **Develop a formal service level agreement (SLA) with clients so that Windows performance and user-services quality continue to meet administrative requirements and do not deteriorate.**

3.1.C. Action Plan of the Relevant Business Unit

The relevant business unit has validated our recommendations and will forward its action plan to us at a later date.

3.2. ACTIVE DIRECTORY RISK ANALYSIS

3.2.A. Background and Findings

A risk analysis identifies and assesses factors that may compromise the success of a project or the ability to fulfill business objectives. More specifically, it determines the risks that pose a threat because of their likelihood and impact.

A risk analysis also allows an organization to develop controls to reduce the probability and impact of possible danger to acceptable levels. This analysis is a basic tool for identifying the various risks facing the city.

An AD risk analysis carried out by the city and the boroughs would allow the administration to pinpoint factors that could compromise security of the confidentiality, integrity and availability of data that is processed by, transmitted through and stored on AD. A risk analysis is the first step in optimizing AD security and should be repeated periodically by the STI. Best practices suggest that this analysis be done internally and documented. It is the basis for determining which security measures (configuration settings, etc.) are appropriate. The findings of the risk analysis will influence how security settings are configured.

FINDING

Although some business units conduct some general IT risk analyses, they do not take into consideration specific AD-related risks.

Without an exhaustive analysis of the AD-related risks for the city or its boroughs, it is difficult for the business units to implement all the controls needed to reduce AD-related risks to an acceptable level. If some risks are not taken into consideration, they may cause vulnerabilities that could be exploited by attackers to undermine AD security and, consequently, the security of servers, workstations and other information assets. As a result, data confidentiality, integrity and availability would no longer be assured.

3.2.B. Recommendations

We recommend that the relevant business units integrate AD-related risks into the current routine IT risk analysis process. Active Directory security controls will need to be adjusted based on the findings of this analysis.

3.2.C. Action Plan of the Relevant Business Unit

The relevant business units have validated our recommendations and will forward their action plan to us at a later date.

3.3. LOG FILES

3.3.A. Background and Findings

A log file is a record of all the events that occur within the city's systems and networks. Log files consist of log entries, each of which contains information on a specific event that has occurred within a system or network. Many log files contain records linked to IT security-related events. These security logs can be generated by numerous sources, including server operating systems, workstations, network equipment, user applications and security software such as antivirus programs, firewalls and intrusion detection and prevention systems.

The number, size and variety of log files have increased considerably in recent years. This has created the need for a log file management process that covers the generation, transmission, storage, analysis and disposal of security log data.

Managing log files is essential to ensuring that security events are recorded in a sufficiently detailed manner for an appropriate length of time. Analyzing log files is vital to detecting security incidents, policy violations, fraudulent activities or operational problems.

Log files are also essential for forensic accounting audits and analyses and internal inquiries and in identifying operational trends and long-term issues. These log files are admissible in court as evidence in cases of fraud or embezzlement.

The accuracy and integrity of log files must be maintained at all times to prevent them from being tampered with by an attacker. Log files on a domain controller, for example, can be modified by anyone with system administrator privileges and read, write and delete rights. As a result, anyone with system administrator privileges is in a position to perform illicit actions and then erase all traces of these actions from the log files.

FINDING

We confirmed that AD-related events are recorded in log files. However, they are not automatically transferred in real time to a dedicated server that restricts system administrators to read-only access. Consequently, anyone with AD administrator rights could intentionally or unintentionally perform illicit actions and, given their high-level privileges, easily erase all traces of these actions from the log files. In the event of an investigation, it would be impossible to trace any such events back to the perpetrator. It would also be difficult to present the incomplete, inaccurate journal logs as admissible evidence in a trial scenario.

FINDING

We determined that AD administrators did not review log files on an ongoing basis. They are checked intermittently whenever a problem arises. Given the volume of information they contain, however, and the lack of automated event filtering tools, system administrators do not have enough time to manually detect suspicious activity in AD. They are therefore unable to respond proactively to potential problems or security breaches.

3.3.B. Recommendations

We recommend that the relevant business unit:

- **Implement the necessary tools to set up a centralized, dedicated server for event logging purposes. Access to this server should be restricted to read-only privileges for system administrators in the division responsible for IT operational security. All read, write, delete and other access rights on this server could be granted to the IT security department that is not in charge of tactical and operational security for the AD environment. This would help ensure the appropriate segregation of duties.**
- **Regularly review log files to detect problems and anomalies in a timely manner.**

3.3.C. Action Plan of the Relevant Business Unit

The relevant business unit has validated our recommendations and will forward its action plan to us at a later date.

3.4. ANTIVIRUS SOFTWARE

3.4.A. Background and Findings

Domain controllers are the brain and central nervous system of Active Directory. If they are not properly protected against malicious software, they could fall victim to a computer virus.

Antivirus programs are applications that make it possible to detect, disable and remove malicious software (e.g., viruses, Trojan horses, worms). Malicious software, or malware, is software that is developed and spread over the Internet for the purpose of compromising the security and performance of computer systems.

An antivirus program generally has two components. The first checks new files and emails in real time. The second performs full scans of all the data on a computer (including the hard disk, memory and any removable media) on an intermittent basis.

Antivirus software uses a signature file (which contains the virus signatures of malicious programs) to detect the presence of malware. It matches these signatures with the data on the computer.

Antivirus software is only effective if the signature file is up to date and able to detect malicious software quickly and efficiently. Having an antivirus program with an obsolete signature file is akin to having no antivirus program at all.

Antivirus software also generates reports and alerts in a timely fashion to keep system administrators abreast of any infections that are found or suspected. Infections must be treated as fast as possible to prevent them from spreading to other Windows workstations and servers. Sound security practices suggest that real-time alerts be sent to administrators' inboxes or pagers and that administrators review reports on a regular basis.

FINDING

For two of the seven ADs, which together are connected to six domain controllers, we determined the following:

- **Four domain controllers were not running an antivirus program.**
- **One domain controller was equipped with an antivirus program that had been disabled.**
- **One domain controller had an antivirus program with an outdated virus signature file.**

Should a virus hit, the risk may spread not only to the domain controllers but also to all AD resources, including workstations and other servers, and possibly beyond. The severity of the infection and the extent of the resulting damage are directly related to the speed with which malware is detected and removed.

3.4.B. Recommendations

We recommend that the relevant business units proceed as follows:

- **Ensure that all domain controllers are equipped with an antivirus program with regularly updated virus signature files**
- **Implement a formal, routine (ideally daily) process for reviewing antivirus reports**

3.4.C. Action Plan of the Relevant Business Unit

The relevant business units have validated our recommendations and will forward their action plan to us at a later date.

3.5. PASSWORD POLICY

3.5.A. Background and Findings

A password policy can be used to require users to create strong passwords. Such a policy is defined by a number of security settings, including password length, complexity, expiry and history.

One of the aspects of password policy requires users to change their passwords frequently. As a rule of thumb, the shorter the interval between password changes, the tighter the security. Similarly, longer passwords are stronger than shorter ones.

The STI procedure entitled *[TRANSLATION] Standard Concerning Access Keys for IT Resources* establishes password requirements such as expiration period, minimum length and history.

In section 3.2 of the *[TRANSLATION] Standard Concerning Access Keys for IT Resources,* the specified password requirements are as follows:

- Regular users:
  - Expiration period: 90 days
  - Minimum length: eight characters
  - Password history: six most recent passwords
- Administrators:
  - Expiration period: not specified, therefore the same as regular users'
  - Minimum length: eight characters
  - Password composition: must contain at least one uppercase letter, one lowercase letter, one numerical digit and one special character
  - Password history: not specified, therefore the same as regular users'

These standards, which are derived from the city's IT security policy, apply to all administrative units, including the 19 boroughs. They are essential, as they ensure a consistent level of security from one domain controller to the next and, consequently, from one AD to the next.

We compared the city's standard 90-day password expiry with Microsoft's recommendation of 30 to 90 days. It is worth nothing that the city's standard expiry for any password was 30 days when we conducted our tests in October 2010. On January 28, 2011, the STI increased the period to 90 days for passwords for Windows, Internet access, the SIMON program and the central IBM computer. Although the 90-day expiry complies with best practices, it is on the upper end of the suggested range.

Password length and complexity are two components that can be used to strengthen network security. For example, there are over 2.1 billion (36^6) combinations possible with a six-character password based on 26 letters (A through Z) and 10 numerical digits (0 through 9). This increases to 2.8 billion (36^8) possible combinations with an eight-character password. These days,

considering the number of password decrypt tools that are readily available online, their level of sophistication and the constant improvements being made by hackers, it is more important than ever to use strong passwords that are more complex than simple dictionary words or rudimentary number combinations (e.g., 11111111).

The password history setting fixes the number of recently used passwords Active Directory records so that AD users and administrators cannot reuse them.

FINDING

We noted the following weaknesses:

- **Expiration period: for one out of seven ADs, passwords have no expiry; users are never prompted by the system to change their password and can therefore keep the same one for an indefinite period of time.**
- **Password length: for five out of seven ADs, the minimum password length falls short of the minimum specified in the city standards.**
- **Complexity: for five of the seven ADs, password complexity verification was not enabled.**

Because current password policy is inadequate, users and administrators passwords could easily be compromised. It has been proven that the strength of a password is directly proportional to how often it changes, its length and its complexity. If the passwords for high-privilege accounts were to fall into the hands of an attacker, the security of the domain controllers and assets managed by ADs would be compromised.

3.5.B. Recommendations

We recommend that the relevant business units set parameters for password expiry, minimum length and complexity to comply with the requirements of the standard established by the city.

3.5.C. Action Plan of the Relevant Business Unit

The relevant business units have validated our recommendations and will forward their action plan to us at a later date.

3.6. ACCOUNT LOCKOUT POLICY

3.6.A. Background and Findings

Account lockout policy can be used for both administrator and user accounts. Its main function is to determine the length of time an account will remain blocked after a given number of failed logon attempts. We examined the following three functions vis-à-vis the provisions in the city's standard (established by the STI):

- Account lockout duration: This security setting determines the number of minutes an account will remain disabled before automatically reverting to unlocked status. The standard is 15 minutes.
- Account lockout threshold: This security setting defines the number of failed logon attempts that triggers the lockout of a user account. A locked account cannot be used until it is reset by an administrator or the lockout duration expires. The recommended number of failed logons in the standard is three.
- Reset account lockout counter: This security setting controls the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset. The standard is set at 15 minutes.

FINDING
We observed that the account lockout feature was disabled in two of the seven ADs.

An unauthorized individual could therefore use special tools to make an unlimited number of attempts to break into the domain controllers. If these attempts were successful, the security of the domain controllers and assets managed by ADs would be compromised.

FINDING
For one AD, the account lockout threshold was set at eight failed logons. In two others, the setting was five. In all three of these cases, the value exceeded the city's standard of three failed logons.

3.6.B. Recommendations

We recommend that the relevant business units align their account lockout policy with city standards.

3.6.C. Action Plan of the Relevant Business Unit

The relevant business units have validated our recommendations and will forward their action plan to us at a later date.

3.7. HIGH-PRIVILEGE ACCOUNTS

3.7.A. Background and Findings

Someone with a high-privilege account can obtain unlimited rights to AD, including domain controllers and workstations. These accounts are assigned to individuals who possess the necessary Windows qualifications, IT security skills and network architecture expertise. They must be trustworthy. In addition, the responsibilities that come with a high-privilege account must not conflict with other job duties, so that the fundamental principle of the segregation of duties is maintained.

Because high-privilege accounts give users access to event and audit logs, an ill-intentioned individual who obtains these rights could engage in illicit activity and then erase all traces of these actions from the log files.

FINDING

For six out of the seven ADs, we determined that there were a large number of high-privilege accounts that are not required for business purposes. This may mean that the accounts are unused or the privileges granted are unjustified. Both scenarios greatly increase the possibility of these privileges being used in an unauthorized manner.

FINDING

For one AD, we noted that some high-privilege accounts were assigned to groups that should not possess this level of access, including consultants, interns, test accounts and so-called generic accounts. In the latter case, the biggest danger is the widespread use by employees of the account passwords. If generic accounts were used by several individuals, it would be difficult to determine who is accountable for actions recorded in event or audit logs.

FINDING

In five of the eight ADs audited, we noticed there were accounts identified as Administrateur or Administrator. These are easy prey for attackers attempting to break in and take control of AD. Generally, an account with a generic, easily identifiable name should be renamed or downgraded. Otherwise, an attacker could use it to take over AD and compromise data, server and workstation security.

Having too many high-privilege accounts that are not required for business purposes greatly increases the risk of an attacker using one of these accounts to take control of AD to commit fraudulent acts. Should such an event occur, asset security, confidentiality, integrity and availability could no longer be assured.

3.7.B. Recommendations

We recommend that the relevant business units proceed as follows:

- **Reduce the number of high-privilege accounts and ensure they are assigned solely to those who legitimately need them.**
- **Revoke high-level privileges from the following types of accounts:**
  - **consultants**
  - **interns**
  - **test accounts**
  - **generic accounts**
- **Rename Administrateur and Administrator accounts.**

3.7.C. Action Plan of the Relevant Business Unit

The relevant business units have validated our recommendations and will forward their action plan to us at a later date.

3.8. DOMAIN CONTROLLER CONFIGURATION STANDARDS

3.8.A. Background and Findings

Domain controller configuration standards are technical guidelines that specify the configuration settings to be applied during server setup. These configuration settings are taken directly from security policies and procedures. The system administrator therefore knows the exact value to assign each configuration setting when installing the operating system so that domain controllers comply with the city's security requirements.

These standards are also necessary to ensure a consistent level of security, since the settings apply to each domain controller. This in turn reduces the danger of one domain controller being more vulnerable than another.

FINDING

In some cases, domain controller installation and configuration procedures are documented but have never been updated. In others, we determined that no standards or configuration guidelines had ever been developed. Servers are configured based on the level of knowledge of the system administrators.

3.8.B. Recommendations

Because setup procedures have not been updated, the configuration settings might be inconsistent with the city's security requirements. As a result, new domain controllers could be set up using inadequate configuration settings, exposing them to potential security risks. We recommend that the relevant business units prepare or update a set of domain controller setup procedures.

3.8.C. Action Plan of the Relevant Business Unit

The relevant business units have validated our recommendations and will forward their action plan to us at a later date.

3.9. NON-ESSENTIAL SERVICES

3.9.A. Background and Findings

A *service* is a type of application that runs in the background of an operating system. Services are not used directly by users, but they support features that are essential for Web, email and database servers. Services are generally long-running, i.e., they execute at system startup and remain in operation until the computer is shut down.

Industry best practices recommend that only essential services be enabled on domain controllers. This is because some services generate security risks that are even higher when a server acts as a domain controller and because each service takes up system resources, which may hinder system performance and, consequently, availability. Limiting services to those that are strictly necessary for the smooth operation of the domain controllers also minimizes the chance of potential attackers using these services to access the system.

There are three settings for enabling (or starting) services:

- Automatic: the service automatically launches when the computer starts up
- Manual: the service can be launched manually by the system administrator or another service that requires it
- Disabled: the service does not launch

Any services that are not essential to the operation of domain controller servers must be set to "Disabled" so that they cannot be enabled without a system administrator.

To determine whether essential services were the only services enabled on the domain controller servers in the business units we audited, we obtained a list of the services on each server, along with the configuration settings of each.

FINDING

We determined that several non-essential services were not disabled in the business units we audited. In some business units, for example, the following were not disabled:

- **IIS Admin Service: This service allows the server to manage Internet services (e.g., Web server). Using IIS Admin Service, unauthorized individuals could take over the system by exploiting numerous website vulnerabilities. Moreover, it is strongly advised that Web servers not share a server with a domain controller. Otherwise, an attack on the website would compromise not only the Web server but also AD as a whole and its resources.**
- **Indexing Service: This service indexes the contents and attributes of files found on local or remote computers. An attacker could use this information to obtain unauthorized access to the information in these files and compromise data confidentiality and integrity.**
- **Special Administrator Console Helper: This service makes it possible to run system administration commands remotely. An attacker could use this service to take over the system, thus compromising domain controller and AD security.**
- **Application Management: This service provides software installation features (assign, publish and delete). Attackers could use this service to install malware or delete applications essential to user workstations, thereby reducing system availability.**
- **Distributed Link Tracking Client: This service enables client programs to track files that have been moved within a system or to another computer. Using this service, attackers could gain access to confidential information about given applications (e.g., employee files anywhere on the system) and thus compromise data confidentiality.**
- **Portable Media Serial Number Service: This service makes it possible to recover serial numbers of any portable devices connected to a computer. Using this service, attackers could download protected content to a device, thereby compromising data confidentiality.**

The startup settings of the non-essential services are not properly configured. The risk of an attack on the servers is therefore greater, as attackers could take advantage of the situation to gain privileged access, similar to that of an administrator, and take over the entire server.

In such a scenario, not only would domain controller security be compromised, but AD security would be vulnerable as well. As a result, the confidentiality, integrity and availability of data and resources would no longer be assured.

3.9.B. Recommendations

We recommend that the relevant business units enable only services required to meet the city's needs and disable all non-essential services in order to increase the level of logical security for the domain controller servers.

3.9.C. Action Plan of the Relevant Business Unit

The relevant business units have validated our recommendations and will forward their action plan to us at a later date.

3.10. DOMAIN CONTROLLER SECURITY PATCHES

3.10.A.Background and Findings

Vulnerabilities are weakness in a computer system that can be exploited by attackers to jeopardize operating system security.

By taking advantage of these vulnerabilities, attackers can gain access to a system, going so far as to take over servers and workstations. Vulnerabilities are generally addressed very quickly by software providers using security patches. However, if the patches are not regularly applied, servers will remain susceptible not only to new vulnerabilities but to older ones as well.

Microsoft addresses AD-related software vulnerabilities as soon as they are identified using Service Pack or Hotfix patches. It is therefore important to ensure domain controllers have the latest Microsoft patches installed, especially as instructions on how to exploit vulnerabilities are often documented and readily available on the Web.

By installing security patches, system administrators can help minimize the possibility of attack.

FINDING

The three domain controllers belonging to one business unit's AD had not been updated since June 2010. This means that these domain controllers have been vulnerable to attack since June 2010.

Should an attack of this nature occur, unauthorized individuals could obtain administrator-level access and take over AD and its resources (e.g., workstation, file server, data).

3.10.B.Recommendations

We recommend that the relevant business unit implement a formal security patch update process on its servers. This process would need to include security patch installation tests in a test or development environment to ensure that patches installed will be compatible with existing applications and not cause any operational problems.

3.10.C.Action Plan of the Relevant Business Unit

The relevant business unit has validated our recommendations and will forward its action plan to us at a later date.

4. APPENDIX

4.1. ACTIVE DIRECTORY GLOSSARY OF TERMS

This appendix contains the definitions of various terms associated with Active Directory, presented in alphabetic order.

DOMAIN:

A domain is the basic structural unit within AD. It is a set of computers or users that share the same directory database. A domain has a unique name within the network. Domains serve as a security boundary by restricting the rights of an administrator or any other user with privileges to the resources in this domain.

DOMAIN CONTROLLER:

A domain controller is a server that stores and duplicates Active Directory data. It propagates any changes made to the directory, authenticates users and logons and performs searches in the directory. A domain can have one or several domain controllers. Each domain controller can receive or duplicate changes made to any other controller in the same domain. It is essential that domain controllers be protected by security settings, because if domain controller security is compromised, all AD security is at risk.

TRUST:

A relationship that allows the users of one AD to have access to the resources of another.