სსე სერვერებისა და საცავის პროექტი

აქტიური / აქტიური HCI

შეთავაზების მოთხოვნა

ზოგადი ტექნიკური მოთხოვნები

1. ტენდერის სპეციფიკაცია HCI პლატფორმისთვის

შემოთავაზებული ორი HCI (ჰიპერ-კონვერგენტული) სისტემა უნდა შედგებოდეს არანაკლებ ოთხი გამოთვლითი კვანძისგან, თითოეული უნდა მოიცავდეს არანაკლებ ერთ საცავ მასივსა და არანაკლებ ორ მაღალი გამტარუნარიანობის მქონე „ Ethernet “კომუტატორს.

2. გამოთვლითი კვანძები

ფორმ ფაქტორი: არაუმეტეს 1U Rack სამონტაჟო. უნდა იყოს უზრუნველყოფილი სასერვერო კარადაში განთავსებისათვის საჭირო კომპლექტით.

პროცესორი: არანაკლებ ორი უახლესი თაობის 24 ბირთვი, არანაკლებ 2.1 GHz საბაზო საათის სიჩქარის პროცესორი.

მეხსიერება: არანაკლებ 1,536 GB DDR4 რეგისტრირებული DIMM (RDIMM, რომელიც მუშაობს 3200 MT/s. მასშტაბირებადი 2.0 ტბ-მდე DDR4 რეგისტრირებული DIMM (RDIMM)-ის გამოყენებით, რომელიც მუშაობს 3200 MT/s სიჩქარით. სერვერს უნდა ჰქონდეს 8.0 ტბ-მდე მხარდაჭერა DDR4 დატვირთვის შემცირებული DIMM (LRDIMM) გამოყენებით, რომელიც მუშაობს 3200 MT/s-ზე.

- ერთ კლასტერს ჯამურად უნდა ჰქონდეს არანაკლებ ექვსი ტერაბიტი მეხსიერება, რომელიც სამომავლოდ უნდა იყოს გაზრდადი აპარატურული ცვლილების გარეშე.

მაკონტროლებელი: სერვერმა უნდა უზრუნველყოს არანაკლებ ორი M.2 დისკი OS Boot მოწყობილობა RAID 1 აპარატურით. (ESXi ოპერაციული სისტემის ჩასატვირთად)

ქსელი: არანაკლებ 2 x 10/25Gb ორ-პორტიანი SFP28 Ethernet ადაპტერი. სერვერს უნდა ჰქონდეს 100 გიგაბიტიანი პორტის ადაპტერების მხარდაჭერა.

ინტერფეისები: USB 3.0 მხარდაჭერა სულ 5-მდე: არანაკლებ 1 წინა, არანაკლებ 2 შიდა, არანაკლებ 2 უკანა. სერვერს უნდა ჰქონდეს სერიული ინტერფეისის მხარდაჭერა.

PCIe: სერვერს უნდა ჰქონდეს არანაკლებ სამი PCI-ექსპრეს 3.0 სლოტის მხარდაჭერა, არანაკლებ ორი x16 PCIe სლოტის მხარდაჭერა.

ელექტრომომარაგება: არანაკლებ ორი 800W შესაერთებელი სარეზერვო დაბალი ჰალოგენური კვების წყაროსთვის, არანაკლებ 94% ეფექტურობით.

გაგრილება: სარეზერვო ცხელი ჩართვის მაღალეფექტური ვენტილატორები.

ინდუსტრიის სტანდარტების შესაბამისობა: სერვერმა უნდა უზრუნველყოს ACPI 6.3 შესაბამისი; PCIe 4.0 თავსებადი; WOL მხარდაჭერა; Microsoft® ლოგოს სერთიფიკატები; PXE მხარდაჭერა; USB 3.0 თავსებადი; SMBIOS 3.2; Redfish API; IPMI 2.0; უსაფრხო ციფრული 4.0; TPM 1.2 და 2.0 მხარდაჭერა; დაშიფვრის გაფართოებული სტანდარტი (AES); მონაცემთა სამმაგი დაშიფვრის სტანდარტი (3DES); SNMP v3; TLS 1.2; DMTF სისტემების მართვის არქიტექტურა სერვერის აპარატურის ბრძანების ხაზისთვის (SMASH CLP); მოქმედი დირექტორია v1.0; ASHRAE A3/A4; UEFI (ერთიანი გაფართოებადი Firmware ინტერფეისის ფორუმი) 2.6;

სისტემის უსაფრთხოება: სერვერმა უნდა უზრუნველყოს UEFI Secure Boot და Secure Start მხარდაჭერა; ნდობის უცვლელი სილიკონის ფესვი; FIPS 140-2 ვალიდაცია; საერთო კრიტერიუმების სერტიფიცირება; კონფიგურირებადი PCI DSS შესაბამისობისთვის; დაშიფვრის გაფართოებული სტანდარტი (AES) და მონაცემთა სამმაგი დაშიფვრის სტანდარტი (3DES) ბრაუზერზე; კომერციული ეროვნული უსაფრთხოების ალგორითმები (CNSA); სერვერის მართვის პროგრამული უზრუნველყოფის უსაფრთხოების რეჟიმები; დეტალური კონტროლი სერვერის მართვის პროგრამულ ინტერფეისებზე; სმარტ ბარათი (PIV/CAC) და Kerberos-ზე დაფუძნებული 2-ფაქტორიანი ავთენტიფიკაცია; შეუფერხებელი განახლებები - კომპონენტები ციფრულად ხელმოწერილი და დამოწმებული; უსაფრთხო აღდგენა - კრიტიკული პროგრამული უზრუნველყოფის აღდგენა ცნობილ კარგ მდგომარეობაში კომპრომეტირებული FW-ის გამოვლენისას; პროგრამული უზრუნველყოფის დაბრუნების შესაძლებლობა; NAND-ის უსაფრთხო წაშლა; TPM (სანდო პლატფორმის მოდული);

ოპერაციული სისტემა: სერვერმა უნდა უზრუნველყოს უახლესი ოპერაციული სისტემები და ვირტუალიზაციის პროგრამული უზრუნველყოფა - Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise სერვერი (SLES); VMware.

ჩაშენებული დისტანციური მართვა და პროგრამული უზრუნველყოფის უსაფრთხოება:

- სისტემის დისტანციურმა მართვამ უნდა უზუნველყოს ბრაუზერზე დაფუძნებული გრაფიკული დისტანციური კონსოლი ვირტუალური ჩართვის ღილაკთან ერთად, დისტანციური ჩატვირთვა USB/CD/DVD დისკის გამოყენებით. მას უნდა შეეძლოს დისტანციური კლიენტიდან პროგრამული უზრუნველყოფის და პატჩების განახლება მედიის/სურათის/საქაღალდის გამოყენებით და უნდა ჰქონდეს მულტიფაქტორიანი ავთენტიფიკაციის მხარდაჭერა.
- სერვერს უნდა ჰქონდეს სპეციალური 1 გბ/წმ დისტანციური მართვის პორტი.
- სერვერს უნდა ჰქონდეს შესაბამისი საცავი, რომელიც გამოყენებული იქნება firmware-ის, დრაივერებისა და პროგრამული კომპონენტების შენახვისთვის. კომპონენტების ორგანიზება შესაძლებელია კომპლექტების დასაყენებლად და მათი გამოყენება შესაძლებელია გაუმართავი პროგრამული უზრუნველყოფის აღდგენა/გასწორებისთვის.
- სერვერმა უნდა უზრუნველყოს აგენტის გარეშე მართვა დისტანციური მართვის პორტის გამოყენებით.
- სერვერმა უნდა უზრუნველყოს სერვერის აპარატურისა და სისტემის კონფიგურაციის ცვლილებების მონიტორინგი და ჩაწერა. მისი დახმარებით შესაძლებელი უნდა იყოს პრობლემების დიაგნოსტირება და სწრაფი გადაწყვეტის მიწოდება სისტემის გაუმართაობის დროს.
- ხელმისაწვდომი უნდა იყოს სერვერზე დისტანციური წვდომის პროგრამები Android ან Apple IOS-ზე დაფუძნებული პოპულარული ხელის მოწყობილობების გამოყენებით.
- დისტანციური კონსოლის გაზიარება ერთდროულად 6-მდე მომხმარებლის ოპერაციული სისტემის მუშაობის დაწყებამდე და მუშაობის დროს. Microsoft Terminal Services Integration, 128-bit SSL დაშიფვრა და Secure Shell Version 2 მხარდაჭერა. უნდა უზრუნველყოს AES და 3DES მხარდაჭერა ბრაუზერზე. უნდა უზრუნველყოს დისტანციური პროგრამული უზრუნველყოფის განახლების ფუნქცია. უნდა უზრუნველყოს Java უფასო გრაფიკული დისტანციური კონსოლის მხარდაჭერა.
- მხარდაჭერილი უნდა იყოს მრავალი სერვერის მართვა - Group Power Control-ის მეშვეობით; ჯგუფური სიმძლავრის დაფარვა; ჯგუფური პროგრამული უზრუნველყოფის განახლება; ჯგუფის კონფიგურაცია; ჯგუფის ვირტუალური მედია და დაშიფრული ვირტუალური მედია; ჯგუფური ლიცენზიის გააქტიურება.
- უნდა ჰქონდეს RESTful API ინტეგრაციის მხარდაჭერა.
- სისტემამ უნდა უზრუნველყოს ჩაშენებული დისტანციური მხარდაჭერა, რათა გადასცეს ტექნიკის მოვლენები პირდაპირ OEM-ზე ან ავტორიზებულ პარტნიორზე სახლის ავტომატური ტელეფონის მხარდაჭერისთვის.

- სერვერს უნდა ჰქონდეს უსაფრთხოების დაფა: რომელიც აჩვენებს უსაფრთხოების მნიშვნელოვანი ფუნქციების სტატუსს, სისტემის უსაფრთხოების საერთო სტატუსსა და უსაფრთხოების მდგომარეობისა და სერვერის კონფიგურაციის დაბლოკვის ფუნქციების მიმდინარე კონფიგურაციას.
- შესაძლებელი უნდა იყოს ერთი ღილაკით უსაფრთხო წაშლა, რომელიც შექმნილია სერვერების ექსპლუატაციის შეწყვეტისა და გადაყენებისთვის.
- უნდა გააჩნდეს - მრჩეველი სამუშაო დატვირთვის შესახებ - სერვერის მუშაობის გასაუმჯობესებლად.

3. <u>საცავი მასივი</u>

შემოთავაზებული საცავის სისტემა უნდა იყოს მხოლოდ All Flash - NVMe მასივი და დაფუძნებული უნდა იყოს უახლესი თაობის PCI Gen4 ტექნოლოგიაზე

შემოთავაზებული საცავი უნდა იყოს ფლაგმანი All NVMe - Flash მასივი ორგანიზაციისგან და მკაფიოდ იყოს აღნიშნული მათ ვებსაიტზე.

ოპერაციული სისტემა და კლასტერული მხარდაჭერა:
საცავის მასივი მხარს უნდა უჭერდეს ინდუსტრიის მოწინავე ოპერაციული სისტემის პლატფორმებს და კლასტერულ მართვას, მათ შორის Windows Server 2016 & 2019, VMware 6.x & 7.x, Linux და UNIX ოპერაციული სისტემას.

ტევადობა და მასშტაბურობა:

- მეხსიერების მასივი უნდა იყოს შემოთავაზებული არანაკლებ 32TB გამოსაყენებელი სიმძლავრით, არანაკლებ x24, 1.92TB დისკების გამოყენებით.
- შემოთავაზებული საცავის მასივი უნდა იყოს მოქნილი როგორც ვერტიკალური მასშტაბის, ასევე ჰორიზონტალური მასშტაბის შემთხვევაში მასივის ჩაშენებული პროგრამული უზრუნველყოფის მხარდაჭერით კლასტერული ტექნოლოგიის გამოყენებით.
- შემოთავაზებული საცავის მასივი უნდა იყოს მასშტაბირებადი არანაკლებ 24 NVMe Flash დისკზე მოცემული კონტროლერის წყვილის შასის ფარგლებში და მომავალში შესაძლებელი იყოს 72 NVMe დისკამდე, დისკის დამატებითი შიგთავსის გამოყენებისას გაფართოების გარემოში.
- ჰორიზონტალური მასშტაბის ტექნოლოგია უნდა სცილდებოდეს ფედერაციულ ტექნოლოგიას, სადაც მას უნდა შეეძლოს მოცულობის ზოლის გადატანა ყველა მასშტაბური შენახვის კონტროლერზე.

ქეში:

- შემოთავაზებული საცავის მასივი უნდა იყოს მიწოდებული არანაკლებ 128 გბ ქეშით/მეხსიერებით თითო კონტროლერზე წაკითხვისა და ჩაწერის ოპერაციებისთვის.
- ჩაწერის ოპერაციები მთლიანად დაცული უნდა იყოს და არ უნდა მოხდეს მონაცემთა დაკარგვა ელექტროენერგიის გამორთვის შემთხვევაში. ეს მექანიზმი არ უნდა იყოს დამოკიდებული ბატარეებზე.

მასპინძელი პორტები:

- შემოთავაზებული საცავის მასივი მიწოდებული უნდა იყოს არანაკლებ ორმაგი კონტროლერებით და არანაკლებ 8 x 1 გბიტი/წმ IP და არანაკლებ 8 x 10/25 გბ/წმ IP პორტებით. ყველა შემოთავაზებულ ბარათს უნდა შეეძლოს იმუშაოს ხაზის სიჩქარეზე.
- ოპტიმალური მუშაობისთვის – თითოეულ საბოლოო PCI სლოტს უნდა ჰქონდეს PCI Gen4 ან 16 გბ/წმ სიჩქარის არანაკლებ 8 ზოლი.
- შემოთავაზებულ საცავის მასივს ასევე უნდა ჰქონდეს 10Gbps და 100Gbps IP პორტების მხარდაჭერა.

- გლობალური ცხელი რეზერვირება: შემოთავაზებული საცავის მასივი მხარს უნდა უჭერდეს განაწილებულ გლობალურ ცხელი რეზერვირების დისკებს შემოთავაზებული დისკებისთვის. გლობალური ცხელი რეზერვირება კონფიგურირებული უნდა იყოს ინდუსტრიის პრაქტიკის მიხედვით.

თხელი უზრუნველყოფა და სივრცის ოპტიმიზაცია:

- შემოთავაზებულმა საცავმა უნდა უზრუნველყოს შენახვის ეფექტურობის კრიტიკული მახასიათებლები - შიდა დე-დუბლიკაცია, შეკუმშვა, თხელი უზრუნველყოფა კონტროლერის დონეზე.
- შემოთავაზებულმა საცავმა უნდა უზრუნველყოს როგორც არადუბლირებული, ასევე დუბლირებული მოცულობა ერთდროულად მასივის შიგნით.
- შემოთავაზებულმა საცავმა უნდა უზრუნველყოს როგორც შეუკუმშველი, ასევე შეკუმშული მოცულობები ერთდროულად მასივის შიგნით.
- შემოთავაზებულ საცავს უნდა ჰქონდეს დომენების კატეგორიზაცია სხვადასხვა დატვირთვის აპლიკაციისთვის ეფექტური დედუბლირებისა და შეკუმშვისთვის. მაგალითად - უნდა ჰქონდეს მონაცემთა ბაზის ერთ დომენში ან დაცვის ჯგუფში ჩატვირთვის და ვირტუალური აპლიკაციის სხვა დომენში ან დაცვის ჯგუფში ჩატვირთვის შესაძლებლობა ეფექტური დედუბლირებისა და შეკუმშვისთვის.

მყისიერი ფოტოგრაფირება / დროის მომენტის ამსახველი ასლი: შემოთავაზებული შენახვის მასივი მხარს უნდა უჭერდეს 1000-ზე მეტ სნეპშოტს LUN/მოცულობით. მომწოდებელმა უნდა გამოიყენოს ეფექტური შესრულების ტექნოლოგია, როგორიცაა გადამისამართება ჩაწერაზე ან უკეთესი ვერსია.

ინტეგრაცია - VMware: შემოთავაზებული საცავის მასივი მჭიდროდ უნდა იყოს ინტეგრირებული VMware-თან და დამოწმებული უნდა იყოს VVOL-ისთვის:

- უნდა იყოს სერტიფიცირებული vVol-ზე დაფუძნებული რეპლიკაციისთვის.
- ხელი უნდა შეუწყოს როგორც შეკუმშვას, ასევე დედუბლირებას.
- უნდა ჰქონდეს კვალიფიკაცია, რომ იმუშაოს როგორც ოპტიკურ ბოჭკოვან (FC) არხთან, ასევე ISCSI-თან.
- მხარი დაუჭიროს დაგეგმილ მყისიერ ფოტოგრაფირებას და მომსახურების ხარისხს.
- მხარი დაუჭიროს დაშიფვრას.

წარუმატებლობის და შესრულების ერთი წერტილი:

- შემოთავაზებული საცავის მასივი უნდა იყოს კონფიგურირებული კონფიგურაციის ერთ წერტილში, მასივის კონტროლერის ბარათის, ქეშის მეხსიერების, ვენტილატორის, კვების წყაროს ჩათვლით.
- არ უნდა მოხდეს შესრულების დეგრადაცია ერთი კომპონენტის ან კონტროლერის გაუმართაობის გამო.

დისკის დრაივერის მხარდაჭერა და დაშიფვრა:

- შემოთავაზებული საცავის მასივი მხარს უნდა უჭერდეს NVMe ფლეშ დრაივების სხვადასხვა ტევადობას.
- შემოთავაზებული საცავის მასივი მიწოდებული უნდა იყოს AES-256 XTS FIPS სერტიფიცირებული დაშიფვრით დეტალურ LUN დონეზე დაშიფრული NVMe ფლეშ დრაივების გამოყენების გარეშე.

რეიდის მხარდაჭერა:

- შემოთავაზებული საცავის მასივი უზრუნველყოფილი უნდა იყოს დისკის დრაივერის გაუმართაობისგან ერთდროულად სამი დამცავი საშუალებით.
- დისკის მაქსიმალური სიმძლავრის მისაღწევად - გადაწყვეტილებას უნდა გააჩნდეს მოქნილობა, რათა მოათავსოს ყველა შემოთავაზებული დისკი ერთ დრაივერზე.

ხელმისაწვდომობა:

- შემოთავაზებული საცავის მასივი უნდა უზრუნველყოფდეს საწარმოს ხელმისაწვდომობას არანაკლებ 99,9999% ან უკეთესი მაჩვენებლით და არ უნდა ჰქონდეს გაუმართაობის არც ერთი წერტილი.
- არ უნდა მოხდეს შესრულების დეგრადაცია ერთი კომპონენტის ან კონტროლერის გაუმართაობის გამო.
- არ უნდა მოხდეს შესრულების დეგრადაცია კრიტიკული მხარდაჭერის აქტივობების დროს, როგორიცაა Firmware-ის განახლება, პატჩის განახლება.

4. ქსელი

არქიტექტურა:

- არაუმეტეს 1U ნახევარი სიგანის, თაროზე დასამაგრებელი, შესაფერისი სტანდარტული 19 დიუმიანი თაროებისთვის, საჭირო ორმაგი, გვერდიგვერდ განლაგების სამონტაჟო ნაკრებითა და AC დენის კაბელით. (უნდა იყოს უზრუნველყოფილი სასერვერო კარადაში განთავსებისათვის საჭირო კომპლექტით).
- არანაკლებ 18-პორტიანი 1/10/25 გბ SFP28 და 4-პორტიანი 40/100 გბ QSFP28.
- არანაკლებ 1-პორტიანი კონსოლი/სერიული კაბელით, არანაკლებ 1-პორტიანი მინი-USB და არანაკლებ 1-პორტიანი OOB 1 გბ Ethernet მართვით.
- არანაკლებ ორმაგი სარეზერვო AC კვების წყარო.
- არანაკლებ ორმაგი სარეზერვო ვენტილატორი.
- არანაკლებ 8 GB სისტემური მეხსიერება (RAM) და არანაკლებ 16 GB Flash/SSD
- არანაკლებ 16 მბ სისტემური ბუფერი.
- არანაკლებ 300ns დაყოვნება.
- არანაკლებ 1.7 Tbps კომუტაციის წარმადობა.
- არანაკლებ 1.26 Bpps გადამისამართების/დამუშავების სიმძლავრე.

მონაცემთა ცენტრის მახასიათებლები:

- პირდაპირი, ასევე შენახვის და გადატანის შესრულების არქიტექტურა.
- გიგანტური ჩარჩოების ზომები 9216 ბაიტამდე.
- VXLAN, VxLAN EVPN, VxLAN აპარატურა VTEP
- VMware NSX ინტეგრაცია არანაკლებ 1000 VNI'-მდე.
- ღია წვდომის მქონე(Openstack) მზა ინტეგრაცია.
- ვირტუალური მარშრუტიზაციისა და გადამისამართების ფუნქციები (VRFs), არანაკლებ 64-მდე VRF ინსტანცია.
- ღია ნაკადი(openflow) 1.3 ან ექვივალენტი SDN კონტროლერის მხარდაჭერით. უნდა ჰქონდეს ჰიბრიდული რეჟიმის მხარდაჭერა.
- IEEE 1588 PTP.
- ფაბრიკის ავტომატური კონფიგურაცია ისეთი ხელსაწყოების გამოყენებით, როგორიცაა Ansible, SaltStack, ZTP და Puppet.

გადართვის მახასიათებლები:

- 802.1Q VLAN, Voice VLAN, QinQ.
- RSTP, MSTP, RPVST, BPDU Filter & Guard, Loop Guard, Root Guard.
- VRRP, LAG, MLAG, LACP.
- მრავალფუნქციური კარიბჭე (MAGP)
- ინტერფეისი და პორტის იზოლაცია, LLDP,
- IGMP v3, IGMP snooping, PIM-SM და PIM-SSM
- სტატიკური მარშრუტი, OSPF, BGP, BFD, ECMP (არანაკლებ 64 გზა)

უსაფრთხოების მახასიათებლები:

- RADIUS, TACACS+ & LDAP
- FIPS 140-2 სისტემის უსაფრთხოება და NIST 800-181A შესაბამისობა.
- წვდომის კონტროლის სიები (ACLs L2-L4 და მომხმარებლის მიერ განსაზღვრული), 802.1X - პორტზე დაფუძნებული ქსელის წვდომის კონტროლი.
- CoPP, პორტის იზოლაცია

მართვა

- მრავალი კონფიგურაციის ფაილი, რომელიც ინახება ფლეშ/SSD საცავში, ZTP.
- sFlow (RFC 3176)/ექვივალენტი, JSON, CLI, WEB/GUI, SSH, Telnet.
- SNMPv3, NTP/SNTP, FTP/TFTP/SCP.
- პორტის სარკისებური ასახვა (SPAN & RSPAN), BER მონიტორინგი, ძირეული მიზეზების ანალიზი, ტელემეტრია, რეალურ დროში რიგის სიღრმის ჰისტოგრამები და ზღურბლები.

გადამცემები/DAC, თითოეული ობიექტისთვის:

- არანაკლებ 2x 100 გბ QSFP28/QSFP28 0,5 მ DAC.
- არანაკლებ 24x 25Gb SFP28-დან SFP28-მდე 3m DAC.
- არანაკლებ 8x 10GbE SFP+ მოკლე დიაპაზონის გადამცემი.
- არანაკლებ 4x QSFP/SFP+ ადაპტერი

5. Backup სისტემის მოთხოვნები:

შემოთავაზებული Backup სისტემის სანახი უნდა იყოს თავსებადი ამჟამად სსე-ს ინფრასტრუქტურაში მყოფ HPE Store Once 5200 გადაწყვეტილებასთან. უნდა გააჩნდეს მაღალი დედუბლიკაცია-კომპრესია.

ფიზიკური მოთხოვნები:

ფორმ ფაქტორი არანაკლებ 2U	Rack Mountable; უნდა იყოს უზრუნველყოფილი სასერვერო კარადაში განთავსებისათვის საჭირო კომპლექტით
Storage Capacity	80 TB raw, 56 TB useable
Data Transfer Rate	არანაკლებ 2 x 10/25Gb 2-port SFP Adapter
Raid ის მხარდაჭერა	RAID 5 or 6
Backup Applications	Virtual Tape Library (iSCSI, FC), and NAS (CIFS, NFS)
Virtual Tape Libraries and NAS Targets რიცხვი	მაქსიმუმ 192
Source Appliances	მაქსიმუმ 24

6. გადაწყვეტის პლატფორმა

პლატფორმა:

- შემოთავაზებული საცავი უნდა იყოს შემდეგი თაობის საცავის პლატფორმა, რომელიც შესთავაზებს როგორც კონვერგირებული, ასევე ჰიპერ-კონვერგიის ფუნქციონირებას, როგორც შენახვის, ასევე გამოთვლის დამოუკიდებელ მასშტაბირებას ყოველგვარი შეფერხების გარეშე.
- შემოთავაზებულ პლატფორმას უნდა ჰქონდეს სრული დამოუკიდებლობა როგორც გამოთვლითი, ასევე შენახვის პლატფორმის სკალირებისთვის. ორივე კომპონენტის სკალირება უნდა იყოს სრულიად დამოუკიდებელი დისკის ხელახალი დაბალანსების ოპერაციის გარეშე.

- **ჰიპერვიზორის მხარდაჭერა:** შემოთავაზებული პლატფორმა უნდა უზრუნველყოფდეს ჰიპერ-კონვერგენციის სიმარტივეს ცნობილი ჰიპერვიზორისგან, როგორიცაა VMware / Microsoft / Linux პლატფორმა, გადაწყვეტილებისთვის საჭირო ყველა ლიცენზიებთან (VMware) ერთად ქვემოთ მოცემული სპეციფიკაციებისა და მოთხოვნების შესაბამისად.

ტევადობა და მასშტაბურობა:

- შემოთავაზებული პლატფორმა მოწოდებული უნდა იქნას არანაკლებ 4 რაოდენობის გამოთვლითი ძრავით ერთ კლასტერში, მასშტაბირებადი არანაკლებ 32-მდე, არანაკლებ 32 ტბ გამოსაყენებელ სიმძლავრესთან ერთად არანაკლებ 1,92 ტბ დისკებით საცავის შრეზე.
- თითოეული გამოთვლითი ძრავა უნდა იყოს იმდენად მოქნილი, რომ დაინახოს და მოიხმაროს საცავის შრის მთელი სიმძლავრე.

მართვა

- სრული პლატფორმის მართვა უნდა მოხდეს უშუალოდ შემოთავაზებული ჰიპერვიზორის მართვის ფენიდან და არ საჭიროებდეს მრავალჯერადი მართვის ხელსაწყოებს ყოველდღიური ოპერაციებისთვის.
- თითოეულ გამოთვლით ძრავას უნდა ჰქონდეს დამატებითი ქსელის პორტი დისტანციური მართვისთვის. დისტანციურ მართვას უნდა ჰქონდეს საკუთარი გამოყოფილი ფლეშ მეხსიერება.
- თითოეულ გამოთვლით ძრავას უნდა ჰქონდეს უცვლელი სილიკონის ნდობის ფესვი, რათა უზრუნველყოს, რომ ნებისმიერ სიტუაციაში – პროგრამული უზრუნველყოფა თავისუფალია ყოველგვარი შეფერხებისგან და შეუძლებელია მისი კომპრომეტირება ნებისმიერ ეტაპზე.

მონაცემთა დაცვა:

- შემოთავაზებულმა პლატფორმამ უნდა გამოიყენოს ყველა NVMe ფლეშ დრაივი მხოლოდ საცავის შრისთვის. ყველა შემოთავაზებული NVMe ფლეშ დრაივი საცავის შრეზე უნდა იყოს კონფიგურირებული ტექნიკური საშუალების რეიდის ალგორითმით, რომელიც ითვალისწინებს არანაკლებ სამი დისკის ერთდროულ გაუმართაობას.
- ნებისმიერი გამოთვლითი ძრავის გაუმართაობამ არ უნდა შეამციროს შეთავაზებული დისკების საერთო რაოდენობა.

შესრულება:

- შემოთავაზებულ პლატფორმას უნდა ჰქონდეს უნარი, გამოიყენოს ყველა შემოთავაზებული დისკი საცავის შრეზე მოცემული ვირტუალური დრაივებისთვის როგორც წაკითხვის, ასევე ჩაწერის ოპერაციებისთვის და არ უნდა შემოიფარგლოს ლოკალური კვანძების განაწილებით.
- არ უნდა მოხდეს შესრულების დეგრადაცია კრიტიკული მხარდაჭერის აქტივობების დროს, როგორიცაა Firmware განახლება, პატჩის განახლება.

გაუმართაობის ერთი წერტილი:

- შემოთავაზებული პლატფორმა არ უნდა იყოს კონფიგურირებული ერთი გაუმართაობის გარემოში. მომწოდებელმა უნდა შეიმუშაოს ისეთი დიზაინი, რომ საცავის შრემ უზრუნველყოს არანაკლებ ცხრა მონაცემის ხელმისაწვდომობა და VM ხელმისაწვდომობის შენარჩუნება შეთავაზებული ჰიპერვიზორის კლასტერინგის მეშვეობით.
- არ უნდა მოხდეს შესრულების დეგრადაცია საცავის შრეზე ერთი კომპონენტის ან შენახვის კვანძის გაუმართაობის გამო.

CPU და დისკების მხარდაჭერა: შემოთავაზებულ პლატფორმას უნდა ჰქონდეს შესაძლებლობა, მხარი დაუჭიროს Intel-ის ან AMD-ს და სხვადასხვა NVMe ფლეშ ტევადობის დისკებს იმავე კლასტერში.

vVol ინტეგრაცია: შემოთავაზებული პლატფორმა მჭიდროდ უნდა იყოს ინტეგრირებული VMware-თან და უნდა იყოს სერტიფიცირებული VVOL-ისთვის. პლატფორმას არ უნდა დასჭირდეს რაიმე სახის დამხმარე პროგრამული უზრუნველყოფა vVols-თან გამართულად მუშაობისთვის და უნდა უზრუნველყოს შემდეგი:

- პლატფორმა მხარს უნდა უჭერდეს როგორც შეკუმშვას, ასევე დუბლირებას vVol-ებისთვის.
- პლატფორმა მხარს უჭერს vVols-ის დაგეგმილ სურათს და მომსახურების ხარისხს.
- პლატფორმა მხარს უჭერს დაშიფვრას vVol-ებისთვის.

ღრუბლოვანი მონიტორინგი, AI მხარდაჭერა და ანალიტიკა:

შემოთავაზებულ პლატფორმას უნდა ჰქონდეს ღრუბლოვანი მონიტორინგი, AI მხარდაჭერა და ანალიტიკური ძრავა პროაქტიული მართვისა და რისკის შესამცირებლად. აღნიშნულისთვის ყველა საჭირო ლიცენზია შეტანილი უნდა იყოს შეთავაზებაში. ღრუბლოვანმა მონიტორინგმა, AI მხარდაჭერამ და ანალიტიკის ძრავამ უნდა უზრუნველყოს შემდეგი:

- პროგრამული უზრუნველყოფის განახლებისა და პაჩის განახლების რეკომენდაციების მიწოდება პროაქტიულად და პლატფორმასთან დაკავშირებული პერიფერიული ინფრასტრუქტურის ინფორმირებულობით.
- ავტომატურად აღკვეთოს პროგრამული უზრუნველყოფის ინსტალაცია, რომელიც შეიძლება არათავსებადო იყოს საცავის შრესთან დაკავშირებულ სხვა ინფრასტრუქტურულ ნაწილებს.
- წუთში ისტორიული სიმძლავრის და შესრულების ტენდენციის ანალიზის უაღრესად დეტალური უზრუნველყოფა ნაგულისხმევად, დამატებითი ჟურნალის ჩართვის, ნებისმიერი მოწყობილობის (ფიზიკური ან ვირტუალური) დაყენების ან რაიმე პროგრამული უზრუნველყოფის დაყენების საჭიროების გარეშე.
- შესრულების ანალიტიკას უნდა შეეძლოს I/O–ს დაშლა I/O ზომის ჰისტოგრამებად, იდენტიფიცირება თანმიმდევრული და შემთხვევითი I/O და AI–ზე დაფუძნებული რჩევების მიწოდება მუშაობის პრობლემების გამოსასწორებლად.
- აღმოფხვრას მომხმარებლის მიერ მხარდაჭერისთვის ჩანაწერების მიწოდების აუცილებლობა, რადგან მხარდაჭერას ექნება საჭირო ინფორმაცია ავტომატურად გაგზავნილი პლატფორმიდან.

- უზრუნველყოს მხარდაჭერის შემთხვევის ისტორიის მიწოდება, რომელიც რეგისტრირებულია მხარდაჭერის გუნდთან ოპერატიული ეფექტურობით. მან ნათლად უნდა აჩვენოს მხარდაჭერის შემთხვევების პროცენტული მაჩვენებელი, რომელიც ავტომატურად დაიხურა ხელით.
- უნდა შეეძლოს უზრუნველყოს ერთი აღმასრულებელი დაფა, რომელიც მოიცავს მონაცემთა შემცირების ტექნოლოგიებისგან სივრცის დაზოგვის სხვადასხვა კრიტიკულ და აუცილებელ ასპექტებს, მონაცემთა დაცვის მზადყოფნას (როგორც RPO, ასევე შენახვის ვადის პერიოდში) საცავზე გაშვებული კლასიფიცირებული აპლიკაციებისთვის და აპლიკაციებისთვის კატასტროფის შედეგების შემდგომი აღდგენისთვის მზადყოფნა. .
- უზრუნველყოს სიჯანსაღის სრული სქემა და განსაზღვროს შესაბამისი წესი კონკრეტულ პირობებზე დაყრდნობით.
- უზრუნველყოს ავტომატური განახლების რეკომენდაციები როგორც პროგრამული უზრუნველყოფის, ასევე აპარატურის შესახებ, კონკრეტული ინსტრუქციებით იმის შესახებ, თუ რა უნდა განახლდეს და რამდენით.

Cloud Native Data Console: HCI-ის შემოთავაზებული საცავის შრეს უნდა ჰქონდეს ღრუბლოვანი მონაცემთა კონსოლი მართვისთვის.

მომსახურების ხარისხი:

- შემოთავაზებულმა პლატფორმამ უნდა უზრუნველყოს სერვისების ხარისხი (QoS -მონაცემთა გადაცემის მომსახურეობის ხარისხი და კლასი) მხარდაჭერა და IOPS და მბ/წმ მოცემულ მონაცემთა შენახვის შერჩევითი კონტროლისთვის.
- შეთავაზებულმა პლატფორმამ ავტომატურად უნდა განახორციელოს მონაცემთა გადაცემის მომსახურეობის ხარისხი და კლასი, რათა თავიდან აიცილოს ერთი სამუშაო დატვირთვის მიერ საერთო საცავი შრის ათვისება.

თხელი უზრუნველყოფა და სივრცის ოპტიმიზაცია:

- შეთავაზებულმა პლატფორმამ უნდა უზრუნველყოს მონაცემთა ეფექტურობის კრიტიკული გლობალური მახასიათებლები - ხაზშიდა დედუბლირება, ხაზშიდა შეკუმშვა და თხელი უზრუნველყოფა ყოველგვარი შესრულების დეგრადაციის გარეშე.
- მონაცემთა ეფექტურობის ყველა ზემოაღნიშნული მახასიათებელი უნდა იყოს ჭეშმარიტად გლობალური და უნდა ჰქონდეს შესაძლებლობა შეადაროს მსხვილი მონაცემები ყველა VM-ში და მონაცემთა საცავში, რომლებიც გააქტიურებულია/ შექმნილია პლატფორმაში.
- შეთავაზებულმა პლატფორმამ ერთდროულად უნდა უზრუნველყოს როგორც არადუბლირებული მონაცემთა ბაზების, ასევე დუბლირებული მონაცემთა ბაზების მხარდაჭერა პლატფორმის შიგნით.
- შემოთავაზებულმა პლატფორმამ ერთდროულად უნდა უზრუნველყოს როგორც შეკუმშული მონაცემთა ბაზების, ასევე არაშეკუმშული მონაცემთა ბაზების მხარდაჭერა პლატფორმის შიგნით.

მყისიერი ფოტო (სნეპშოტი) / დროის ამსახველი ასლი / ნულოვანი ასლის კლონი/ თხელი კლონი

- შეთავაზებულმა პლატფორმამ უნდა უზრუნველყოს არანაკლებ 1000-ზე მეტი მყისიერი Snapshot - ის მხარდაჭერა მოცემული მონაცემთა ბაზისთვის. მომწოდებელმა უნდა გამოიყენოს ეფექტური შესრულების ტექნოლოგია, როგორიცაა გადამისამართება ჩაწერაზე.
- ყველა შექმნილმა სნეპშოტმა უნდა უზრუნველყოს გლობალური დედუბლირება და შეკუმშვა.
- შემოთავაზებულმა პლატფორმამ უნდა უზრუნველყოს მრავალი სნეპშოტის, კლონის და რეპლიკაციის სესიის მხარდაჭერა, შესრულებაზე რაიმე ზემოქმედების გარეშე.

მონაცემთა მთლიანობა და დაშიფვრა:

- შემოთავაზებულმა პლატფორმამ უნდა შესთავაზოს საკონტროლო შეჯამება, რომლებიც სცილდება T10-PI სტანდარტს. საკონტროლო შეჯამება ავტომატურად უნდა აღმოაჩენდეს და თავიდან იცილებდეს შეცდომებს, რომლებიც წარმოიქმნება დაკარგული/არასწორი წაკითხვის ან ჩაწერის შედეგად, რომელსაც T10-PI და ექვივალენტური შემოწმების შეჯამების სისტემები ვერ გამოასწორებენ.
- შეთავაზებული პლატფორმა უზრუნველყოფილი უნდა იყოს AES-256 XTS FIPS სერტიფიცირებული დაშიფვრით დეტალურ მონაცემთა ბაზის დონეზე დაშიფრული NVMe ფლეშ დრაივების გამოყენების გარეშე.

დისტანციური რეპლიკაცია:

- შემოთავაზებულმა პლატფორმამ მხარი უნდა დაუჭიროს გაზრდილ კლასტერს სხვადასხვა ადგილზე, ამასთან, უზრუნველყოს, რომ ორმაგი ჩაწერა შენარჩუნებულია თითოეულ ადგილას. რეპლიკაცია ადგილებზე უნდა იყოს მშობლიური პლატფორმის შიგნით.
- შემოთავაზებულ პლატფორმას უნდა ჰქონდეს მხოლოდ დამატებითი ცვლილებების გამეორების შესაძლებლობა ორ საიტს შორის (პირველადი და მეორადი).
- შემოთავაზებულმა პლატფორმამ უნდა უზრუნველყოს FAN out ასინქრონული რეპლიკაცია პირველადი მდებარეობიდან არანაკლებ ორ მეორად ადგილას მოცემული მოცულობის / მონაცემთა საცავისთვის. მან უნდა უზრუნველყოს მოქნილობა, რათა განისაზღვროს ცალკე გრაფიკი თითოეული რეპლიკაციის ურთიერთობისთვის.

ლიცენზიები: მომწოდებელმა უნდა უზრუნველყოს ლიცენზია ყველა კრიტიკულ ფუნქციაზე, როგორიცაა სიმძლავრის გაფართოება, სნეპშოტი, თხელი კლონი, რეპლიკაცია და მონაცემთა გადაცემის მომსახურეობის ხარისხი და კლასი. შემდგომში არ უნდა იყოს საჭირო დამატებითი პროგრამული უზრუნველყოფის ლიცენზიის მოთხოვნა მომავალი სიმძლავრის განახლებისთვის.

7. აქტიური– აქტიური DC ბრანდმაური (დამცავი სისტემები)– ორი წყვილი (HA აქტიური– აქტიური)

ძირითადი მოთხოვნები
• შემოთავაზებული NGFW უნდა იყოს ლიდერი გარტნერის უახლეს ჯადოსნურ კვადრატში საწარმოს ქსელის ფაირვოლებისთვის. • შემოთავაზებული NGFW უნდა იყოს სერტიფიცირებული cTUVus, CB უსაფრთხოება, FCC კლასი A, CE კლასი A, VCCI კლასი A, KCC კლასი A, BSMI კლასი A - ებით. • შემოთავაზებულ NGFW-ს არ უნდა სჭირდებოდეს გადატვირთვა უსაფრთხოების განახლებების შესამოწმებლად და ინსტალაციისთვის. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს ინტეგრირებული ანგარიშგების შესაძლებლობები, რომელიც არ საჭიროებს დამატებით აპარატურას ანგარიშების გენერირებისთვის • შემოთავაზებულმა NGFW-მ უნდა განსაზღვროს აპლიკაციები პორტის, SSL/SSH დაშიფვრის ან გამოყენებული ავარიული ტექნიკის მიუხედავად. • შემოთავაზებულმა NGFW-მა უნდა მოახდინოს დაუდგენელი აპლიკაციების კატეგორიზაცია პოლიტიკის კონტროლის, საფრთხეების სასამართლო ექსპერტიზის ან განაცხადის იდენტიფიკაციის ტექნოლოგიის განვითარებისთვის. • შემოთავაზებული NGFW უნდა იყოს ბუნებრივად შემუშავებული უსაფრთხოების გადაწყვეტა (არა აპლიკაციის საკონტროლო Blade - ი, რომელსაც აქვს ძირითადი სახელმწიფო ინსპექტირების ფაირვოლი). • შემოთავაზებული NGFW უნდა იყოს „natively“-ი ინჟინერიის მქონე მოწყობილობა, ერთი პარალელური დამუშავების არქიტექტურით ტრაფიკის დამუშავებისთვის. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს ინტეგრირებული ტრაფიკის ფორმირების ფუნქცია (მონაცემთა გადაცემის მომსახურეობის ხარისხი და კლასი) წყაროს/დანიშნულების IP, პორტის, პროტოკოლისა და აპლიკაციის საფუძველზე. • შემოთავაზებულმა NGFW-მა უნდა განსაზღვროს აპლიკაციის სხვადასხვა ნაწილი, როგორიცაა Facebook ჩეთის დაშვება, მაგრამ ფაილის გადაცემის შესაძლებლობის დაბლოკვა. • შემოთავაზებულმა NGFW-მა უნდა გააკონტროლოს წვდომა და განახორციელოს პოლიტიკა ვებსაიტებზე და აპლიკაციებზე, მათ შორის SaaS აპლიკაციებზე. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს ერთი OS ყველა ფორმის ფაქტორზე.

- შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს უსაფრთხოების პოლიტიკის შექმნას რწმუნებათა სიგელების მოპარვის თავიდან ასაცილებლად.
- შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს შიდა აპლიკაციებში მრავალფაქტორიანი ავთენტიფიკაციის განხორციელებას.
- შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს შეუზღუდავი ღია API-ის გარეშე paywall (გამოწერა) Dev Toolkit-ზე, ინსტრუმენტებზე, სკრიპტებსა და ნიმუშებზე წვდომისთვის.
- შემოთავაზებულმა NGFW-მ უნდა უზრუნველყოს მომხმარებლის/მომხმარებლების/მომხმარებლების ჯგუფების დინამიურად და ავტომატურად გადაჯგუფების შესაძლებლობა ამ მომხმარებლის უსაფრთხოების მოვლენებზე დაყრდნობით.
- შემოთავაზებული NGFW - ი უნდა უზრუნველყოფდეს ხილვადობას და აპლიკაციების შეზღუდვის შესაძლებლობას არასტანდარტული პორტების გამოყენებით უსაფრთხოების პოლიტიკის ერთი წესით.
- შემოთავაზებულ NGFW-ს უნდა შეეძლოს ობიექტების მონიშვნა, რათა ჩართოს პოლიტიკის დინამიური აღსრულება, მიუხედავად IP-ის, არეალის ან მიმართულების ცვლილებისა.
- შემოთავაზებულმა NGFW-მა უნდა გასცეს OS-ის მარტივი განახლებები, გარკვეული კომბინაციების საჭიროების გარეშე, სწრაფი შესწორებების ან პატჩებისთვის.
- შემოთავაზებულ NGFW-ს უნდა ჰქონდეს მრავალი OS გამოსახულების შენახვის ფუნქცია ვერსიის განახლების დროს მდგრადობისა და მარტივი rollback - ის მხარდასაჭერად
- შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს უსაფრთხოების ნებისმიერი ახალი შეთავაზების ჩართვას მასში გამავალი ტრაფიკის მუშაობაზე გავლენის გარეშე.
- შემოთავაზებულ NGFW-ს უნდა ჰქონდეს ფუნქცია, განსაზღვროს რომელი აპლიკაციები ემთხვევა უსაფრთხოების პოლიტიკას და ამ პოლიტიკის მიგრაციას აპლიკაციებზე დაფუძნებულ პოლიტიკაში.
- უნდა შეიცავდეს საჭირო გამოწერის ლიცენზიებს და მომწოდებლის მხარდაჭერას ერთი წლის განმავლობაში. ძირითადი ლიცენზიების ჩამონათვალი:
    - Advanced Threat Prevention Subscription
    - Sandbox Subscription
- ზემო აღნიშნული ზოგიერთი ფუნქციონალის ჩამონათვალი მხარს უნდა უჭერდეს და აქტიურდებოდეს შემოთავაზებულ გადაწყვეტილებას მხოლოდ დამატებითი ლიცენზიების შემდგომსი შეძენით.

- მოწოდებულ ბრანდმაურს უნდა გააჩნდეს შემდეგი პროტოკოლების მხარდაჭერა:

    - OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
    - Policy-based forwarding
    - Point-to-point protocol over Ethernet (PPPoE)
    - Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
    - Bidirectional Forwarding Detection (BFD)
    - 802.1Q VLAN tags per device/per interface: არანაკლებ 4,094/4,094
    - Aggregate interfaces (802.3ad), LACP
    - NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
    - NAT64, NPTv6
    - Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription
    - Failure detection: path monitoring, interface monitoring

არქიტექტურა, ფიზიკური და შესრულების სპეციფიკაციები
• თითოეული შემოთავაზებული NGFW გადაწყვეტა არ უნდა შეიცავდეს დამატებით დატვირთვის ბალანსერს ან გადამრთველზე დაფუძნებულ მრავალ მოწყობილობას. • თითოეულმა შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს NGFW ფაირვოლის გამტარუნარიანობის არანაკლებ 24 გბიტი/წმ და უზრუნველყოს მაქსიმუმ არანაკლებ 30.2 გბ/წმ-მდე გამტაროობა. (ფაირვოლის გამტარუნარიანობა იზომება App-ით და ჩართული რეგისტრაციით არაუმეტეს 64 KB HTTP/appmix ტრანზაქციების გამოყენებით)" • თითოეულმა შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს არანაკელბ 11 გბიტი/წმ threat prevention throughput - ი და მხარი დაუჭიროს მაქსიმუმ არანაკლებ 12.8 გბ/წმ-მდე გამტაროობას. (threat prevention throughput იზომება App, IPS, ანტივირუსული, ანტი-ჯაშუშური, sandbox, DNS უსაფრთხოება, ფაილების დაბლოკვით, არაუმეტეს 64 KB HTTP/appmix ტრანზაქციების გამოყენებით)" • თითოეულმა შემოთავაზებულმა NGFW-მ უნდა უზრუნველყოს არანაკელბ 14.5 გბიტი/წმ IPsec VPN გამტარუნარიანობა“(IPsec VPN გამტარუნარიანობა იზომება არაუმეტეს 64 KB HTTP ტრანზაქციებით). • თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს არანაკლებ 3,000,000 მაქსიმალური სესიის მხარდაჭერა. • თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს არანაკლებ 268,000 ახალი კავშირების მხარდაჭერა წამში (გაზომილი აპლიკაციის გადაფარვით, არაუმეტეს 1 ბაიტი HTTP ტრანზაქციის გამოყენებით). • თითოეულმა შემოთავაზებულმა NGFW-მ უნდა უზრუნველყოს ვირტუალური სისტემების დამატება მომავალი გაფართოებისთვის არანაკლებ 11 Virtual Systems (დამატებითი ლიცენზიის შემთხვევაში). • თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს Gigabit Ethernet და ბოჭკოვანი ინტერფეისების მხარდაჭერა მაღალი ხარისხის კავშირის მისაღებად, რომელიც მოერგება ქსელის ცვლილებებს. • თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს: ➢ არანაკლებ 12 - 1G/2.5G/5G/10G RJ45 ელექტრული ინტერფეისი. ➢ არანაკლებ 10 - 1G/10G SFP/SFP+ ოპტიკური ინტერფეისი. ➢ არანაკლებ 4 - 25G SFP28 ოპტიკური ინტერფეისი. ➢ არანაკლებ 2 - 40G/100G QSFP/QSFP28 ოპტიკური ინტერფეისი. • თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს მხარდაჭერილი: ➢ არანაკლებ 1 - 100/1000 out-of-band management port ➢ არანაკლებ 2 - 100/1000 high availability ➢ არანაკლებ 1 - 10G SFP+ high availability ➢ არანაკლებ 1 - RJ-45 console port ➢ არანაკლებ 1 - Micro USB • თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს სარეზერვო ცვლადი დენის წყარო.(AC) • თითოეულმა შემოთავაზებულმა NGFW-მ უნდა უზრუნველყოს აქტიური/აქტიური, აქტიური/პასიური და კლასტერული განლაგება. აქტიურ - აქტიურ გადაწყვეტილებას უნდა შეეძლოს შემდეგი ტრაფიკისა და სესიების ბალანსეირების მექანიზმები: ➢ Route-Based Redundancy. ➢ Floating IP Address and Virtual MAC Address. ➢ ARP Load-Sharing.

- თითოეულმა შემოთავაზებულმა NGFW-მ უნდა უზრუნველყოს სრული სესიის შენარჩუნება მოლოდინის ერთეულზე შეფერხების შემთხვევაში.
- თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს მაღალი ხელმისაწვდომობის ფუნქცია NAT/მარშრუტის ან გამჭვირვალე რეჟიმისთვის.
- თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს მრავალი პერიოდული სიგნალის ბმულის მხარდაჭერა.
- თითოეულმა შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს L3, L2, L1 გამჭვირვალე და შეხების რეჟიმის განლაგება.
- თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს SSL გაშიფვრის სარკისებური მხარდაჭერა
- თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს SSL გაშიფვრის ბროკერის მხარდაჭერა შიდა შემოწმებისთვის და ქსელის პაკეტის ბროკერისთვის (ორმხრივი-TCP-UDP) (ფენის 1 და ფენის 3 რეჟიმები).
- თითოეულ შემოთავაზებულ NGFW-ს უნდა ჰქონდეს SSH გაშიფვრის მხარდაჭერა SSH გვირაბის გამოსავლენად.

უსაფრთხოების პოლიტიკის კონტროლის მახასიათებლები

- შემოთავაზებულმა NGFW-მა მხარს უნდა უჭირდეს უსაფრთხოების პოლიტიკის შექმნას მე-7 შრის აპლიკაციებზე, რომლებიც შეუსაბამოა TCP/UDP პორტის ნომერთან (არაპროფილზე დაფუძნებული აპლიკაციის კონტროლი).
- შემოთავაზებულ NGFW-ს უნდა ჰქონდეს ჩაშენებული უსაფრთხოების პოლიტიკის ოპტიმიზაციის ინსტრუმენტი, რომელიც ხელს უწყობს მე-4 პორტზე დაფუძნებული უსაფრთხოების პოლიტიკის მე-7 შრის აპლიკაციებზე დაფუძნებულ კონვერტაციას. პოლიტიკის ოპტიმიზაციის ხელსაწყოს უნდა შეეძლოს აჩვენოს აპლიკაციის გამოყენების კონკრეტული წესი ბოლო 15, 30 დღის განმავლობაში.
- შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს უსაფრთხოების პოლიტიკის აღსრულებას გრაფიკის საფუძველზე.
- შემოთავაზებულმა NGFW-მა უნდა გაამარტივოს წესების გამოყენების თვალყურის დევნება დროის შტამპის მეშვეობით წესების უახლესი შესაბამისობისთვის, დროის შტამპის პირველი წესის შესატყვისი და წესების შესაბამისი მრიცხველის მეშვეობით.

საფრთხის პრევენციის მახასიათებლები
• შემოთავაზებული NGFW-ი უნდა იცავდეს ქსელებს მრავალშრიანი პრევენციის უზრუნველყოფით, შეტევის თითოეულ ფაზაში საფრთხეებთან დაპირისპირებით. • შემოთავაზებულმა NGFW-მა უნდა აღმოაჩინოს და დაბლოკოს საფრთხეები ნებისმიერ და ყველა პორტზე, წინასწარ განსაზღვრული პორტების შეზღუდული ნაკრების საფუძველზე ხელმოწერების გამოძახების ნაცვლად. • შემოთავაზებულმა NGFW უნდა ისარგებლოს ღრუბელში მოწოდებული უსაფრთხოების სხვა ხელმოწერებით ყოველდღიური განახლებისთვის, რომლებიც აჩერებენ ექსპლუატაციას, მავნე პროგრამას, მავნე URL-ებს, ბრძანებებს და კონტროლს (C2) და ჯაშუშურ პროგრამებს. • შემოთავაზებულმა NGFW-მა უნდა გამოიყენოს მავნე პროგრამების ხაზშიდა დაცვა — ხელმოწერების მეშვეობით, რომლებიც დაფუძნებულია დატვირთვაზე და არა ჰეშზე. • შემოთავაზებულმა NGFW-მა უნდა გამოიყენოს ევრისტიკაზე დაფუძნებული ანალიზი, რომელიც აღმოაჩენს ანომალიურ პაკეტებს და ტრაფიკის შაბლონებს, როგორიცაა პორტების სკანირება, ჰოსტის გაწმენდა და სერვისის უარყოფის (DoS) შეტევები. • შემოთავაზებულმა NGFW-მა ხელი უნდა შეუწყოს მორგებული ხელმოწერების შექმნას, რაც ქსელის უნიკალურ საჭიროებებზე თავდასხმის პრევენციის შესაძლებლობების მორგებას უზრუნველყოფს. • შემოთავაზებულმა NGFW-მ მხარი უნდა დაუჭიროს თავდასხმისგან დაცვის სხვა შესაძლებლობებს, როგორიცაა არასწორი ან მავნე ფორმის პაკეტების დაბლოკვა, IP დეფრაგმენტაცია და TCP ხელახლა შეკრება. • შემოთავაზებულმა NGFW-მა უნდა გამოიყენოს ბუნებრივად ინტეგრირებული თავდაცვითი ტექნოლოგიები, რათა უზრუნველყოფილი იყოს საფრთხის განეიტრალება. ანუ, როდესაც საფრთხე თავს არიდებს ერთ ტექნოლოგიას, მეორე ტექნოლოგია დაიჭერს მას.

- შემოთავაზებულმა NGFW-მ უნდა შეამოწმოს და მოახდინოს ტრაფიკის კლასიფიკაცია, ასევე აღმოაჩინოს და დაბლოკოს როგორც მავნე პროგრამები, ასევე დაუცველობა ერთ მარშრუტზე.
- შემოთავაზებულმა NGFW-მა უნდა მოაწესრიგოს თითოეული პაკეტი პლატფორმაზე გავლისას და ყურადღებით დააკვირდეს ბაიტის თანმიმდევრობებს როგორც პაკეტის სათაურში, ასევე დატვირთვაში.
- შემოთავაზებულმა NGFW-მა უნდა გააანალიზოს კონტექსტი, რომელიც მოცემულია მრავალი პაკეტის შემოსვლის ბრძანებით და თანმიმდევრობით, რათა დაიჭიროს და აღკვეთოს თავიდან აცილების ტექნიკა.
- შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს პროტოკოლის დეკოდერზე დაფუძნებულ ანალიზს.
- შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს პროტოკოლის ანომალიაზე დაფუძნებული დაცვა.
- შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს შეკუმშულ ფაილებსა და ვებ შინაარსში დამალული მავნე პროგრამის გამოვლენასა და პრევენციას.
- შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს დაცვა გადატვირთვისგან, რომლებიც დამალულია ფაილის საერთო ტიპებში, როგორიცაა Office/Microsoft 365 დოკუმენტები და PDF-ები.
- შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს დაკავშირებული საფრთხის მოვლენების სერიის კორელაცია (მაგ., საფრთხის პრევენციის ჟურნალებიდან), რომლებიც კომბინირებულად მიუთითებენ სავარაუდო თავდასხმაზე.
- შემოთავაზებულ NGFW-ს უნდა ჰქონდეს გამონაკლისის კონფიგურაციის შესაძლებლობა.
- შემოთავაზებულ NGFW-ს უნდა შეეძლოს მავნე პროგრამის აღმოჩენა და თავიდან აცილება სხვადასხვა ფაილის ტიპების სკანირებით.
- შემოთავაზებულ NGFW-ს უნდა შეეძლოს მავნე პროგრამების იდენტიფიცირება შემომავალი ფაილებიდან და ინტერნეტიდან ჩამოტვირთული მავნე პროგრამებისგან.
- შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს აპლიკაციებისთვის მორგებული ხელმოწერის შექმნის შესაძლებლობა.
- შემოთავაზებულ NGFW-ს უნდა ჰქონდეს ყველა ძირითადი აპლიკაციის ხელმოწერა და მას უნდა შეეძლოს ისეთი ცნობილი აპლიკაციის იდენტიფიცირება, როგორიცაა P2P.
- შემოთავაზებულ NGFW-ეს უნდა ჰქონდეს მხარდაჭერა ჩართოს DNS მოთხოვნაზე პასუხის გაყალბება ცნობილი მავნე დომენისთვის და გამოიწვიოს ამ მავნე დომენის სახელის მიწოდება კლიენტისთვის მიცემული IP მისამართით, ინფიცირებული ჰოსტების იდენტიფიცირებისთვის.
- შემოთავაზებულმა NGFW-მა უნდა დაუშვას ცალკეული პოლიტიკის მოქმედებების განსაზღვრა, ისევე როგორც ჩანაწერის დონე კონკრეტული ხელმოწერის ტიპისთვის.
- შემოთავაზებულმა NGFW-მა უნდა განსაზღვროს DGA-ების გამოყენება, რომელიც აწარმოებს შემთხვევით დომენებს მავნე პროგრამისთვის C2 სერვერზე დასაბრუნებლად გამოსაყენებლად.
- შემოთავაზებულმა NGFW-მა უნდა განსაზღვროს DGA (დომენის გენერაციის ალგორითმები) დომენები ლექსიკონის სიტყვებზე დაყრდნობით.
- შემოთავაზებულმა NGFW-მა უნდა დაიცვას მომხმარებლები დომენებთან დაკავშირებისაგან, რომლებიც შეიძლება გამოყენებულ იქნას DDoS შეტევების დასაწყებად.
- შემოთავაზებული NGFW მხარდაჭერის პროტოკოლები უნდა იყოს SMTP, POP3, SMB, FTP, IMAP, HTTP, HTTPS.

მომხმარებლის იდენტიფიკაციისა და ავთენტიფიკაციის მახასიათებლები
• შემოთავაზებულმა NGFW-მა ხელი უნდა შეუწყოს მომხმარებლის ID-ის იდენტიფიკაციას აქტიური დირექტორიასთან WinRM-ისა და WMI-ის ინტეგრირების მეშვეობით. • შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს მომხმარებლის ID-ის იდენტიფიკაციას Exchange-თან WinRM-ისა და WMI-ის ინტეგრირების მეშვეობით. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს მომხმარებლის ID-ის იდენტიფიკაცია syslog მიმღებად გაშვებით. • შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს მომხმარებლის ID-ის იდენტიფიკაციას XML API-ების მესამე მხარის გადაწყვეტილებებთან ინტეგრირებით. • შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს მომხმარებლის ID-ის იდენტიფიკაციას დაკავებული პორტალის მეშვეობით. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს მომხმარებლის ID-ის იდენტიფიკაცია ტერმინალის სერვერებში. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს მომხმარებლის ID-ის იდენტიფიკაცია მომხმარებლის აპარატებზე აგენტის გაშვებით. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს პირდაპირი მრავალფაქტორიანი ავთენტიფიკაციის ინტეგრაცია RSA, Okta, PingID და Duo-სთან. • შემოთავაზებულმა NGFW-მ უნდა უზრუნველყოს SSO ავტორიზაცია. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს მრავალი სერვერის პროფილების მხარდაჭერა, როგორიცაა SAML 2.0, Radius, LDAP, Tacacs+ და Kerberos.

მართვის, რეგისტრაციისა და ანგარიშგების ფუნქციები
• შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს ბრძანების ხაზის ინტერფეისი (CLI) • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს ჩაშენებული ვებ ინტერფეისი, არა Java-ბაზის (GUI). • შემოთავაზებულმა NGFW-მ მხარი უნდა დაუჭიროს XML Rest API-ზე დაფუძნებულ მართვას. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს ვალდებულებაზე დაფუძნებული კონფიგურაციის მართვა • შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს კონფიგურაციის აუდიტს გაშვებული კონფიგურაციის კანდიდატის კონფიგურაციის შედარებით. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს ინტერაქტიული გრაფიკული შეჯამება აპლიკაციების, მომხმარებლების, URL-ების, საფრთხეებისა და კონტენტის გარშემო, რომლებიც გადის ქსელში. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს მორგებულ გრაფიკზე დაფუძნებული ქსელის აქტივობა აპლიკაციებისთვის, რომლებიც იყენებენ არასტანდარტულ პორტებს. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს მორგებული გრაფიკზე დაფუძნებული დაბლოკილი აქტივობები, რომელიც მოიცავს დაბლოკილი აპლიკაციების აქტივობას, დაბლოკილი მომხმარებლების აქტივობას, დაბლოკილი კონტენტის აქტივობას, დაბლოკილი საფრთხეების აქტივობასა და უსაფრთხოების პოლიტიკის დაბლოკვის აქტივობას. • შემოთავაზებულმა NGFW-მა უნდა შესთავაზოს მორგებულ გრაფიკზე დაფუძნებული გვირაბის აქტივობები, მათ შორის გვირაბის ID/ტეგი, გვირაბის აპლიკაციის გამოყენება, გვირაბის მომხმარებლის აქტივობა და გვირაბის IP წყარო/დანიშნულების აქტივობა. • შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს მორგებულ მოხსენებას მომხმარებლის, მომხმარებელთა ჯგუფისა და აპლიკაციის შესახებ ანგარიშის გენერირების შესაძლებლობით. • შემოთავაზებულმა NGFW-მ მხარი უნდა დაუჭიროს ანგარიშების ექსპორტს PDF-ში და ანგარიშების გაგზავნას ელ.ფოსტით. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს გამოყოფილი SaaS აპლიკაციების გამოყენების ანგარიში. • შემოთავაზებულ NGFW-ს უნდა ჰქონდეს გამოყოფილი ჩანაწერების კომპლექტები ტრაფიკისთვის, საფრთხეებისთვის, URL-ის ფილტრაციისთვის, მონაცემთა გაფილტვრისთვის, ფაილების კონტროლისთვის, მომხმარებლის იდენტიფიკაციის რუკებისთვის, ავთენტიფიკაციისთვის, კონფიგურაციისთვის, სისტემისა და სიგნალიზაციისთვის. • შემოთავაზებულმა NGFW-მა მხარი უნდა დაუჭიროს ადმინისტრატორის მორგებულ როლებს. • შემოთავაზებულმა NGFW-მა უნდა მისცეს ადმინისტრატორებს უფლება, იმუშაონ პირდაპირ მოწყობილობაზე და საჭიროებისამებრ განახორციელონ კონფიგურაციის ცვლილებები ცენტრალურ მენეჯერში შესვლის გარეშე. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს ცენტრალურ ადმინისტრატორებს ადგილობრივი ადმინისტრატორების მიერ განხორციელებული ცვლილებების მონიტორინგი და დათვალიერების საშუალება. • შემოთავაზებული NGFW-ის მენეჯმენტი უნდა განხორციელდეს უშუალოდ მოწყობილობის მეშვეობით კლიენტების ან ვირტუალური მანქანების დაყენების საჭიროების გარეშე. • შემოთავაზებულმა NGFW-მა უნდა შესთავაზოს შესაძლებლობა აირჩიოს, რომელი ფაიერვოლ ადმინისტრატორის კონფიგურაციის ცვლილებები განხორციელდეს ფაიერვოლებზე. • შემოთავაზებულმა NGFW-მა უნდა უზრუნველყოს კონკრეტული მომხმარებლებისგან ცვლილებების სწრაფად დაბრუნების და კონფიგურაციის აღდგენის შესაძლებლობა.

8. მხარდაჭერა და ტექნიკური მომსახურება.

- შემოთავაზებულ Active / Active HCI სისტემას უნდა მოყვებოდეს მწარმოებლის 3 წლიანი მხარდაჭერა.
- შემოთავაზებულ Backup -ის სისტემას უნდა მოყვებოდეს მწარმოებლის 3 წლიანი მხარდაჭერა.
- შემოთავაზებულ HCI - სისტემაში შემავალ კომუტატორებს უნდა მოყვებოდეს მწარმოებლის 3 წლიანი მხარდაჭერა.
- შემოთავაზებული Active / Active HCI სისტემა უნდა მოიცავდეს ვირტუალი ჰიპერვიზორის ყველა ლიცენზიას (VMware - ის შემთხვევაში - VMware ESXi, VMware vCenter) და უნდა იყოს 3 წლიანი მხარდაჭერით.
- შემოთავაზებული Active / Active HCI გადაწყვეტილება, მასში შემავალი კომუტატორები და Backup სისტემა უნდა იყოს ერთი და იმავე მწარმოებლის.
- შემოთავაზებული Active / Active HA ბრანდმაურებეს უნდა მოყვებოდეს მწარმოებლის 1 წლიანი მხარდაჭერა.
- მომწოდებელმა უნდა უზრუნველყოს თანმდევი ტექნიკური მომსახურება გადაწყვეტილებების სრული ინტეგრაციით შემსყიდველის IT თანამშრომლებთან ერთად.
    - აპარატურის ფიზიკური მონტაჟი და დაკაბელება;
    - აპარატურის ამოცანის შესაბამისად კონფიგურაცია, Firmware-ების ბოლო სტაბილურ ვერსიამდე განახლება და ლიცენზიების აქტივაცია;
    - მონაცემთა დამუშავების ცენტრალურ და სარეზერვო ცენტრებს შორის გაწელილი vSphere ვირტუალიზაციის კლასტერის აგება და ტესტირება.
    - ბრანდამურების Active / Active კლასტერი მოწყობა და ტესტირება.
    - არსებული DC ქსელის რედიზაინი და ახალ გადაწყვეტილებაში გაშვება.
    - Failover - ის მექანიზმების შემუშავება მწარმოებლის Best Practice - ზე დაფუძნებით.
    - ბრანმაურებზე პოლიტიკებისა და რულების განსაზღვრა სსე - ს ინფორმაციული უსაფრთხოების განყოფილებასთან შეთანხმებით.
- მომწოდებელმა უნდა უზრუნველყოს შემსყიდველის არსებული სერვისების მიგრაცია ახალ სისტემაზე, გატესტვა და წარმოებაში გაშვება.
- მომწოდებელს უნდა გააჩნდეს სერთიფიცირებული ინჟინრები შემოთავაზებული ვენდორების გაცემული სერთიფიკატებით.
- შემსყიდველმა უნდა უზრუნველყოს დამოუკიდებელი მოწყობილობა Witness - ის სერვერისთვის.

9. ტრენინგები.

- ყველა შეთავაზება უნდა მოიცავდეს ტრენინგებს სსე-ს თანამშრომლებისთვის.

- ტრენინგი უნდა მოიცავდეს კურს(ებ)ს, რომელიც მოიცავს შემოთავაზებული ტექნიკისა და პროგრამული უზრუნველყოფის კომპონენტების ძირითად, შუალედურ და გაფართოებულ ოპერაციებს, კონფიგურაციას, ტექნიკური მომსახურებისა და პრობლემების მოგვარების თემებს

- ტრენინგების ენა უნდა იყოს ინგლისური. პროვაიდერმა დამსწრეებს უნდა მიაწოდოს მომხმარებლის სახელმძღვანელი და დოკუმენტაცია.

- წინადადებაში ტრენინგის განყოფილება უნდა შეიცავდეს შემდეგ ინფორმაციას:
    - კურსების სია.
    - მოკლე აღწერა თითოეული კურსისთვის.
    - ხანგრძლივობა თითოეული კურსისთვის.

- ყველა სასწავლო კურსი უნდა ჩატარდეს ინსტრუქტორის მიერ.
- ტრენინგი შეიძლება ჩატარდეს სსე-ის შენობაში ან მიმწოდებლის/ტრენინგ პარტნიორის შენობაში:
- ყველა სასწავლო კურსი უნდა მოიცავდეს პრაქტიკულ ლაბორატორიულ სექციებსაც.

10.მომწოდებლის მოთხოვნები:

- შემოთავაზებული გადაწყვეტილებების მომწოდებელს უნდა ჰქონდეს წარმომადგენლობითი ოფისი საქართველოში ან ჰყავდეს ძლიერი პარტნიორი ტექნიკური მხარდაჭერისა და განხორციელების სერვისების გაწევის უნარით.

11.პრეტენდენტის მოთხოვნები / წარსადგენი დოკუმენტაცია:

- პრეტენდენტმა უნდა წარმოადგინოს მწარმოებლების ავტორიზაციის ფორმა (MAF).
- პრეტენდენტს უნდა ჰქონდეს შესაბამისი კვალიფიკაცია პროექტის განსახორციელებლად.

<u>დამატებითი მოთხოვნები - პასიური ინვენტარი:</u>

- არანაკლებ 30 ცალი SFP+ SR ოპტიკური გამსხივებელი თავსებადი მოთხოვნილ აპარატურასთან
- არანაკლებ 20 ცალი SFP+ LR ოპტიკური გამსხივებელი თავსებადი მოთხოვნილ აპარატურასთან
- არანაკლებ 8 ცალი SFP+ ZR ოპტიკური გამსხივებელი თავსებადი მოთხოვნილ აპარატურასთან
- არანაკლებ 12 ცალი 40/100 QSFP28 BASE - SR ოპტიკური გამსხიველებელი თავსებადი მოთხოვნილ აპარატურასთან
- არანაკლებ 20 ცალი 1G SFP-T ოპტიკური გამსხივებელი თავსებადი მოთხოვნილ აპარატურასთან
- არანაკლებ 20 ცალი OM3 1 მეტრიანი ოპტიკური პაჩკორდი MM
- არანაკლებ 20 ცალი OM3 5 მეტრიანი ოპტიკური პაჩკორდი MM
- არანაკლებ 20 ცალი SM 15 მეტრიანი ოპტიკური პაჩკორდი.
- არანაკლებ 10 ცალი SM 5 მეტრიანი ოპტიკური პაჩკორდი.