**Funkcjonalności systemu zarządzania hasłami i dostępem uprzywilejowanym (System PAM).**

**Kluczowe funkcjonalności:**

1. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych

2. System działa na pojedynczej bazie danych

3. System posiada wbudowane skrypty, które pozwalają na: backup bazy danych, odtworzenie bazy danych, zmianę bazy danych

4. System pozwala na podłączenie certyfikatu w formie .PFX(PKSC12)

5. Dostęp do systemu dla użytkownika jest zapewniony za pośrednictwem konsoli webowej

6. System działa bezagentowo

7. Logowanie z dowolnej przeglądarki wspierającej protokół HTML5 dla sesji Windows RDP, VNC, SQL, SSH i Telnet bez konieczności instalacji agentów.

8. System umożliwia połączenie z działającymi u Zamawiającego oprogramowaniami: ADSelfService, DesktopCentral, ServiceDesk Plus firmy ManageEngine

9. System umożliwia użycie SAML’a 2.0 dla SSO

10. System umożliwia dwupoziomową autentykację, za pomocą Phone Factor, RSA SecurID, Google Aunthenticator, Microsoft Aunthenticator, Okta Verify, Radius Authenticator, Duo Security, YubiKey, Zoho OneAuth Authenticator, Oracle Authenticator oraz wysyłanie jednorazowego hasła na wybraną skrzynkę pocztową.

**Możliwości oprogramowania:**

1. System posiada wbudowaną opcję przeglądania głównych informacji w postaci dashboard’u.

2. System posiada funkcjonalność centralnego repozytorium haseł przechowywanych w zabezpieczony sposób

3. System posiada funkcje definiowania właścicieli haseł

4. Domyślnie administrator dodający hasło musi zostać jego właścicielem

5. Właściciel ma możliwość przydzielania następujących poziomów uprawnień: tylko do przeglądu, przegląd i modyfikacja

6. Dostęp do systemu dla użytkownika jest zapewniony za pośrednictwem konsoli webowej

7. System umożliwia zdalny reset haseł dla systemów Windows, domeny Windows, systemów Linux, IBM AIX, HP UNIX, Solaris, Mac OS, MS SQ, MySQL, Oracle DB, Sybase ASE, urządzeń HP ProCurve, Cisco (IOS, CatOS, Pix).

8. Zdalny reset haseł jest możliwy bezagentowo lub za pośrednictwem agenta.

9. Oprogramowanie umożliwia dostęp do tworzenia statycznych i dynamicznych grup oraz ich usuwanie oraz zbiorczą konfigurację.

10. System umożliwia modyfikację atrybutów dla wybranej grupy w środowisku domenowym.

11. System posiada wbudowaną funkcję definiowania polityki haseł.

12. PAM zapewnia integrację z posiadanym przez Zamawiającego systemem zgłoszeń o nazwie Service Desk Plus firmy ManageEngine w celu automatycznej weryfikacji zgłoszeń serwisowych, związanych z uprzywilejowanym dostępem.

13. Oprogramowanie umożliwia export danych grupy do pliku „xlsx” lub w formie zaszyfrowanej w postaci pliku „html”, jak i do Dropboxa, Boxa oraz Amazona S3 dla urządzeń mobilnych.

14. System jest wyposażony w notyfikację w przypadku uruchomienia procedury resetu haseł.

15. Oprogramowanie umożliwia generowanie raportu dla wybranej grupy, a w szczególności: spisu haseł, zgodności polityk, wygasłych haseł

16. Oprogramowanie umożliwia zdalne logowanie

17. Logowanie z dowolnej przeglądarki wspierającej protokół HTML5 dla sesji Windows RDP, VNC, SQL, SSH i Telnet bez konieczności instalacji agentów.

18. Zdalne sesje są tunelowane przez serwer centralny systemu zarządzania hasłami bez konieczności bezpośredniej komunikacji urządzenia użytkownika z urządzeniem docelowym.

19. Zdalne sesje dają administratorowi możliwość śledzenia sesji otwartej przez innego użytkownika, na żywo, tzw. Session shadowing.

20. Zdalne sesje użytkownika mogą być przerwane w dowolnym momencie przez administratora.

21. System umożliwia nagrywanie sesji użytkownika, wraz z możliwością ich eksportu

22. Sesje mogą być usuwane po określonym czasie

23. Sesje oraz wykonany chat podczas sesji mają możliwość wybiórczego usuwania

24. Oprogramowanie umożliwia zarządzanie kluczami SSH dla połączenia z serwerem, w szczególności: tworzenie, usuwanie, importowanie, przypisywanie, odłącznie, zamianę i przeglądanie historii klucza SSH

25. System potrafi generować powiadomienia każdej operacji na haśle w tym możliwość definiowania powiadomień email, możliwość generowania pułapek SNMP lub rejestrów syslog i przesłania ich do systemów SIEM (Security Information and Event Management) oraz możliwość generowania zdarzeń w ramach rejestrów syslog

26. Oprogramowanie umożliwia dodawanie, tworzenie, przypisywanie, skanowanie certyfikatu na podatność/wrażliwość, tworzenie grupy dla certyfikatu, sprawdzanie daty wygaśnięcia domeny, zaznaczenie jako „root”, synchronizacja z CMDB, importowanie klucza, edytowanie certyfikatu, udostępnienie użytkownikom lub grupie użytkowników, oraz usuwanie certyfikatu.

27. System pozwala na łatwe wykrycie certyfikatów za pomocą: adresu IP/pliku/Subnet’u, certyfikatów serwerów email, modułu równoważenia obciążenia (Load Balancer) oraz angetów.

28. System pozwala na dodawanie, usuwanie i zarządzanie próśb przydzieleń certyfikatów nadesłanych przez użytkowników

29. System pozwala na podłączenie certyfikatu w formie .PFX(PKSC12)

30. Oprogramowanie umożliwia certyfikowanie poprzez wystawców: „Let’s Encrypt”, „GoDaddy”, „The SSL Store”

31. System umożliwia integrację z systemem Windows Active Directory (AD), usługami LDAP oraz Azure AD.

32. Oprogramowanie umożliwia logowanie do systemu zarządzania hasłami za pośrednictwem usług katalogowych: Windows Active Directory (AD), usługami LDAP oraz Azure AD

33. System uwzględnia restrykcje uwierzytelniania AD/LDAP/Azure AD podczas logowania.

34. Administrator systemu zarządzania hasłami umożliwia importowanie użytkowników/ grup użytkowników z AD/LDAP/Azure AD do systemu.

35. Oprogramowanie umożliwia automatyczne dodawanie użytkownika do systemu, po utworzeniu go w AD/LDAP/Azure AD.

36. System PAM posiada szereg możliwości dla ustawień własnych systemu, w szczególności:

- Definiowanie polityk haseł, jak: długość hasła, wymuszanie cyfr i ich ilość, wymuszanie znaków specjalnych i ich ilość, zabronione znaki, czy hasło może zawierać login, czy hasło ma się zaczynać literą alfabetu, jak długo może utrzymywać się jedno hasło oraz jak długo nie można użyć ponownie tego samego hasła.

- Tworzenie, definiowanie i przypisywanie ról dla wybranych użytkowników

36. System PAM posiada narzędzia do: wyszukiwania zmian haseł, Rebrand- dostosowywania wyglądu strony, konfiguracji szablonu wyglądu wiadomości email, konfiguracji pluginu resetu hasła, konfiguracji komend SSH

37. System umożliwia dwupoziomową autentykację, za pomocą Phone Factor, RSA SecurID, Google Aunthenticator, Microsoft Aunthenticator, Okta Verify, Radius Authenticator, Duo Security, YubiKey oraz wysyłanie jednorazowego hasła na wybraną skrzynkę pocztową realizowaną poprzez konfigurację SSO dzięki użyciu protokołu SAML w wersji 2.0, oraz za pomocą smart card’ów, PKI oraz certyfikatów.

38. Administrator / administrator haseł może mieć status ‘super administratora’ po przydzieleniu przez innego administratora (statusu tego nie można przydzielić samemu sobie) – ‘super administrator’ posiada uprawnienia zarządzania wszystkimi zasobami dodanymi do systemu zarządzania hasłami przez wszystkich administratorów/użytkowników.

39. System umożliwia ustawienia, w szczególności:

a) System pozwala na dwa typy wyświetlania logów: „DEBUG” – pokazuje wszystkie przypisy wiadomości – oraz „INFO” – wyświetla tylko informacje o wiadomościach

b) System zapewnia wiele opcji do bezpiecznego dostępu offline, oraz określone opcje eksportu dla użytkowników

c) System zapewnia konfigurację skrzynki pocztowej, dla powiadomień użytkowników

d) System umożliwia konfigurację serwera proxy

40. PAM zapewnia backup’owanie bazy danych, wraz z możliwością ustawień powtarzalności, godziny kiedy ma być wykonany backup i ile backup’ów ma być trzymanych na przeznaczonym do tego folderze. Pozwala też na odtworzenie bazy danych oraz zmianę bazy danych

41. System umożliwia definiowanie dopuszczalnych IP oraz tych, które mają być blokowane

42. System ma moduł API (Application Programming Interface), którego wykorzystanie zapewnia programowalne wykonanie zapytań przez aplikacje lub skryptu o pozyskanie hasła z systemu zarządzania hasłami, aby nawiązać połączenie z inną aplikacją czy bazą danych.

43. PAM zapisuje bazę danych haseł w wybranym serwerze i szyfruje je za pomocą AES-256

44. PAM możliwość szyfrowania za pomocą Safenet HSM, gdzie zaszyfrowany klucz znajduje się na oddzielnym urządzeniu

45. System umożliwia powiadomienie wszystkich użytkowników za pomocą wiadomości email, dla osób nieposiadających konta PAM lub alertu online

46. System umożliwia tworzenie harmonogramów zadań lub użycie pre-definiowanych harmonogramów

47. System zapewnia podgląd próśb użytkowników o dostęp haseł

48. PAM zapewnia integrację: Chmurową, z platformami CI/CD, Jenkins, Ansible, Chef, Puppet

49. PAM zapewnia integrację z innymi programami ManageEngine tj.: ServiceDesk Plus, ADSelfService Plus, Analyticks Plus, Eventlog Analyzer, Log360 UEBA, ADManager Plus

50. PAM zapewnia możliwość instalacji agenta, dla: Windows Agent w wersji 32- lub 64-bitowej, Windows Domain Agent w wersji 32- lub 64-bitowej, Linux Agent w wersji 32- lub 64-bitowej

51. Oprogramowanie umożliwia audyt operacji, jak:

1. Audyt zasobów – wszystkie operacje związane z zasobami, grupami zasobów, kontami, hasłami, udziałami i politykami

2. Audyt użytkowników – wszystkie operacje wykonane w systemie zarządzania hasłami przez jego użytkowników

3. Audyt zadań – rejestr zdefiniowanych zadań

4. Odtwarzanie nagranych sesji

5. Audyt nagranych połączeń

6. Audyt aktywnych sesji

7. Audyt przypisanych kluczy

52. System posiada możliwość funkcjonowania w trybie wysokiej dostępności ( High Availability) w tym:

1. Wszyscy użytkownicy rejestrują się do serwera głównego

2. Druga instancja serwera funkcjonuje jako serwer typu Secondary / Standby

3. Synchronizacja danych między serwerem głównym a Secondary / Standby następuje w bezpieczny sposób

4. W dowolnym momencie czasu, w sytuacji awarii serwera głównego, serwer Secondary/ Standby przejmuje wszystkie funkcje serwera głównego

53. System posiada możliwość włączenia dodatkowej kontroli dostępu do zasobów oraz ograniczenia możliwości łączenia zdalnej sesji spoza systemu. W tym:

1. Możliwość włączenia i wyłączenia zatwierdzania dostępu

2. Możliwość wyłączenia podglądu haseł

3. Możliwość automatycznego resetowania haseł po każdej sesji

4. Możliwość automatycznego przydzielania dostępu

54. System posiada możliwość natychmiastowego wyłączenia w przypadku sytuacji awaryjnej, w tym wyłączenia wszelkiej komunikacji z agentami oraz po API

55. System posiada zdefiniowane raporty oraz zabezpieczenia wspierające zgodność z RODO, w tym:

1. Kontrola IP, z jakich następuje połączenie z aplikacją, zarówno sesji webowej jak i API

2. Dostęp, aktywność oraz raport użytkowników, nieprzydzielonych do żadnej grupy

3. Podsumowanie dostępu haseł, działań i naruszeń zasad

4. Przynależności, tworzenia i dokładny obieg kluczy SSH wykonanych w PAM

5. System posiada możliwość wyłączenia podglądu danych osobowych

6. System zapewnia możliwość zaszyfrowanego eksportu danych

7. System pozwala „ponawiać” okresowe resetowanie hasła grup zasobów, konfigurując ustawienia ponownych prób resetowania hasła, które obejmują ich liczbę i interwał.

8. System umożliwia organizacjom klienckim tworzenie własnych konfiguracji SAML.

9. System pozwala zaimplementować ograniczenia kont domeny dla zasobów docelowych, tj. użytkownikom kont domeny Windows można przyznać dostęp tylko do określonych zasobów, do których faktycznie chcą uzyskać dostęp, zamiast do wszystkich współdzielonych z nimi zasobów.

10. System jest dostępny w języku portugalskim.

11. System posiada typ zasobu – Cisco Nexus OS.

12. System posiada interfejsy RESTAPI: Fetch User GroupID, Configure Remote Password Reset for Linux resources, Share Resource i Share account to User Group.

13. System pozwala przeglądać wszystkie certyfikaty skojarzone z określonym agentem.

14. System pozwala wykrywać certyfikaty wydane przez określony „Microsoft Certificate Authoritory” wprowadzając podczas wykrywania nazwę MSCA w odpowiednim polu tekstowym. Dostępne dla PAM na serwerach z systemem Windows.

15. System pozwala na dodanie nazwy Wildcard w polu SAN podczas tworzenia CSR lub certyfikatu z podpisem własnym. Dzięki certyfikatom Wildcard można zabezpieczyć nieograniczoną liczbę subdomen dla zarejestrowanej domeny bazowej.

16. System obsługuje zaplanowane zadania wykrywania SSL i MS Certificate Store Discovery za pomocą agenta KMP.

17. System pozwala na dostosowanie liczby dni na automatyczne odnawianie certyfikatów przed ich wygaśnięciem.

18. System pozwala podczas podpisywania CSR certyfikatów SSL za pomocą agenta KMP na określenie wartości limitu czasu agenta w sekundach.

19. System pozwala użytkownikom wybierać określone certyfikaty lub grupy certyfikatów podczas generowania typu harmonogramu „SSL Certificates Report”.

20. System umożliwia użytkownikom dodawanie i edytowanie listy wdrożonych serwerów. Nowo dodane serwery zostaną zmapowane z najnowszą wersją certyfikatu w repozytorium certyfikatów.

21. System obsługuje wykrywanie zakresów adresów IP na potrzeby wykrywania magazynu certyfikatów MS przy użyciu usługi PAM z kontem administratora domeny, co pozwala administratorom wykrywać certyfikaty w sieciach.

22. System obsługuje wykrywanie certyfikatów „Load Balancer” dla urządzeń Citrix. Począwszy od kompilacji 11300, system obsługuje również zaplanowane wykrywanie certyfikatów z systemów równoważnia obciążenia opartych na systemie Linux, takich jak BIG-IP F5, Nginx i Citrix.

23. System pozwala użytkownikom na ominięcie ustawień serwera proxy podczas wykrywania certyfikatów SSL.

24. System pozwala na automatyczne wdrożenie certyfikatów MSCA/self-signed, jeśli poświadczenia użytkownika są dostępne.

25. System umożliwia użytkownikom wybranie „Certificate type” [CER/DER/P7B/CRT] i „Keystore type” [JKS/PKCS/PEM/KEY] podczas wdrażania certyfikatów na komputerach z systemem Windows i Linux oraz podczas eksportowania certyfikatów.

26. System pozwala na odnowienie certyfikatów typu MSCA z nowym kluczem prywatnym, jeśli klucz prywatny nie jest jeszcze dostępny.

27. System obsługuje ClouDNS, aby zakończyć weryfikację kontroli domeny podczas uzyskiwania certyfikatów od publicznych urzędów certyfikacji.

28. System obsługuje magazyny kluczy PKCS12 z szyfrowaniem AES256 podczas dodawania magazynów kluczy certyfikatów.

29. System pozwala użytkownikom wybrać do pięciu szablonów certyfikatów podczas wykrywania certyfikatów lokalnych CA na podstawie agenta.

30. System począwszy od wersji 11300 umożliwia wyszukiwanie w niestandardowych kolumnach certyfikatów SSL i kluczy SSH.

31. System pozwala na dołączenie wielu serwerów dla certyfikatów w powiadomieniach o wygaśnięciu certyfikatu SSL.

32. System umożliwia użytkownikom bezpośrednio importować istniejące certyfikaty ze swojego konta GoDaddy do repozytorium.

33. System posiada możliwość skojarzenia kluczy lokalnie, jeśli zdalne skojarzenie nie powiedzie się dla użytkowników, których dostęp został przerwany.

34. System posiada interfejsy API REST „Get Password Policies” i “Get Resource Types”.

35. System obsługuje wykrywanie certyfikatów SSL ze ścieżek współdzielonych UNC (Uniwersal Naming Convention) dla komputerów z systemem Windows, Linux i Mac OS.

36. System umożliwia wykrywanie certyfikatów SSL z katalogów na zdalnych maszynach, które nie są bezpośrednio dostępne przez PAM – wszystko za pośrednictwem agenta KMP. Opcja ta jest również dostępna podczas zaplanowanego wykrywania certyfikatów.

37. System umożliwia użytkownikom wdrażanie certyfikatów SSL w przeglądarkach dla następujących typów serwerów: Windows, Linux i MacOS.

38. System umożliwia ograniczenie użytkownikom bezpośredniego dostępu do użytkowników root poprzez wyłączenie logowania użytkownika root. Włączenie tej opcji podnosi poziom logowania użytkownika z użytkownika innego niż root do użytkownika root i kojarzy klucze ze wszystkimi innymi użytkownikami na serwerze.

39. System posiada interfejs API REST „Deploy Certificate”.

40. System umożliwia ponowne odnajdywanie certyfikatów SSL z tego samego źródła przy użyciu danych serwera wprowadzonych podczas poprzedniej operacji wykrywania.

41. System integruje się z Buypass Go SSL i ZeroSSL – dwoma urzędami certyfikacji, które korzystają z protokołu Automatic Certificate Management Environment (ACME) w celu dostarczania bezpłatnych, bezpiecznych certyfikatów SSL. Użytkownicy mogą żądać, pozyskiwać, tworzyć, wdrażać, odnawiać i automatyzować kompleksowe zarządzanie certyfikatami SSL/TLS wydanymi przez Buypass Go SSL i ZeroSSL.

42. System integruje się z ManageEngine Mobile Device manager (MDM) Plus. Integracja ta wykorzystuje interfejsy API ManageEngine MDM do wykrywania I wdrażania certyfikatów SSL na i z urządzeń mobilnych zarządzanych przez serwer MDM. System umożliwia następnie filtrowanie wykrytych certyfikatów SSL na podstawie typu systemu operacyjnego, takiego jak: Android, Windows, Chrome OS, Mac OS i Apple tvOS. Możliwe jest również eksportowanie raportów certyfikatów MDM zarządzanych w repozytorium systemu w wybranym okresie. Można też zaplanować okresowe generowanie raportów certyfikatów MDM.

43. System umożliwia globalną modyfikację poziomu dostępu współdzielonych certyfikatów.

44. System posiada interfejsy API REST: 'Share SSL Certificate to User', 'Share SSL Certificate to User Group', 'Share SSL Certificate Group to User', 'Share SSL Certificate Group to User Group', 'Revoke SSL Certificate from User', 'Revoke SSL Certificate from User Group', 'Revoke SSL Certificate Group from User', 'Revoke SSL Certificate Group from User Group', 'Create SSL Certificate Group', 'Delete SSL Certificate Group', 'Edit SSL Certificate Group', 'Generate an Agent Install Key'.

56. System posiada dwa nowe agenty: agent C# dla Windows/Windows Domain i agent Go dla Linuxa. Umożliwia to użytkownikom ograniczenie kont użytkowników dodawanych za

pośrednictwem agentów (tylko nowi agency) podczas wykrywania kont, przy użyciu wzorców regularnych.

57. System posiada security framework w najnowszej wersji, aby ograniczyć występowanie luk w zabezpieczeniach i poprawić ogólne bezpieczeństwo.

58. System posiada serwer PostgreSQL w wersji 10.18.

59. System posiada serwer Apache Tomcat wwersji 9.0.54.

60. System posiada narzędzie Rubyrep w wersji 2.0.1.

61. System przeniesiono na platformę OpenJDK w wersji 1.8.0\_252.

62. System obsługuje sterownik Microsoft JDBC w wersji 8.4.1 oprócz sterownika JTDS JDBC do łączenia z serwerem SQL.

63. System obsługuje weryfikacje integralności poprawki, która odtąd będzie wymagać importowania certyfikatu SSL za każdym razem, gdy produkt zostanie zaktualizowany przy pomocy pliku PPM.

64. System pozwala użytkownikom na dodawanie kont za pośrednictwem agenta domeny Windows, gdy filtr kont jest dostarczany przy użyciu wzorców regularnych.

65. System pozwala administratorom ograniczyć użytkownikowi możliwość konfigurowania hasła szyfrowania dla jego haseł osobistych, użytkownik może skonfigurować „klucz szyfrowania” dla swoich haseł osobistych na karcie „Osobiste”. Mogą również swobodnie wybierać między przechowywaniem lub nie przechowywaniem klucza szyfrowania, a korzystaniem z klucza szyfrowania aplikacji.

66. System posiada możliwość przeniesienia użytkowników RESTAPI do klienta. Obsługiwane organizacje klienckie z pełnym dostępem mogą zarządzać zasobami i kontami.

67. System posiada pojedynczy harmonogram „Kontroli czyszczenia i podsumowania”, który został połączony z sześciu harmonogramów audytu: „Harmonogram czyszczenia audytu zasobów”, „Harmonogram podsumowania audytu zasobów”, „Harmonogram czyszczenia UserAudit”, „Harmonogram czyszczenia UserAudit”, „Harmonogram czyszczenia TaskAudit” i „Harmonogram podsumowania audytu TaskAudit”.

68. System posiada „Harmonogram aktywności wykresu tablicy rozdzielczej”.

69. System pozwala na usunięcie starych rekordów - na podstawie daty z określeniem odpowiedniego typu operacji. Dla przykładu - system pozwoli na usunięcie danych audytowych starszych niż 365 dni, w których wykonano akcję restart hasła.

70. System pozwala administratorom MSP replikować ustawienia typu operacji inspekcji i ustawienia czyszczenia inspekcji we wszystkich organizacjach klienckich.

71. System posiada nową wersję API REST. Nowa wersja zawiera kilka nowych interfejsów dla następujących operacji: powiązanie zasobu z grupą zasobów, odpięcie zasobu od grupy zasobów, pobranie grup zasobów powiązanych z zasobem, usuwanie grup zasobów i pobieranie identyfikatora grup zasobów.

72. System posiada możliwość wprowadzenia nazwy hosta użytkownika interfejsu API bez uwzględnienia wielkości liter.

73. System posiada Apache Log4j w wersji 2.17.2.

74. System umożliwia konfigurację harmonogramów automatycznego wykrywania kont uprzywilejowanych podczas wykrywania systemu: Linux, urządzeń sieciowych oraz VWware.

75. System posiada możliwość konfiguracji SAML w układzie High Availability.

76. System posiada Dropbox SDK w wersji 5.0.0

77. System posiada możliwość konfiguracji wiadomości powitalnej po rozpoczęci sesji zdalnej.

78. System wspiera SAML Single Logout – który automatycznie kończy wszystkie powiązane sesje nawiązane za pomocą SAML SSO w chwili wylogowania użytkownika z interfejsu aplikacji.

79. Funkcja rotowania kluczem szyfrującym PAM jest dostępna dla wszystkich edycji produktu.

80. Oprogramowanie PAM pozwala na zdalne łączenie się bezpośrednio do aplikacji w systemie Windows przy pomocy RemoteApp

81. System umożliwia podnoszenie uprawnień dla użytkowników przy pomocy funkcji Just-in-time privilege elevation dla rozszerzeń plików CMD, EXE, MSI, MSC oraz BAT. Dzięki czemu użytkownik końcowy jest w stanie uruchomić wyszczególnione aplikację z uprawnieniami administratora.

82. System posiada możliwość integracji z systemem ticketowym BMC Helix Remedyforce

83. System posiada możliwość integracji z rozwiązaniem Entrust nShield Hardware Security Module (HSM)

84. System posiada natywnego klienta (PAM Remote Connect), który ułatwia nawiązanie bezpośredniego zdalnego dostępu do zasobów docelowych opartych na systemie Windows i SSH, bez potrzeby korzystania z wielu zdalnych klientów lub przeglądarek internetowych. PAM Remote Connect wykorzystuje zdolność natywnego klienta pulpitu zdalnego systemu Windows i klienta SSH Putty do uruchamiania połączeń opartych na protokole RDP i SSH ze scentralizowanej konsoli.

85. System posiada integrację z rozwiązaniem Kubernetes

86. System posiada integrację z rozwiązaniem SIEM Microsoft Sentinel

87. System posiada możliwość weryfikacji komend wpisywanych przez użytkowników podczas połączenia SSH oraz blokowanie wybranych zachowań.

88. System posiada możliwość samoobsługowego podniesienia uprawnień dla systemu Linux

89. System posiada funkcję HTTPS Gateway, która pozwala użytkownikom uruchamiać uprzywilejowane połączenia HTTPS z wewnętrznymi i zewnętrznymi stronami internetowymi, które nie są bezpośrednio dostępne z urządzeń końcowych użytkowników.

90. System posiada możliwość skonfigurowania Zero Trust Approach, dzięki któremu możemy na podstawie wskaźnika zaufania użytkownika ograniczyć mu funkcję aplikacji.

91. System umożliwia regularne sprawdzanie stanu synchronizacji certyfikatów SSL wdrożonych bezpośrednio na wielu serwerach.

92. System zawiera teraz kategorię „Narzędzia”, która umożliwia użytkownikom niezależne przeprowadzanie konwersji certyfikatów, parsowanie SSL/CSR i skanowanie pod kątem luk w zabezpieczeniach bez dodawania certyfikatów do repozytorium PAM

93. System posiada integrację z AWS Certificate Manager - zaufanym urzędem certyfikacji i menedżerem certyfikatów.

94. System pozwala na zarządzanie całym cyklem życia certyfikatów MSCA

95. System posiada integrację z Azure Key Vault - usługą zarządzania certyfikatami SSL oferowaną przez firmę Microsoft.

96. System posiada integrację z Sectigo Certificate Manager - platformą zarządzania PKI stworzoną do zarządzania certyfikatami SSL/TLS, kluczami SSH i innymi tożsamościami cyfrowymi.

97. System posiada możliwość wdrażania certyfikatów w systemie Citrix ADC Load Balancer

98. System pozwala na obsługę wielu domen LDAP

99. System posiada interfejsy API REST: 'Fetch All Users', 'Fetch All User Groups', 'Bulk Share Resource Groups to Users or User Groups', 'Bulk Share Resources to Users or User Groups', 'Bulk Share Accounts to Users or User Groups'

100. System posiada typ zasobu – RabbitMQ.

101. System posiada możliwość importowania użytkowników, zasobów, organizacji i haseł z plików Excel tak jak .xls, .xlsx

102. System pozwala na logowanie do aplikacji przy pomocy kodów QR

103. System posiada integrację z Zoho Flow

104. System posiada dashboard dotyczący bezpieczeństwa środowiska serwera oraz aplikacji