Table of Contents

Project Summary 1

Review of Other Work 3

Project Rationale 5

Systems Analysis and Methodology 7

Goals and Objectives 10

Project Deliverables 15

Project Timeline 21

Project Development 21

Conclusion 26

Appendix A: Implementation Configuration Documentation 28

Appendix B: Testing Documentation 29

Appendix C: Maintenance Procedures 32

References 34

Capstone Project Summary

I have been employed with [redacted] a medium sized financial institution, as a Network and Data Center Administrator for the last five years. The company has a headquarters location and seven branch locations. Some of my assigned duties are the management of network devices, management of Microsoft Windows servers, and access control management for user account access to network resources. The company's security policy requires all users to change their user account passwords every forty days. The policy includes all network access user accounts including the accounts of the network administrators that manage devices.

The security policy is actively enforced on Microsoft Active Directory user accounts. There is a Group Policy set up in Active Directory that causes each user account password to expire after forty days forcing users to change their passwords. The user accounts used by network administrators to manage the company's network switches were not the same as their Active Directory user accounts and the policy was only passively enforced. Each switch was configured to use a local database of user accounts for administrators.

There are a total of fifteen network switches in the company and three network administrators to manage them. There are eight switches installed at the headquarters location and one switch at each of the seven branch locations. Since each switch had its own database of user accounts, the network administrators were required to connect to each switch every forty days to change their password. There were mixed results for each administrator every forty days.

Sometimes an administrator would change their passwords on all fifteen switches as required by the security policy, but unfortunately it didn't always happen that way. There were times they would change their passwords on some, but not all of the switches leaving some

completely unchanged. Many times the passwords were not changed in the forty-day time frame as required. When the appropriate password changes did not meet the forty-day requirement, the administrator, and the department, were no longer compliant with the security policy.

To resolve the possible non-compliance issues, it was determined that the network administrators should use their Microsoft Active Directory user accounts to access and manage these switches. As mentioned above, there is a Group Policy in place forcing users to change their account passwords every forty days. By using their one centrally managed Microsoft Active Directory user account for network management it eliminates the requirement for the administrators to change user account passwords on all fifteen switches every forty days.

The company already utilized a Remote Authentication Dial-In User Service or RADIUS configured on a Windows Server to authenticate with Active Directory user accounts for VPN access. For this project I configured RADIUS to also be used to authenticate the user accounts of the network administrators for managing the network switches.

To complete this project, I configured each switch as a RADIUS client on the Windows Server. I then, on that same server, created a network policy that grants access to the three network administrator's Active Directory user accounts.

Once the RADIUS configuration was completed on the server I configured each of the fifteen switches. Each individual switch needed to be configured with the IP address of the RADIUS server, and to use that server for its authentication method. Each switch was then configured to use both RADIUS and a local user account database as a backup in case the server is unavailable. The individual local user accounts for the network administrators were removed from each switch and a single local user account has been created for that backup purpose.

At the completion of each switch configuration, access was tested for all three network administrator's user accounts and recorded in a report for documentation of its success. Other documentation of this project includes sample Force 10 configuration commands detailing how RADIUS was implemented, a sampling of the RADIUS debug command output recording a user being authenticated for management access to a switch, and documentation on maintaining users and switches in the future.

Review of Other Work

The proposed solution to the issue of the corporate security policy's forty-day password requirement and network administrators' non-compliance will required multiple technologies, but there was one technology at the solution's core and that is Remote Authentication Dial-In User Service (RADIUS). RADIUS is an Internet Engineering Task Force (IETF) standard protocol described by Cisco Systems (2006) as "a client/server protocol" where the "client passes user information to designated RADIUS servers…RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary"

Using the description from Cisco Systems as a model, the Force 10 switches were configured as the RADIUS clients, that pass user information to the company RADIUS server. The RADIUS server then authenticates the network administrator user accounts from Active Directory to grant access for management of the switches. To allow this communication between the switches and the server using the RADIUS protocol both the server and the switches required new configuration changes.

The company already utilized a server with Windows Server 2008 R2 and the Network Policy Server (NPS) role installed. "Network Policy Server (NPS) is Microsoft's implementation

of a RADIUS server in Windows Server 2008 R2." (Panek, 2011, p. 662). Within NPS there were two necessary configuration changes.

The first NPS configuration change was to add each Force 10 switch as an individual RADIUS client. The requirements for a RADIUS client configuration are the IP address of the switch and a phrase or word that will be used as a shared secret. A shared secret is "a text string that serves as a password between: A Remote Authentication Dial-In User Service (RADIUS) client and RADIUS server." (Microsoft TechNet Library, 2008). The second NPS configuration change was to create a Network Access Policy to be used with the RADIUS clients. This policy is used to "determine who can and cannot connect; you define rules with conditions that the system evaluates to see whether a particular user can connect." (Panek, 2011, p. 689). Each Network Access Policy has assigned attributes, and this new policy has been assigned a Windows Group and the newly created clients. Any user accounts assigned to the Windows Group chosen in the policy will be granted access to the RADIUS client. A new group was created in Active Directory for this purpose.

Microsoft Active Directory is defined as "an extensible directory service that enables centralized management of network resources." (Smart Brain Training Solutions, 2014, p. 7). Active Directory's role or responsibility is determined to be "authorizing access, managing identities, and controlling the relationships between the resources." (Smart Brain Training Solutions, 2014, p. 7). Within the directory are manageable objects such as Users, Computers, or Groups. Microsoft TechNet Library (2009) defines an Active Directory group as "a collection of user and computer accounts, contacts, and other groups that you can manage as a single unit. Users and computers that belong to a particular group are referred to as group members." A new

Active Directory group, with all the network administrators' user objects added as group members, have been created for use with the NPS Network Access Policy.

Once all the RADIUS server configurations were completed the Force 10 switches also needed three configuration changes in order to complete the communication channel with the server. The first configuration change required the IP address of the RADIUS server and the same shared secret configured for the client configurations on the server.

The next change configured authentication with the RADIUS server through the "Authentication, Authorization, and Accounting mechanism, commonly referred to as AAA." (Bhatnagar, 2002, p. 221). That required the creation of "a method list that defines what resource will be used…such as the local database". (Santos & Stuppi, 2015, p. 285). For this method list RADIUS and local database has been chosen, with local database used only as a backup if the RADIUS server becomes unavailable.

The third and final switch configuration change applied the method list as the default list for remote connections via SSH over the VTY lines or "virtual terminal because it emulates the function of a terminal." (Bhatnagar, 2002, p. 83) allowing the network administrators to connect to the switches remotely for management.

Once the RADIUS server and Force 10 switch configuration changes had been completed the the network administrators have tested authentication with their Active Directory user accounts to verify proper communication of the RADIUS protocol.

Project Rationale

The project rationale was really simple – it provided a no cost solution to the company's discovered issues. The project's solution utilized software and hardware already within the

company's network environment. This means that there was no need for new software licensing or hardware to be procured. As a result, the company saved both time and money.

In addition to the time and cost savings, there is strong rationale for the solution's answer to the network environment's user account management and security policy non-compliance issues. By using Microsoft Active Directory user accounts for the management of the Force 10 switches two solutions have been provided – a central user account management system and active enforcement of the company security policy's password requirements.

Before this project there was a decentralized user account management system in place for the Force 10 switches. The user account databases were splintered individually – one database for each switch. Managing multiple user accounts on multiple devices was much more complicated and far less efficient than managing user accounts centrally, or from one database or device. By moving the user accounts off of each individual switch the user accounts database has become simpler to manage. There is now no longer be a need to connect to each switch to add new, disable old, or change passwords for current user accounts. The solution has provided one central management platform for user account management.

In addition to centralized management of user accounts, Active Directory has a Group Policy that is applied to all user accounts causing passwords to expire every forty days. This actively enforces the company security policy's password change requirements by compelling the users to change their passwords in the proper time frame. Not making the proper changes will result in no access to any network resources for the user – including management access to the Force 10 switches. To regain access, the user will need to contact a network administrator to unlock the expired user account and then make the proper password changes. Using Active

Directory user accounts for Force 10 management access will ultimately lead to full compliance with the company security policy for all network administrators.

To configure Active Directory user account access to the Force 10 switches, current services within the company's environment were used. As previously mentioned, Remote Authentication Dial-In User Service (RADIUS) was already configured on a Windows Server and was used to authenticate Active Directory user accounts for VPN access. Since Force 10 switches support RADIUS authentication, leveraging the current RADIUS server was the logical choice to enable Active Directory user account access.

To review, the rationale behind this project was a quick, no cost solution, that utilized licenses and equipment within the current network environment, and centralized user account management across all devices with active enforcement of the corporate security policy's password requirements.

Systems Analysis and Methodology

The successful execution of any project requires a systematic approach that breaks a project down into smaller or more manageable phases. While this project is not related to software programming and development, it has followed the Software Development Lifecycle (SDLC) methodology – a methodology that has broken down the project into the following phases: Analysis, Design, Implementation, Testing, and Maintenance.

The Analysis phase comprised of a preliminary analysis of the state of the company's network environment and the desired future state. Then the differences between the two states were compared. This analysis attempted to determine how the project could provide a solution to the performance gap between the two states. The preliminary analysis exposed an issue that has, at times, led to non-compliance with the corporate security policy's password requirements.

The issue stemmed from decentralized or splintered user account databases located across fifteen network switches. The fifteen switches were each configured with local user account databases and no active enforcement of the policy's password requirement, which states passwords must be changed every forty days. This had caused some network administrators to become non-compliant with the policy by not changing their password on some, or all of the switches, within the required timeframe.

The desired state of my company's network environment was the elimination of the decentralized user account databases from each individual switch. This was accomplished by replacing them with the one centralized Active Directory database currently in place within the company's network environment. By using Active Directory as the user database it will now also actively enforce the forty-day password change requirements by using a Group Policy that causes user accounts to expire if not changed within the appropriate time. The performance gap has been closed by leveraging the company's RADIUS server to authenticate user accounts for Force 10 switch access.

The Design phase consisted of the planning and design of the project. While planning this solution, the analysis information from the previous phase was used to determine it was best to utilize the resources that were already in place within the company's network environment. These resources included the company's Active Directory for the user account database, the company's Remote Authentication Dial-In User Service (RADIUS) server, and the Authentication, Authorization, and Accounting (AAA) support of the Force 10 network switches.

The first part of the design required the creation of an Active Directory user group for group member access to the switches. The next entailed the configuration of the RADIUS server, which required the configuration of each Force 10 switch as an individual RADIUS client. Then

the creation of a new Network Access Policy within Network Policy Server (NPS) was required. The Network Access Policy needed to be configured to allow access to the newly created Active Directory group and applied to the new RADIUS clients. The final piece in the design was the configuration of AAA authentication using the RADIUS server as its primary method on each Force 10 switch.

The Implementation phase of the project carried out the design detailed in the Design phase. All of the new configurations within Active Directory, Windows Server 2008 NPS, and Force 10 were performed to implement the project's solution. All of the required configuration changes were completed successfully and recorded in the implementation configuration documentation.

Once the Implementation phase had completed the Testing phase began. Each newly configured switch had been tested by all three of the network administrators. Each administrator attempted to log in to each switch with their Active Directory user account to test for proper functionality. After each attempt, the administrator provided a handwritten check mark with the date noted next to it in either the success or failure column of a cart. The chart lists all of the locations, switches, and network administrators. All of the switches and user accounts have logged in successfully as evidenced from the chart.

The final phase of the project was the Maintenance phase. This phase documented and detailed how to maintain the newly implemented solution. This documentation included a how-to guide that will provide step-by-step instructions on how to add or remove additional Force 10 switches in the future.

Goals and Objectives

After the most recent internal audit report, the Information Technology (IT) department was found to be non-compliant with the corporate security policy's password requirements for user accounts on the company's network switches. The security policy's passwords requirements determine approved password attributes, such as the minimum amount of characters to be used in a password, the complexity of each password, and the duration a password can be used. The duration requirement in particular states that all passwords must be changed every forty days. The audit report exposed network administrator user account passwords that did not meet the forty-day requirement.

Due to the poor result in the audit report, the Director of Information Technology set a goal for the department to become fully compliant with the security policy before the company's next audit, and to do whatever possible to prevent the failure being repeated in the future. He further declared that this goal be achieved with the least amount of outside resources as possible since additional costs are not accounted for in the department's budget.

After learning of the new department goal from the Director, the IT Manager introduced a new project for the department and chose to assign the role of Project Lead to me. I immediately began the Analysis phase of the project by analyzing the current state of the network environment. The research revealed that each Force 10 switch has its own database of user accounts and the network administrators must connect to each switch every forty days to change their password. Sometimes administrators change their passwords on all fifteen switches within the forty days as required by the security policy, but unfortunately that doesn't always happen. I then met with the IT Manger to discuss these findings. The result of that meeting

kicked off the beginning of the Design phase of the project and the following objective was determined – configure Active Directory authentication for the Force 10 switches.

This objective was determined due to the analysis revealing a compounded network environmental issue that has already lead to, and could continue to lead to, the departments' non-compliance. The compounded issue was the combination of the individual user account databases on each of the switches along with no active enforcement of the corporate security policy's password requirements. This created a scenario where network administrators were required to change their password once on each of the fifteen switches every forty days, and if they failed to do so, there was no active enforcement of the password requirements leaving any overdue accounts enabled.

By using Active Directory, the network administrators no longer have to manage fifteen different user accounts across as many devices. They have just the one Active Directory user account. That one user account has the password duration requirement actively enforced to disable any account with passwords forty days or older. That has fulfilled the department goal of not allowing the issue to reoccur. By utilizing resources already in place within the network environment, the cost has been kept very low, and implementation has been completed before the next audit. Completing this one objective meets all the requirements set in the department goal.

To complete this objective, I leveraged the Authentication, Authorization, and Accounting (AAA) support of the Force 10 switches. That feature allows authentication with a Remote Authentication Dial-In User Service (RADIUS) server. The company already had a RADIUS server running on a Windows server within its network environment. The design consisted of new configuration changes within Active Directory, the Windows RADIUS server,

and each Force 10 switch. To manage the required configuration changes more efficiently the objective had been broken down into three configuration phases.

The first configuration phase involved all required changes within Active Directory. A new Active Directory user group was created. This new group will be used to control which users can access the Force 10 switches. There are currently three network administrators that require management access to the switches, so the user objects of those network administrators have been added as group members to ensure they are granted proper access. Once those steps had been completed the first phase was considered complete.

The second configuration phase comprised of all the necessary changes within Network Policy Server (NPS) – the Windows Server 2008 R2 role that acts as the company's Remote Authentication Dial-In User Service (RADIUS) server. The first configuration to NPS was the creation of each Force 10 switch as an individual RADIUS client. To complete this change, the IP address of each switch and a shared secret password were required. Each switch's NPS RADIUS client has been named with the same prefix. That is was necessary to complete the next step of this phase – the creation of a new Network Access Policy.

Once the new RADIUS client configurations had been completed a new Network Access Policy was created. This new policy required two attributes – a Client Friendly Name and a Windows Group. The Client Friendly Name was configured with a wild card. That wild card is the prefix commonly used with each of the NPS RADIUS clients created in the previous step followed by an asterisks. That applies the policy to all the RADIUS clients beginning with that same prefix. The Windows Group attribute was configured with the Active Directory group that had been created in the first configuration phase of this project objective. The access policy must be set to either grant or allow access. The completed Network Access Policy configuration

resulted in granting access to the combined attributes – allowing the members of the Active Directory group access to the RADIUS clients.

Each configuration phase has helped the next. The first phase created the Active Directory group for use in the second phase. Then the second phase created the Force 10 switches as clients of the RADIUS server. The third and final configuration phase encompassed all of the Force 10 network switch configurations required to communicate properly with the RADIUS server. All the steps of this phase have been performed or repeated on each individual switch.

The third phase required the IP addresses of both the RADIUS server and each RADIUS client, as well as the shared secret password configured on each RADIUS client. The server IP address was configured as the RADIUS host on each Force 10 switch. That also included the shared secret used on the client. The shared secret must be the same or match for each server and client created. The second step located the switch interface configured with the same IP address on the switch that was used to create the RADIUS client in the previous phase. That switch interface with that same IP address has now been assigned as the RADIUS source-interface. The source-interface assignment ensures that the RADIUS server only receives communication from the same IP address the RADIUS client is configured to use. The RADIUS server will only respond to a device using the IP addresses configured for the clients.

Once the RADIUS host and source-interface changes were completed the Authentication, Authorization, and Accounting (AAA) configuration began. A new method list for authentication was created. This list configuration began with the AAA command for authentication, and was followed by the user group name, and login method types in the order they will be used. The

login method types order for this project design determined that the RADIUS server will be used first and then the local user database.

The local user database is still going to be needed as a backup login solution in case of a network or server outage that could prevent the switch from communicating with the RADIUS server. A new local database administrator user account has been created in the local database. This was configured as the same user name and password on each switch. Eventually, all the other local user accounts were deleted, but not till after all was tested and verified to function properly during the project's Testing phase.

Once the AAA method list and new local administrator user account was created the next step began. Each of the network administrators routinely access these switches remotely, so the method list has been applied to all of the virtual terminals or VTY lines of each switch. The method list was applied by using the login command, followed by the word authentication signifying the type of list to use, and the user group name that was assigned in the method list configured in the previous step. This was configured on each virtual line. Additionally, another command setting the privilege level on each VTY line was issued. The privilege level has been set to the number fifteen, which grants the highest privilege to those that login on each of those lines.

Once these three configuration phases had been completed the Testing phase of the project began. Access to each switch was tested by the three network administrators that have been assigned as members of the Active Directory group. All of the network administrators successfully logged in to each of the configured Force 10 switches using their Active Directory user accounts. This verified that the project's objective of configuring Active Directory

authentication for the Force 10 switches had been completed successfully, and as a result, achieved the IT Department goal.

The goal set forth by the Director of IT has been fully achieved. The solution provided in this project has corrected the the non-compliance issue found in the internal audit report. By utilizing the current network resources of Active Directory and RADIUS it provided a low to no cost solution. Also, by using Active Directory for authentication it prevents the issue from happening again.

Project Deliverables

Each phase of this project has had its own output or deliverable. Some of beginning sections of this document are the measurable result of this project's Analysis and Design phases. An Information Technology (IT) department goal may have been set by management, but an actionable objective to achieve that goal could not be determined without all of the analyzing, meeting, and discussing that had taken place. Those activities have produced the concepts and design that ultimately led to some the various sections within this document. It is the extensive research of the various publications during the Analysis phase that has led to the creation of the Review of Other Work, and the meetings and discussions during the Design phase that has determined the Project Rationale section. Just as the Analysis and Design phases produced some sort of output or deliverable, so too will the Implementation, Testing, and Maintenance phases.

The plan and design of this project had determined that the Implementation phase of the project be broken into three separate configuration phases in order to satisfy the objective and achieve the department's goal. From these various configurations there was certain output that was recorded or documented. That output has become the first deliverable of this project and it has been titled the Implementation Configuration Documentation.

The first of these three configuration phases covered the Active Directory configuration. The beginning of this deliverable documents the details of the Active Directory changes that were made during implementation. That included the name of the Active Directory group chosen during its creation, and the user objects that were added as group members.

The second configuration phase comprised of the steps completed during the configuration of the Remote Authentication Dial-In User Service (RADIUS) server. This included the configuration of the RADIUS clients and the Network Access Policy of the Network policy Server (NPS). The second section of this first deliverable includes all of the relevant changes made within the NPS server role. Each of the fifteen Force 10 switches have been created as RADIUS clients in NPS, and they are listed in a table. Each row of this table includes the host name for each switch, the client name chosen when configured in NPS for that switch, and the IP address of the switch used for the RADIUS client configuration. The actual shared secret password for each RADIUS client is also included in each table row found within the official company documentation, but it will be left blank for the purpose of this public deliverable.

In addition to the RADIUS client table, the other half of this second section of the deliverable documents the details of the Network Access Policy configuration. It lists the name chosen during the configuration of the access policy, the access type chosen during the configuration, the Active Directory group name chosen for the Windows Group attribute, and then it lists the Client Friendly Name wild card that was configured.

The third and final section of this deliverable lists sample commands used to configure each of the Force 10 switches. These sample commands list all of the required commands that have been used to implement the proper communication between each of the switches and the

RADIUS server. The first command is the radius-server command. It was used to configure the RADIUS server IP address. The second command is the source-interface command. It was used to set the particular interface the switch will use to communicate with the RADIUS server. The two commands were used together to ensure that the communication channel between each switch (RADIUS client) and the RADIUS server always come from the same source IP address.

Additional Force 10 commands required list the configuration of the Authentication, Authorization, and Accounting (AAA) functions necessary for allowing the RADIUS server be used for authentication. The next command in the deliverable is the AAA command for authentication. It is used to configure the authentication method list. It includes the user group name configured on each switch and the login method types in the order they are to be used. The order of the login method types for this project are the RADIUS server and then the local user database.

These last commands included in the sample listing applies the method list to the virtual lines. It will allow RADIUS authentication via remote access connection. The first of these two commands is the login command. The login command lists the authentication method list that was created during the configuration and includes the user group name. The final command in this deliverable is the privilege level command. This lists the command parameters used in the configuration of the switch.

Once the work of the Implementation phase was finished and the configuration documentation produced, the project's first deliverable was complete. Then the Testing phase of the project began. It produced the project's second deliverable titled Testing Documentation. This deliverable includes two sections. The first section is a listing of all the Force 10 switches by branch name and and it includes each of their IP addresses. Under each of the switches is a

list of the three network administrators. Next to each of the administrators' names are two lines – left column for success and right column for fail. Each of the three network administrators have tested their ability to log in to each of the Force 10 switches with their Active Directory user account. With each attempt, they they have checked off whether their attempt was a success or a fail, and then they noted the date next to each check mark. There were no failures for any of the network administrators.

If issues were to arise, the Force 10 command for debugging RADIUS could be used to troubleshoot and help resolve the issue. The debug command allows a more granular visibility of the messages sent between the RADIUS client and server. The last section of this deliverable lists a sampling of the debug radius command output. The output sampling includes specific details about the communication channel conversation such as the IP address of the RADIUS server it is attempting to communicate with, the IP address of the switch's interface used to communicate with the RADIUS server, and the username being used in that authentication attempt.

Once all of the network administrators had completed and recorded all their log in attempts successfully the Testing Documentation was finished. The final phase of the project was the Maintenance phase. The deliverable for this phase of the project provided documentation of how to maintain the new configurations within the network environment. Similar to the deliverable from the Implementation phase this was broken into three sections. This deliverable has been titled Maintenance Procedures.

The first section of this deliverable describes how to manage and maintain the Active Directory users that will require or no longer require management access to the Force 10 switches. The IT department will see network administrators come and go. As a result, the

department procedure for adding and removing network administrator user accounts from the necessary Active Directory group is documented here. It includes the Active Directory group name and the steps to add or remove user accounts to the group using the Active Directory Users and Computers application.

The company's network environment is always changing. Sometimes a company branch location will need to be closed down, and other times a new branch will be opened. These situations call for the removal or adding of additional network switches in the future. This second section of the final deliverable documents the IT department's new procedure for configuring and maintaining any new and old RADIUS clients within Network Policy Server (NPS). This includes the required steps necessary to add new and remove old network switches as RADIUS clients within the Network Policy Server application.

As previously mentioned, there are times when new switches will need to be added to company's network environment. These situations arise when there is need to accommodate a new branch location, or when a branch location will require a network expansion to accommodate more employees. When these occasions come up, the IT department will rely upon the step-by-step procedure on how to configure RADIUS authentication on a Force 10 switch found within this third and final section. The first of the steps begins with how to configure the RADIUS server by using the radius-server and source-interface commands and includes the proper parameters. It then moves on to the AAA authentication method list creation steps.

The first step of the authentication method includes the AAA authentication command and the proper parameters required. The first parameter dictates the user group name to be used on all new switches. The second parameter of the method states the proper order of authentication types to be used in the list. Another step explains the creation of a local database

user account that is to be added as the backup account in case there is a communication problem with the RADIUS server.

The final steps of the switch configuration procedure provide instructions to enable the method list on each of the virtual or VTY lines. The first of these necessary commands is the authentication command. The step shows the proper user group parameters to be used on company switches. The final step explains how to issue the privilege level command on each of the VTY lines. It is used to enable the users that connect via the VTY lines to have all the administrative privileges they will need to manage the switch remotely.

These deliverables have provided evidence of the the project's completion. The Implementation Configuration Documentation deliverable documents the changes that were made within the network environment during the implementation. Further evidence is provided by the Testing Documentation, as it has proven that the configuration is functioning properly. Finally, the Maintenance Procedures, will document how to maintain the network environment in the future providing a step-by-step how-to guide to add and remove new devices as required.

Project Timeline

Project Deliverable or Milestone	Actual Duration	Actual Start Date	Actual End Date
Complete Implementation phase	½ day	2/1/2016	2/1/2016
Deliverable – Implementation Configuration Documentation	½ day	2/1/2016	2/1/2016
Complete Testing Phase	½ day	2/2/2016	2/2/2016
Deliverable – Testing Documentation	½ day	2/2/2016	2/2/2016
Complete Maintenance phase	½ day	2/3/2016	2/3/2016
Deliverable – Maintenance Procedures	½ day	2/3/2016	2/3/2016

Project Development

A recent audit report revealed that some of the company's user accounts on network switches were non-compliant. The Director of Information Technology (IT) set a goal for the IT department to become fully compliant with our company's security policy's password duration requirements. He also added that the issue should be prevented from happening again, and that whatever the solution, it should not generate any cost since the department had no budget for it.

The IT manager assigned the project to me. I manage the Force 10 network switches as well as Windows servers. I had implemented the company's RADIUS server in a previous project. That previous project was to configure Active Directory authentication for the company's VPN users. As a result of the experience I had gained from the previous project I had become very familiar with the company's RADIUS server. Since the Force 10 switches' Authentication, Authorization, and Accounting (AAA) feature supports RADIUS it was the logical choice to use the technology for this project's solution as well.

During the Analysis phase of this project, the objective of configuring Active Directory authentication for the company's Force 10 switches was chosen to achieve the IT department's goal set by the Director. By completing that objective, the goal was fully achieved by meeting all of the specific conditions set. Active Directory authentication has centralized the user account management of the Force 10 switches, will prevent future occurrences of non-compliance by enforcing the password duration requirements, was fully implemented before the next audit, and there were no additional department costs.

Problems Encountered

As a result of my prior experience with the company's RADIUS server, and additional experiences with both Force 10 and Cisco Systems AAA configurations, there were no problems or issues to report. I have learned greatly from those experiences. One example of an issue that came up in the past that has aided in the planning an implementation of this solution is the need of the Force 10 source-interface command.

In my past experience with the RADIUS server I had learned that a RADIUS client configuration can only allow one IP address and will accept communication from only that address. The company's Force 10 switch configurations have many interfaces with different IP addresses. The switch could choose to send RADIUS communication out any of the different configured interfaces and that communication could fail if chosen incorrectly. Knowing this information about the RADIUS client prompted me to thoroughly research and plan for the requirement. I found the source-interface command in that research. Setting the source-interface command on the Force 10 switches ensured that the proper interfaces and IP addresses are always used when communicating with the RADIUS server.

Another example of past experience would be understanding the output of the debug radius command on the Force 10 switches. When communication between a RADIUS server and client do not function correctly this output can be used to determine the cause. It causes a very verbose logging output and can determine the exact area where the communication fails. I was prepared with this information beforehand, but ultimately did not require to use it since the configurations went so amazingly well.

Reasons for Change

Project scope management can be difficult for many projects. Sometimes changes to scope are repeatedly requested and other times scope must change as a necessity. Whatever the reason for changes may be it usually will effect the project in both time and cost, and could lead to some delicate balancing in order to meet all that is required. At no time did this project require such balancing.

There were never any additional changes or requirements made by management. The project's scope had been distinctly defined, and its planning accounted for many of the possible issues that could have arose. As previously mentioned, past experience with the various technologies have aided greatly. As a result, there was never any reason for the scope of this project to change.

Unanticipated Requirements

Unknown factors could be considered normal obstacles in the planning and implementation of a project. Stirring around or moving through such obstacles could ultimately lead to unanticipated project requirements. Some may say that every project will encounter those

unknown or unanticipated factors. That every project scope will change as these factors will create new requirements. That has not been the experience with this project.

This project's scope, as mentioned above, did not see any need for a change in scope. The goal set forth by the Director of IT was very distinct and simply achievable. The objective of the project was specifically targeted to achieve that goal. Prior experiences have led to efficient planning and proper execution. As a result, there were no unanticipated project requirements. The objective was met and the goal has been achieved with no additional requirements.

Actual and Potential Effects

Implementing a new technology or solution has various effects on a company's environment. The actual effects this project has had on the company's network environment are less complicated user account management and full security policy compliance. This was the desired effects and they result in evidence of a successful completion of the IT department's goal.

This particular solution may have been a potential effect of the previously mentioned project of configuring the company's RADIUS server. The experience gained from that project was leaned on heavily in this one. It was the lessons learned from that project that ultimately led to choosing RADIUS as the solution here.

Configuring RADIUS in that project, and again in this one, may also lead to even more potential effects. The Network Policy Server (NPS) of Windows Server 2008 R2 provides RADIUS server capabilities. Those abilities include accounting as well well. A future project may include setting up the RADIUS accounting function on the Force 10 switches to keep a log of network administrator login activity for the switches.

Furthermore, NPS also features a module for Network Access Protection(NAP). This technology is also being explored as a future option for my company. It could be used to automatically move non-compliant laptop computers off of the production network, and to a different management network to provide proper remediation. The type of non-compliance it would remedy are laptops that have not had the proper security and anti-malware patches. By moving them to the remediation network they will receive the proper patches. Leaving these laptops on the production network creates potential unnecessary risk.

Conclusion

The recent [redacted] internal audit report that revealed user account passwords being found non-compliant with the company security policy's password requirements had set this project in motion. After receiving the failed audit report the Director of Information Technology (IT) was determined to have a perfect score in the next report. He set an IT department goal to become fully compliant by the next audit. He stated that the department should be fully compliant, that the password duration requirement issue must not happen again, and that it must be solved at no cost since there was no budget for it.

I was assigned the project and my network environmental analysis, paired with prior experience, chose to configure Active Directory authentication for the company's Force 10 switches as the project's primary objective. I then successfully implemented the required configurations within Active Directory, Microsoft Network Policy Server (NPS), and each of the fifteen Force 10 switches. Each network administrator tested proper access to each of the switches with their Active Directory accounts and encountered no issues at all. Consequently, the project objective was completed quickly and without issue to achieve the goal set by the Director.

The solution implemented for this project has been completely effective. The network administrators that manage the network switches no longer need to change their user account password once on each of fifteen switches every forty days. They now only need to change their Active Directory password as that account is now used for all of the devices. Also, since Active Directory enforces the password requirements, they are prompted to change their passwords when nearing the forty-day mark preventing the non-compliance issue from reoccurring.

Management is extremely delighted with the results of this new solution and is looking forward to the next audit. They are also pleased in the fact that the entire project has been accomplished both quickly and without additional cost. Subsequently, the project has been both an overwhelming success and an extremely effective solution.

Appendix A: Implementation Configuration Documentation

Active Directory

Group Name: Network-Switch
Members Added: netuser1
netuser2
netuser3

Network Policy Server (NPS)

Switch Hostname	RADIUS Client Name	IP Address	Shared Secret
HQSWITCH1	SW-HQ1	[redacted]	
HQSWITCH2	SW-HQ2	[redacted]	
HQSWITCH3	SW-HQ3	[redacted]	
HQSWITCH4	SW-HQ4	[redacted]	
HQSWITCH5	SW-HQ5	[redacted]	
HQSWITCH6	SW-HQ6	[redacted]	
HQSWITCH7	SW-HQ7	[redacted]	
HQSWITCH8	SW-HQ8	[redacted]	
BR1SWITCH	SW-BR1	[redacted]	
BR2SWITCH	SW-BR2	[redacted]	
BR2SWITCH	SW-BR3	[redacted]	
BR3SWITCH	SW-BR4	[redacted]	
BR4SWITCH	SW-BR5	[redacted]	
BR5SWITCH	SW-BR6	[redacted]	
BR6SWITCH	SW-BR7	[redacted]	

Network Access Policy

Policy Name: Network-Switch
Access Type: Grant Access
Windows Group Name: Active Directory Group – Network-Switch
Client Friendly Name: SW-* (wildcard)

Force 10

ip radius source-interface GigabitEthernet 0/48
radius-server host [redacted] key *(shared secret)*
aaa authentication login adgroup radius local
login authentication adgroup
privilege level 15

Appendix B: Testing Documentation

	Success	Failure
Headquarters		
Switch1 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Switch2 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Switch3 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Switch4 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Switch5 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Switch6 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Switch7 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Switch8 [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	
Branch 1		
Switch [redacted]		
Network Administrator 1	√ 2/2/2016	
Network Administrator 2	√ 2/2/2016	
Network Administrator 3	√ 2/2/2016	

	Success	Failure
Branch 2		
Switch [redacted]		
Network Administrator 1	√2/2/2016	
Network Administrator 2	√2/2/2016	
Network Administrator 3	√2/2/2016	
Branch 3		
Switch [redacted]		
Network Administrator 1	√2/2/2016	
Network Administrator 2	√2/2/2016	
Network Administrator 3	√2/2/2016	
Branch 4		
Switch [redacted]		
Network Administrator 1	√2/2/2016	
Network Administrator 2	√2/2/2016	
Network Administrator 3	√2/2/2016	
Branch 5		
Switch [redacted]		
Network Administrator 1	√2/2/2016	
Network Administrator 2	√2/2/2016	
Network Administrator 3	√2/2/2016	
Branch 6		
Switch [redacted]		
Network Administrator 1	√2/2/2016	
Network Administrator 2	√2/2/2016	
Network Administrator 3	√2/2/2016	
Branch 7		
Switch [redacted]		
Network Administrator 1	√2/2/2016	
Network Administrator 2	√2/2/2016	
Network Administrator 3	√2/2/2016	

Sampling from a Force 10 debug radius Command

These sample output shows one of the successful login attempts made by netuser1. It shows the server address as [redacted] *The switch is contacting the server from the Calling-station-id of* [redacted] *This output can be useful when communication fails. It could list the exact area where it fails.*

Feb 2 09:08:04 UTC: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user netuser1on line vty1 ([redacted]

Feb 2 09:08:04 UTC: %STKUNIT0-M:CP %SEC-5-RADIUS_ACCESS_ACCEPTED: Radius access accepted for user "netuser1"

```
26w2d12h :      Attribute 26      length 10      VSA : ...7.....x
26w2d12h :      Attribute 26      length 10      VSA : ...7.....2
26w2d12h :      Attribute 25      length 44      Class : L......7.......y.................x.{M........
26w2d12h :      Attribute  6      length  4      Service Type : 2
26w2d12h :      Attribute  7      length  4      Unknown :
26w2d12h : RADIUS: Received from id 29, code 2, Access-Accept
26w2d12h :      Attribute  1      length  6      User Name : netuser1
26w2d12h :      Attribute 31      length 12      Calling-station-id : [redacted]
26w2d12h :      Attribute  5      length  4      NAS Port : 1
26w2d12h :      Attribute 61      length  4      NAS Port type : 5
26w2d12h :      Attribute  4      length  4      NAS IP Address : [redacted]
26w2d12h :      Attribute  2      length 16      Password : *****
26w2d12h : RADIUS: Initial Transmit id 29, code 1, len 78, Access-Request
26w2d12h : RADIUS: Calling Station ID = [redacted]
26w2d12h : RADIUS: Try server [redacted] for id 29
```

Appendix C: Maintenance Procedures

Active Directory

These instructions are for adding or removing user accounts from group access to manage Force 10 switches.

- Open the Active Directory Users and Computers application
- Click Action from the menu-bar and click Find
- Keep the default "Find:" field of Users, Contacts, Groups, but change the "From:" field to Entire Directory
- In the Name field of the Users, Contacts, Groups tab type the group name Network-Switch and click the Find Now button
- The Network-Switch group will appear in "Search results:" box. Double-click the Network-Switch group
- Click on the Members tab of the Network-Switch Properties window
- To add a member(s) click the Add button and type the name(s) of the user(s) to search for in the "Enter the object names to select:" field
- To remove members, highlight a member in the list and click the Remove button. Only one member can be removed at a time

Network Policy Server (NPS)

These instructions are for adding a new Force 10 switch as a RADIUS client. Replacement switches do not need a new RADIUS client.

- Connect to the RADIUS server ([redacted]
- Launch the Network Policy Server (NPS) role application
- Expand the RADIUS Clients and Servers folder in the left hand pane of the application
- Right click RADIUS Clients and click new – a New RADIUS Client dialog box opens
- In the Settings tab, fill in the Friendly name field. Force 10 switches naming convention must always begin with the SW- prefix
- Fill in the IP Address of the new switch in the Address (IP or DNS) field
- Type the company shared secret password in the two appropriate fields to confirm
- Make sure that Enable this RADIUS client has a check mark and click OK

Force 10

These instructions detail adding only the RADIUS authentication configuration on a new Force 10 switch. Instructions to configure an entire new switch have been updated on the company documentation site.

- Connect to the switch via console cable and log in with the local administrator account
- Enter the configuration terminal command to edit the switch configuration
- Enter the radius-server host [redacted] key *(shared secret)* command using the company's shared secret password
- Enter the ip radius source-interface GigabitEthernet ?/? command filling in the ?/? with the interface number that has the RADIUS client IP Address
- Enter the aaa authentication login adgroup radius local command to set up the method list
- Enter the line vty 0 9 command to enter line configuration mode to edit the VTY line configurations
- Enter the login authentication adgroup command to configure the lines to use the adgroup configured in the method list
- Enter the privilege level 15 command to allow proper administrative permission to adgroup users that connect to the lines
- Enter the end command to return exit all configuration modes
- Enter the write memory command to save the new switch configuration

References

Bhatnagar, K. (2002). *Cisco Security.* Boston, MA: Course Technology / Cengage Learning.

Cisco Systems, Inc. (2006, January 19). *How Does RADIUS Work?* Retrieved from http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Microsoft TechNet Library. (2008, October 21). *NPS Shared Secrets*. Retrieved from Microsoft TechNet Library: https://technet.microsoft.com/en-us/library/dd197468%28v=ws.10%29.aspx

Microsoft TechNet Library. (2009, February 17). *Understanding Groups*. Retrieved from Microsoft TechNet Library: https://technet.microsoft.com/en-us/library/dd861330.aspx

Panek, W. (2011). *MCTS : Windows Server 2008 R2 Complete Study Guide (Exams 70-640, 70-642 And 70-643).* Hoboken, NJ: Sybex.

Santos, O., & Stuppi, J. (2015). *CCNA Security 210-260 Official Cert Guide.* Indianapolis, IN, 46240: Cisco Press.

Smart Brain Training Solutions. (2014). *Active Directory Fast Start : A Quick Start Guide for Active Directory.* Seattle, WA: RP Media.