სატენდერო დოკუმენტაცია
შპს "თბილისი ენერჯი"-ს (შემდგომში - "შემსყიდველი")
მიერ ვირტუალური დესკტოპ ინფრასტრუქტურის შესყიდვასთან დაკავშირებით
გამოცხადებულ ტენდერში მონაწილეობის მისაღებად

წინამდებარე სატენდერო დოკუმენტაცია შემუშავებულია შპს „თბილისი ენერჯი"-ს გენერალური დირექტორის ბრძანებით დამტკიცებული შპს "თბილისი ენერჯი"-ში შესყიდვების დაგეგმვისა და განხორციელების წესის შესახებ დებულების" საფუძველზე.
სატენდერო დოკუმენტაცია გადაეცემა პოტენციურ მიმწოდებელს შესაბამისი სატენდერო განაცხადის მოსამზადებლად.

1. ზოგადი დებულებები

1.1. სატენდერო დოკუმენტაცია განკუთვნილია პოტენციური მიმწოდებლისათვის და მიზნად ისახავს მისთვის სატენდერო პირობების შესახებ სრული ინფორმაციის მიწოდებას.
1.2. ტენდერი ტარდება ვირტუალური დესკტოპ ინფრასტრუქტურის (შემდგომში - "საქონელი") მიმწოდებლის გამოსავლენად.

2. საქონელი

2.1. იხ. ტექნიკური დავალება დანართი #3;
2.2. ანგარიშსწორება ხორციელდება:
სრულად საქონლის მოწოდებიდან და აქტივაციიდან 30 კალენდარული დღის ვადაში;

3. საკვალიფიკაციო მოთხოვნები

3.1. ტენდერში მონაწილეობისთვის პოტენციურმა მიმწოდებელმა (პრეტენდენტმა) უნდა წარმოადგინოს შემდეგი დოკუმენტაცია:
ა) ტექნიკური შეფასების კრიტერიუმებით და პირობებით მოთხოვნილი (იხ.დანართი #1);
ბ) დოკუმენტაცია ტექნიკური შეთავაზების წერილი (იხ.დანართი #2);
გ) კომერციული შეთავაზება (ფასების ცხრილის გათვალისწინებით);
პრეტენდენტი არ უნდა იყოს შეტანილი შესაბამისი სახელმწიფო ორგანოს მიერ წარმოებულ შესყიდვებში მონაწილე არაკეთილსინდისიერ პირთა რეესტრში (შავი სია);
პრეტენდენტი უნდა აკმაყოფილებდეს საქართველოს კანონმდებლობითა და სატენდერო დოკუმენტაციით განსაზღვრულ სხვა მოთხოვნებს.
3.2. პოტენციურმა მიმწოდებელმა (პრეტენდენტმა) საზოგადოებას უნდა წარუდგინოს მოწმობების, ლიცენზიების, ცნობებისა და სხვა დოკუმენტების ასლები, რომლებიც ადასტურებენ მის შესაბამისობას საკვალიფიკაციო მოთხოვნებთან.
3.3. შემსყიდველი არ განიხილავს სატენდერო განაცხადს, თუ პოტენციური მიმწოდებელი არ წარმოადგენს საკვალიფიკაციო მოთხოვნებთან შესაბამისობის დამადასტურებელ დოკუმენტაციას ან თუ წარმოდგენილი დოკუმენტაცია არასრული, არაზუსტი ან/და მცდარი აღმოჩნდება.
3.4. სატენდერო განაცხადებაში მითითებული მონაცემების საკვალიფიკაციო და სხვა მოთხოვნებთან შესაბამისობის დადგენის მიზნით შემსყიდველი უფლებამოსილია, ტენდერის მიმდინარეობისას განახორციელოს მონაწილეების წინასწარი საკვალიფიკაციო შერჩევა. შეუსაბამობის გამოვლენის შემთხვევაში, პოტენციური მიმწოდებელი შეფასებაზე არ დაიშვება.
3.5. პოტენციური მიმწოდებლის მიერ ტენდერზე წარმოდგენილი ცნობები გაცემული უნდა იყოს ტენდერის გამოცხადების შემდგომ პერიოდში.

4. სატენდერო განაცხადების წარდგენა. სატენდერო განაცხადების მოქმედების ვადა

4.1. ტენდერში მონაწილეობის მსურველმა პოტენციურმა მიმწოდებელმა, შემსყიდველს უნდა წარუდგინოს ორ დალუქულ კონვერტში მოთავსებული სატენდერო განაცხადი, ერთ კონვერტში

ტექნიკური შეთავაზების წერილი და შეფასების კრიტერიუმებით და პირობებით მოთხოვნილი დოკუმენტაცია, მეორე კონვერტში-ფასების ცხრილი, რომლებიც უნდა შეესაბამებოდეს სატენდერო დოკუმენტაციის 2-ე მუხლის მოთხოვნებს.
4.2. კონვერტზე სავალდებულოა პოტენციური მიმწოდებლის სახელწოდებისა და მისამართის მითითება, აგრეთვე მასზე აღნიშნული უნდა იყოს: შპს "თბილისი ენერჯისათვის" ვირტუალური დესკტოპ ინფრასტრუქტურის შესყიდვის ტენდერი", კონვერტი 1 ტექნიკური შეთავაზება, კონვერტი 2 კომერციული შეთავაზება.
4.3. შემსყიდველისათვის წარდგენილი დოკუმენტები დამოწმებული უნდა იყოს პოტენციური მიმწოდებლის ბეჭდით (თუ იგი სარგებლობს ბეჭდით).
4.4. სატენდერო განაცხადში ფასები მიეთითება ლარში.
4.5. სატენდერო განაცხადი შემსყიდველს წარედგინება 2023 წლის 28 ივლისის 17:00 საათამდე (შემდგომში - "საბოლოო ვადა"), შემდეგ მისამართზე: ქ. თბილისი, მიცკევიჩის ქ. №18ა, შპს "თბილისი ენერჯის" კანცელარია. კანცელარიაში პოტენციური მიმწოდებლის სატენდერო განაცხადის მიღებისას აუცილებელია განაცხადის უშუალო მომწოდებლის პირადობის დამადასტურებელი დოკუმენტის ასლის დართვა მისაღებ დოკუმენტაციასთან ერთად, რომელზეც დაფიქსირდება დოკუმენტაციის წარმოდგენის ზუსტი თარიღი და დრო.
4.6. სატენდერო კომისიის მიერ არ განიხილება პოტენციური მიმწოდებლების (პრეტენდენტების) მიერ ვადების დარღვევით წარდგენილ სატენდერო განაცხადი.
4.7. პოტენციური მიმწოდებელი (პრეტენდენტი) გაიღებს ყველა ხარჯს, რომელიც დაკავშირებულია მისი სატენდერო განაცხადის მომზადებასა და წარდგენასთან. საზოგადოებასა და სატენდერო კომისიას არ ეკისრებათ ამ ხარჯების ანაზღაურების ვალდებულება, მიუხედავად ტენდერის ჩატარების შედეგებისა.
4.8. პოტენციური მიმწოდებელი (პრეტენდენტი) ვალდებულია მიუთითოს თავის სატენდერო განაცხადში მისი მოქმედების ვადა. სატენდერო განაცხადები რჩება ძალაში იმ პერიოდის განმავლობაში, რომელიც მითითებულია სატენდერო დოკუმენტაციაში, მაგრამ არანაკლებ 15 (თხუთმეტი) დღისა სატენდერო განაცხადების შემცველი კონვერტების გახსნის თარიღის შემდეგ. სატენდერო განაცხადი, რომელზეც მითითებულია უფრო ნაკლები მოქმედების ვადა, ვიდრე ეს მოთხოვნილია სატენდერო დოკუმენტაციით, განიხილება, როგორც სატენდერო დოკუმენტაციის მოთხოვნებთან შეუსაბამო.
4.9. სატენდერო განაცხადების მოქმედების ვადის ამოწურვამდე სატენდერო კომისიას შეუძლია სთხოვოს პოტენციურ მიმწოდებელს (პრეტენდენტს) დამატებით გააგრძელოს აღნიშნული ვადა კონკრეტული დროის პერიოდზე. პოტენციურ მიმწოდებელს (პრეტენდენტს) შეუძლია უარი თქვას აღნიშნული თხოვნის დაკმაყოფილებაზე და ამასთან.
4.10. პოტენციურ მიმწოდებელს უფლება აქვს შეცვალოს ან გაიხმოს თავისი სატენდერო განაცხადი სატენდერო განაცხადების წარდგენისათვის დადგენილი საბოლოო ვადის გასვლამდე.
4.11. შემსყიდველი უფლებამოსილია, პოტენციური მიმწოდებლის წერილობითი თხოვნის საფუძველზე ან თავისი ინიციატივით, განმარტოს/დააზუსტოს სატენდერო დოკუმენტაციაში მითითებული ინფორმაცია, რაც ფორმდება სატენდერო დოკუმენტაციის დამატების სახით და ეგზავნება ყველა პოტენციურ მიმწოდებელს საკვალიფიკაციო მონაცემების დამადასტურებელი დოკუმენტებისა და სატენდერო წინადადებების მიღების ვადის დასრულებამდე არა უგვიანეს 5 კალენდარული დღისა.

5. სატენდერო განაცხადების შემცველი კონვერტის გახსნა, სატენდერო განაცხადის განხილვა და შეფასება

5.1. კონვერტი 1, რომლებშიც მოთავსებულია სატენდერო დოკუმენტაციის 3.1. პუნქტის ა) და ბ) ქვეპუნქტებით მოთხოვნილი დოკუმენტაცია, სავარაუდოდ გაიხსნება 2023 წლის 31 ივლისს.
5.2. სატენდერო კომისია არ განიხილავს შეფასებისთვის სატენდერო განაცხადს, თუ:

ა) სატენდერო განაცხადის წარმდგენი პოტენციური მიმწოდებელი (პრეტენდენტი) ვერ აკმაყოფილებს საკვალიფიკაციო მოთხოვნებს;
ბ) მოცემული სატენდერო განაცხადი არ პასუხობს სატენდერო დოკუმენტაციის მოთხოვნებს;
გ) სატენდერო განაცხადი არ არის გაფორმებული და დამოწმებული დადგენილი წესით;
5.3. პოტენციური მიმწოდებლის მცდელობა ზეწოლა მოახდინოს სატენდერო კომისიის საქმიანობაზე, წარმოადგენს მისი დისკვალიფიკაციის საფუძველს.
5.4. სატენდერო კომისია აჯამებს ტენდერის შედეგებს სატენდერო განაცხადების შემცველი კონვერტების გახსნის თარიღიდან არა უგვიანეს 15 დღისა.
5.5 სატენდერო კომისია უფლებამოსილია არ განიხილოს მიღებული განაცხადები, უარი განაცხადოს გამარჯვებულის გამოვლენაზე და გამოაცხადოს ტენდერი არშემდგარად, თუ მიმწოდებელთა მიერ შეთავაზებული ფასი და შესყიდვის ობიექტის სხვა მახასიათებლები არ შეესაბამება შემსყიდველის მოთხოვნებს.

6. შესყიდვის ხელშეკრულების დადება

6.1. ტენდერით შერჩეულ (გამარჯვებულ) პოტენციურ მიმწოდებელთან (პრეტენდენტთან) ფორმდება შესყიდვის ხელშეკრულება საქართველოს კანონმდებლობის შესაბამისად.
6.2. ტენდერით შერჩეული (გამარჯვებული) პოტენციური მიმწოდებელი (პრეტენდენტი) გამარჯვებულად გამოცხადების შესახებ შეტყობინებისა და შესყიდვის ხელშეკრულების პროექტის გადაცემიდან 2 (ორი) სამუშაო დღის ვადაში ხელს აწერს ხელშეკრულებას.
6.3. თუ მიმწოდებელი გამოცხადებულია ტენდერის გამარჯვებულად და იგი ხელს არ აწერს შესყიდვის ხელშეკრულებას ამ მუხლის 6.2. პუნქტით განსაზღვრულ ვადაში, შემსყიდველი უფლებამოსილია დადოს შესყიდვის ხელშეკრულება ტენდერის სხვა მონაწილესთან, რომლის წინადადება, ამ სატენდერო დოკუმენტაციით განსაზღვრული კრიტერიუმების გათვალისწინებით, წარმოადგენს ყველაზე უფრო ხელსაყრელს გამარჯვებულის წინადადების შემდეგ, რაც დასტურდება ტენდერის შედეგების ოქმით.
6.4. არ დაიშვება ცვლილებების ან/და ახალი პირობების შეტანა შესყიდვის ხელშეკრულების პროექტში ან ხელმოწერილ შესყიდვის ხელშეკრულებაში (გარდა ფასის შემცირებისა), რამაც შესაძლებელია შეცვალოს იმ წინადადების შინაარსი, რომელიც წარმოადგენს მიმწოდებლის შერჩევის საფუძველს. დასაშვებია ცვლილებების შეტანა შესყიდვის ხელშეკრულების პროექტში ან ხელმოწერილ შესყიდვის ხელშეკრულებაში ფასის შემცირების ნაწილში იმ პირობით, რომ ხარისხი, მოცულობა და სხვა პირობები, რაც წარმოადგენს მიმწოდებლის შერჩევის საფუძველს, დარჩება უცვლელი.
6.5. შესყიდვის ხელშეკრულების ხელმოწერამდე შემსყიდველი უფლებამოსილია აწარმოოს მოლაპარაკებები ტენდერში გამარჯვებულ პოტენციურ მიმწოდებელთან (პრეტენდენტთან) ხელშეკრულების ფასის შემცირების თაობაზე.
6.6. იმ შემთხვევაში, თუ შესყიდვების ხელშეკრულების განხორციელების პროცესში შესაბამის საქონელზე შემცირდა ფასები, შემსყიდველისა და მიმწოდებლის ურთიერთშეთანხმების საფუძველზე შესყიდვების ხელშეკრულებაში შესაძლებელია შეტანილი იქნეს შესაბამისი ცვლილება ფასის შემცირების თაობაზე.

ტექნიკური შეფასების კრიტერიუმები და პირობები დანართი #1

მიღებულ შემოთავაზებებს შემსყიდველი აფასებს შემდეგ კრიტერიუმების საფუძველზე.

წარმოდგენილი საბუთები უნდა შეიცავდეს ინფორმაციას გამარჯვებულის გამოვლენის შემდეგ ხელშეკრულების გასაფორმებელად.

კომერციული შეფასების დროს განიხილება მხოლოდ ის ტექნიკური შეთავაზებები, რომლებიც შეესაბამება ტექნიკური შეფასების კრიტერიუმებს და პირობებს.

№	კრიტერიუმი	მოთხოვნილი საბუთები	კრიტერიუმების გამოვლენის და შეფასების პირობები
1.	ტექნიკური შემოთავაზება	• ტექნიკური შეთავაზების წერილი	ტექნიკური შეთავაზების წერილი შინაარსის შეუცვლელად, უნდა იყოს უფლებამოსილი პირის მიერ ხელმოწერილი, დალუქული და დათარიღებული.
1.1.	შესაბამისი გამოცდილება	• **ფორმა 1: მსგავსი სამუშაო გამოცდილება** ○ მიღება-ჩაბარების აქტები (დასრულებული პროექტებისთვის) ○ ხელშეკრულებები ○ პორტფოლიო საბუთები: - კომპანიის ზოგადი პროტფოლიო (ვებგვერდი)	უნდა მომზადდეს დეტალური ინფორმაცია პროექტის დავალების საბუთში მითითებული 2 მსგავსი დასრულებული ან მიმდინარე (70%-ით დასრულებული) პროექტის შესახებ ბოლო 5 წლის განმავლობაში. პროექტების მსგავსების შესაფასებლად, ინფორმაციას თან უნდა დაერთოს ხელშეკრულებები და მიღება-ჩაბარების აქტები თითოეული შესრულებული სამუშაოსთვის.
1.2.	მონაწილეობის კრიტერიუმები	• **ფორმა 3** ○ საჯარო რეესტრის ეროვნული სააგენტო - ამონაწერი მეწარმეთა და არასამეწარმეო იურიდიული პირების რეესტრიდან. ეს საბუთი შეიცავს: ინფორმაციას ლიკვიდაციის, რეორგანიზაციის, გადახდისუუნარობის, ასევე ყადაღის, აკრძალვის, გირაოსა და თავდებობის შესახებ.	ტენდერში მონაწილეობის მისაღებად ვენდორი უდნა იყოს გადახდისუნარიანი, არ უნდა იმყოფებოდეს ლიკვიდაციაში, მის ქონებას არ უნდა ედოს ყადაღა, მისი ეკონომიკურ-ფინანსური აქტივობა არ უნდა იყოს შეჩერებული საქართველოს კანონმდებლობით დადგენილი წესის მიხედვით.
1.3.	მონაწილეობის კრიტერიუმები	• **ფორმა 4** ○ შემოსავლების სამსახური – ამონაწერი საბიუჯეტო ან/და საკრედიტო ინსტიტუტებისადმი ვადაგადაცილებული დავალიანების შესახებ.	ტენდერში მონაწილეობის მისაღებად ვენდორს არ უნდა ჰქონდეს ვადაგადაცილებული საბიუჯეტო დავალიანება.

ტექნიკური შეთავაზების წერილი

შპს „თბილისი ენერჯი“-ს:

ჩვენ, ქვემოთ ხელის მომწერნი ვაცხადებთ:

(a) **უცვლელობა:** ჩვენ განვიხილეთ სატენდერო დოკუმენტი ყველა მიმაგრებული ფაილის ჩათვლით, სრულიად ვაცნობიერებთ ვირტუალური დესკტოპ ინფრასტრუქტურის მიწოდების პირობებს, რომელიც ამ დოკუმენტებით არის დამტკიცებული და მათში ცვლილებები არ შეგვაქვს;

(b) **დაშვების უფლება:** ჩვენ არ ვარღვევთ ტენდერში დაშვების მოთხოვნებს და ვადასტურებთ, რომ არ არსებობს ინტერესთა კონფლიქტი;

(c) **ტექნიკური შესაბამისობა:** ჩვენ გთავაზობთ ლიცენზიების მიწოდებას სატენდერო მოთხოვნების შესაბამისად.

(d) **შეთავაზების მოქმედების ვადა**: ჩვენი ტექნიკური და კომერციული შემოთავაზება ძალაშია წინადადების წარდგენისთვის განსაზღვრული საბოლოო თარიღიდან *15 დღის* განმავლობაში (ან, საჭიროების შემთხვევაში, გადაანგარიშდება შეცვლილი თარიღის მიხედვით), და უცვლელი სახით ძალაში დარჩება აღნიშნული პერიოდის განმავლობაში.

(e) **ხელშეკრულება:** ჩვენ ვაცნობიერებთ, რომ ჩვენი წინადადება თქვენს დასტურთან ერთად წარმოადგენს სავალდებულო ძალის მქონე დოკუმენტს ოფიციალური ხელშეკრულების გაფორმებამდე. ტენდერის დოკუმენტაციაში წარმოდგენილი ხელშეკრულების შაბლონში (მონიშნეთ “X” სიმბოლოთი შემდეგი დებულებები);

( ) ჩვენ არ შეგვაქვს ცვლილებები

( ) შეგვაქვს ცვლილებები (ჩამატებულია ხელშეკრულებაში)

(f) **წინადადების მიღების არასავალდებულოობა**: ჩვენ ვაცნობიერებთ, რომ თქვენ არ ხართ ვალდებული მიიღოთ ყველაზე დაბალი ფასის, ტექნიკური პირობებით ყველაზე მეტად შესაფერისი ან ნებისმიერი სხვა სახის წინადადება.

(g) **თაღლითობა და კორუფცია:** ვადასტურებთ, რომ მიღებული გვაქვს თაღლითობისა და კორუფციის აღმკვეთი ყველა შესაძლო ზომა და გარწმუნებთ, რომ ჩვენი სახელით მოქმედი არც ერთი პიროვნება არ არის გარეული თაღლითობასა და კორუფციაში.

სახელი და გვარი: _____

თანამდებობა: _____

ხელმოწერა და ბეჭედი: _____

უფლებამოსილია ხელი მოაწეროს წინადადებას კომპანიის სახელით ___*(პრეტენდენტის სრული დასახელება)*___ .

თარიღი: _____

ფორმა 1: მსგავსი სამუშაოების შესრულების გამოცდილება

No	დაწყებისა და დასრულების თარიღი[1]	შემსყიდველი / საკონტაქტო პიროვნება / საკონტაქტო ნომერი	შესრულებული სამუშაოს დეტალური აღწერა (ადგილმდებარეობა, ძირითადი შემადგენელი ნაწილები, რაოდენობა/მოცულობა) და მოთხოვნილ სამუშაოსთან შესაბამისობის აღწერა	ხელშეკრულების ღირებულება *(USD)*	დასრულების პროცენტული მაჩვენებელი[2]
1.					
2.					
3.					
4.					
5.					

შენიშვნა: ფორმას თან უნდა ახლდეს მხარეთა მიერ დამოწმებული მიღება-ჩაბარების აქტები, რომლებშიც გაწერილი იქნება დასრულებული სამუშაოების დეტალები/მოცულობა ან მიმდინარე სამუშაოებისთვის საბოლოო შესრულების აქტები.

[1] ჩასვით თვე და რიცხვი

[2] თუ სამუშაო მიმდინარეა, %-ის საშუალებით მიუთითეთ ამ სამუშაოს რა ნაწილი არის დასრულებული (დასაშვებია მინიმუმ 80%-იანი შესრულების მითითება)

ტექნიკური დავალება

VDI - Virtual Desktop Infrastructure გადაწყვეტილების ტექნიკური მოთხოვნები

- მომხმარებლების რაოდენობა - არანაკლებ 500 (200 x persistence, 300 x non-persistence)

მომხმარებლების ტიპები და პროფილები:

500 მომხმარებელი				
Clients - General	**vCPU**	**vRAM**	**vDisk**	AMD
460	**(4 - 1/4)**	**8**	**100**	
	AMD			
Clients - Graphics	**vCPU**	**vRAM**	**vDisk**	
40	**(8 - 1/2)**	**16**	**100**	vWS
	GPU			40

- გადაწყვეტილება უნდა ეფუძნებოდეს VSAN ready stretch cluster - ის ტექნოლოგიას.
- გადაწყვეტილება უნდა დაინერგოს გეოგრაფიულად დაშორებულ ორ Data Centre - ში. VDI - მომხმარებლების ბალანსირება შესაძლებელი უნდა იყოს ორივე Data Centre - ში. ერთი Data Centre - ის პირობებში VSAN კლასტერის დატვირთვა გათვლილი უნდა იყოს არანაკლებ 90% - ზე.
- გადაწყვეტილება უნდა იყოს VMware Horizon - ის არქიტექტურაზე დაფუძნებული.
- გადაწყვეტილება უნდა იყოს სრულად ცენტრალიზებული.

მოთხოვნები სერვერების მიმართ:

ატიპიკური სერვერი - არანაკლებ ოდენობა	
HPE DL385 Gen11 GPU CTO Svr	2
AMD EPYC 9654 2.4GHz 96-core 360W Processor	4
HPE 64GB (1x64GB) Dual Rank x4 DDR5-4800 CAS-40-39-39 EC8 Registered Smart Memory Kit	48
HPE ProLiant DL3X5 Gen11 GPU 8SFF U.3 FIO Backplane Kit	2
HPE 1.6TB NVMe Gen4 Mainstream Performance Mixed Use SFF BC U.3 Static Multi Vendor SSD	2
HPE 3.84TB NVMe Gen4 Mainstream Performance Read Intensive SFF BC U.3 Static Multi Vendor SSD	6
Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	4
HPE 25Gb SFP28 SR 100m Transceiver	8
HPE 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit	4
HPE ProLiant DL385 Gen11 4 Double Wide GPU FIO Enablement Kit	2
HPE ProLiant DL385 Gen11 CPU 8-pin GPU Power Cable From Power Distribution Board	2
HPE ProLiant DL385 Gen11 2U High Performance FIO Air Baffle Kit	2
HPE ProLiant DL3X5 Gen11 2U Performance Fan Kit	12
HPE Bezel Lock Kit	2
HPE Gen11 2U Bezel Kit	2
HPE DL38X Gen10 Plus 2U Cable Management Arm for Rail Kit	2
HPE NS204i-u Gen11 NVMe Hot Plug Boot Optimized Storage Device	2
HPE Ball Bearing Rail 8 Kit	2
HPE ProLiant DL3X5 Gen11 Secondary NS204i-u NVMe Hot Plug Boot Device Enablement Kit	2
HPE ProLiant DL385 Gen11 Power Distribution Board Kit	2
HPE ProLiant DL3X5 Gen11 Max Performance 2U Heat Sink Kit	4
HPE ProLiant vSAN Original Storage Architecture Tracking	2

HPE OneView including 3yr 24x7 Support Flexible Quantity E-LTU	2
HPE 3Y Tech Care Basic Service	1
HPE DL385 GEN11 Support	2

B ტიპის სერვერი - არანაკლებ ორი ცალი	
HPE DL385 Gen11 GPU CTO Svr	2
HPEDL385Gen11GPUCTOServer	2
AMD EPYC 9654 2.4GHz 96-core 360W Processor for HPE	4
HPE 64GB (1x64GB) Dual Rank x4 DDR5-4800 CAS-40-39-39 EC8 Registered Smart Memory Kit	48
HPE ProLiant DL3X5 Gen11 GPU 8SFF U.3 FIO Backplane Kit	2
HPE 1.6TB NVMe Gen4 Mainstream Performance Mixed Use SFF BC U.3 Static Multi Vendor SSD	2
HPE 3.84TB NVMe Gen4 Mainstream Performance Read Intensive SFF BC U.3 Static Multi Vendor SSD	6
Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	4
HPE 25Gb SFP28 SR 100m Transceiver	8
HPE 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit	4
HPE ProLiant DL385 Gen11 4 Double Wide GPU FIO Enablement Kit	2
HPE ProLiant DL385 Gen11 CPU 8-pin GPU Power Cable From Power Distribution Board	2
HPE ProLiant DL385 Gen11 2U High Performance FIO Air Baffle Kit	2
HPE ProLiant DL3X5 Gen11 2U Performance Fan Kit	12
NVIDIA L40 48GB PCIe Accelerator for HPE	2
HPE Bezel Lock Kit	2
HPE Gen11 2U Bezel Kit	2
HPE DL38X Gen10 Plus 2U Cable Management Arm for Rail Kit	2
HPE NS204i-u Gen11 NVMe Hot Plug Boot Optimized Storage Device	2
HPE Ball Bearing Rail 8 Kit	2
HPE ProLiant DL3X5 Gen11 Secondary NS204i-u NVMe Hot Plug Boot Device Enablement Kit	2
HPE ProLiant DL385 Gen11 Power Distribution Board Kit	2
HPE ProLiant DL3X5 Gen11 Max Performance 2U Heat Sink Kit	4
HPE ProLiant vSAN Original Storage Architecture Tracking	2
HPE OneView including 3yr 24x7 Support Flexible Quantity E-LTU	2
HPE 3Y Tech Care Basic Service	1
HPE DL385 GEN11 Support	2

C ტიპის სერვერი - არანაკლებ ოთხი ცალი	
HPE DL385 Gen11 GPU CTO Svr	4
HPEDL385Gen11GPUCTOServer	4
AMD EPYC 9654 2.4GHz 96-core 360W Processor for HPE	8
HPE 64GB (1x64GB) Dual Rank x4 DDR5-4800 CAS-40-39-39 EC8 Registered Smart Memory Kit	96
HPE ProLiant DL3X5 Gen11 GPU 8SFF U.3 FIO Backplane Kit	4
HPE 1.6TB NVMe Gen4 Mainstream Performance Mixed Use SFF BC U.3 Static Multi Vendor SSD	4
HPE 3.84TB NVMe Gen4 Mainstream Performance Read Intensive SFF BC U.3 Static Multi Vendor SSD	12
Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	8
HPE 25Gb SFP28 SR 100m Transceiver	16
HPE 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit	8
HPE ProLiant DL385 Gen11 4 Double Wide GPU FIO Enablement Kit	4
HPE ProLiant DL385 Gen11 CPU 8-pin GPU Power Cable From Power Distribution Board	4

HPE ProLiant DL385 Gen11 2U High Performance FIO Air Baffle Kit	4
HPE ProLiant DL3X5 Gen11 2U Performance Fan Kit	24
NVIDIA L40 48GB PCIe Accelerator for HPE	8
HPE Bezel Lock Kit	4
HPE Gen11 2U Bezel Kit	4
HPE DL38X Gen10 Plus 2U Cable Management Arm for Rail Kit	4
HPE NS204i-u Gen11 NVMe Hot Plug Boot Optimized Storage Device	4
HPE Ball Bearing Rail 8 Kit	4
HPE ProLiant DL3X5 Gen11 Secondary NS204i-u NVMe Hot Plug Boot Device Enablement Kit	4
HPE ProLiant DL385 Gen11 Power Distribution Board Kit	4
HPE ProLiant DL3X5 Gen11 Max Performance 2U Heat Sink Kit	8
HPE ProLiant vSAN Original Storage Architecture Tracking	4
HPE OneView including 3yr 24x7 Support Flexible Quantity E-LTU	4
HPE 3Y Tech Care Basic Service	1
HPE DL385 GEN11 Support	4

მოთხოვნები ვირტუალიზაციის მიმართ

- VMware Horizon Enterprise Term 10-pack Concurrent Users 3-year - არანაკლებ 50
- NVIDIA RTX Virtual Workstation 1 Concurrent User 3-year Subscription - არანაკლებ 40 ცალ

მოთხოვნები ტრაფიკის ბალანსერის მიმართ:

Solution technical requirements

1. General requirements

1.1. Solution manufacturer must be present on the Application Delivery Controllers (ADC) market for at least 10 years.
1.2. Hardware and virtual solutions must have same functionality;
1.3. Support for the same SSL/TLS encryption settings on physical and virtual devices of the solution manufacturer.
1.4. Special license must be available in vendor portfolio for the test environment.
1.5. The existence of successful implementations of the balancer in Georgia.
1.6. Availability of a support center in region for at least the last 4 years with the possibility of providing support in English and Russian language;
1.7. The supplier or distributor must have at least two expert-level engineers confirmed by relevant certificates.
1.8. The supplier or distributor must have at least two load balancing specialist -level engineers confirmed by relevant certificates.
1.9. The supplier or distributor must have at least five administrator-level engineers confirmed by relevant certificates.
1.10. 24x7 support for 3 year;
1.11. Closest support center must be with maximum 2-hour time zone with Tbilisi with certified specialist as requested in previous bullets.
1.12. Providing support in English and Russian.
1.13. The presence of accredited by the manufacturer training center with the possibility of training in English and Russian.
1.14. Online training for 3 people which cover administration, load balancing and troubleshooting must be included.
1.15. Availability of an authorization letter from the manufacturer of the solution.

2. Virtual solution performance requirements

2.1. Virtual machine requirements

2.1.1. Hypervisor support: VMware ESXi, KVM, Microsoft Hyper-V.

2.1.2. Public cloud deployment support: AWS, Google Cloud, IBM Cloud, Microsoft Azure, Oracle Cloud.

2.1.3. The implementation of all functions must be performed within a single VM.

2.1.4. Solution must propose of 2 VMs as cluster;

2.1.5. Ability to migrate all settings to "per core" license type up to 24 vCPU or "per app" license types with no functional limitation;

2.1.6. VM License must support reactivation on another virtual machine on the local DC hypervisor and in the public cloud.

2.1.7. The virtual machine must support SR-IOV.

2.1.8. Virtual machine must support minimum 8 vCPU with no RAM and storage license limitation;

2.2. Throughput:

2.2.1. OSI L4 throughput - 10 Gbit / s

2.2.2. OSI L7 throughput – 10 Gbit / s

2.2.3. The number of TCP connections per second – 4000 as minimum with the possibility of increasing to 135,000. This number must not be limited by license.

2.2.4. The maximum number of simultaneous TCP sessions – 1,000,000 as minimum which can be increased up to 10,000,000. This number must not be limited by license.

2.2.5. The number of requests L7 level per second – 3000 as minimum with the possibility of increasing to 450,000. This number must not be limited by license.

2.3. Compressed throughput:

2.3.1. Compression Performance – 1 Gbit/s
2.3.2. VM must support optional hardware compression.

2.4. SSL/TLS performance:

2.4.1. SSL/TLS traffic encryption performance - 1 Gbit/s
2.4.2. SSL/TLS TPS performance (2k keys) – 900 TPS, upgradable to 3,800 TPS.
2.4.3. TLS 1.3 support.
2.4.4. SSL/TLS TPS must not be limit by license.
2.4.5. VM must support optional hardware crypto module as an option for future needs.
2.4.6. VM must support optional HSM module as an option for future needs.

3. Solution management

3.1. Solutions settings may modified both from the GUI-console and the CLI-console.
3.2. The control subsystem can be isolated from the traffic processing subsystem.
3.3. API interface for management.
3.4. Interface management is responsible for trimming IPv4 and IPv6
3.5. Solution must be able to do device analytics for uploading to vendor analyzer for rapid security analysis and best practice advice

4. Clustering and scaling

4.1. Failover Active/Passive and Active/Active schemes support;

4.2. Maximum number of devices/VM in cluster for config sync is 32;
4.3. Must support Load Sharing mode;
4.4. Maximum number of devices/VM in cluster for load sharing is 8;
4.5. Solution must support physical and virtual buildings in same cluster;
4.6. Solution must support combining different HW or VE licenses into a single cluster.
4.7. Solution must sync session data (L2, L3, L4 and HTTP OSI metrics) to sustain session when cluster failover.
4.8. Solution must sync load balancing data to sustain session when cluster failover.
4.9. The Graceful Shutdown load balancing server mechanism must supported.
4.10. Solution must support manual and/or auto configuration sync in cluster.
4.11. Solution OS family must be on market at least for 5 years.

5. Network connectivity requirements

5.1. L2 OSI requirements

5.1.1. Support for 802.1q VLAN, VLAN Groups.

5.1.2. STP support.

5.1.3. LACP support.

5.1.4. LLDP support.

5.1.5. Support VXLAN, NVGRE.

5.1.6. Support L2TP, PPP, PPP.

5.2. L3 OSI requirements

5.2.1. Support for IPv4 and IPv6, IPX/SPX.
5.2.2. NAT, PAT, SNAT support.
5.2.3. Support lan-to-lan IPSEC, GRE tunneling.
5.2.4. QoS support.
5.2.5. WCCP support.
5.2.6. Supports packet filtering function.

5.3. Routing

5.3.1. Solution must support dynamic routing protocols as an option for future needs:
- BGP.
- OSPF.
- IS-IS.
- RIP.

5.3.2. VRF support.
5.3.3. VRRP support.
5.3.4. Static routing. An isolated routing table must be provided for the management interface.

6. System functions requirements

6.1. Solution modules management

6.1.1. It should be possible to add/remove functional modules of the solution.
6.1.2. Addition/removal of functional modules must take place without changing the hardware or VE configuration.
6.1.3. Adding/removing functional modules must be done without the need to install additional software.
6.1.4. Guaranteed allocation of resources for each functional module must be supported.

6.1.5. Resource usage control must be supported when adding/removing functional modules.
6.1.6. A geolocation database must be maintained without the need for any additional licenses and provide regular updates on the manufacturer's website.

6.2. Management of SSL/TLS certificates

6.2.1. It should be possible to add/remove certificates for SSL traffic.
6.2.2. It should be possible to monitor the status of SSL traffic certificates.
6.2.3. Solution must support HSM modules for future needs as optional licence.

6.3. A role model for system users (RBAC)

6.3.1. User directory:
- Integration with LDAP must be supported.
- RADIUS integration should be supported.
- Integration with TACACS+ should be supported.
- Integration with Microsoft AD must be supported.
- Integration with ClientCert LDAP must be supported.
- A local user directory must be provided.

6.3.2. A mechanism for assigning user roles to access the solution must be provided.
6.3.3. A mechanism for dividing the change at the logical level with granting access rights to it must be provided.
6.3.4. It is necessary to ensure the division of the device into several administrative sections for access by different groups to administrate different application;

6.4. Management of system logs

6.4.1. It should be possible to download system logs in real-time to third-party software.
6.4.2. Log filtering rules must be provided.
6.4.3. A mechanism for different user access roles to system logs must be supported.
6.4.4. The functionality to manage the configuration of the syslog message level from both the GUI interface and the CLI interface must be supported.
6.4.5. System log management must be provided for each individual solution module.
6.4.6. You need to support the mechanism for creating custom logs using the built-in scripting language.

6.5. Management of system configuration backups

6.5.1. Must support an archive creation of the entire solution configuration from the GUI and/or CLI.
6.5.2. Must support different versions of the configuration archive creation.
6.5.3. Must support configuration archives management (creation, deletion, export, import).

7. System monitoring

7.1. System performance reporting must be provided with the following parameters:
- RAM in use.
- CPU in use.
- Cache memory.
- Number of active sessions, new sessions.
- Used bandwidth in bits/s, packets/s.
- Number of HTTP requests.
- Number of SSL/TLS transactions.

7.2. It must be possible to monitor the solution by third-party software.
7.3. The following monitoring protocols must be supported:
- SNMP v1/2/3, SNMP Traps.
- sFlow

7.4. Ability to monitor the status of published/protected/load balanced applications using system monitoring protocols.

8. Traffic steering and setting apply.

8.1. Possibility of independent application of settings both on the client and server side according to the following criteria:
- IP
- TCP/UDP
- HTTP
- HTTP/2
- LDAP
- WebSocket

8.2. Must support pre-configured templates with best practice configuration for various using the solution scenarios, for example WAN network, LAN network, mobile network.

8.3. The ability to apply individual traffic processing rules based on, but not limited to, the criteria in this subsection.

9. SSL/TLS traffic processing

9.1. An SSL/TLS Offload mechanism should be provided, which will allow transferring the process of encryption/decryption of traffic to the user from the proposed solution.

9.2. Ability to apply different encryption settings on the client and server side.

9.3. The SSL processing mechanism must be implemented at the cpu level by means of the proposed solution with option to add hardware crypto device.

9.4. The ability to offload SSL traffic processing to optional hardware-accelerated devices as part of the failover scheme must be supported.

9.5. It should be possible to send decrypted ICAP traffic by analyzing it.

9.6. Individual rules for working with SSL/TLS traffic and routing to analysis tools based on FQDN and/or IP address should be provided.

9.7. It should be possible to use third-party certificate centers (Microsoft PKI).

9.8. The subsystem for protection against targeted and zero-day attacks must be integrated with the SSL inspection subsystem.

10. Load balancing requirements

10.1. Load balancing modes

10.1.1. The following modes of load balancing should be provided:

- **Standard application load balancing mode, which allows user sessions to be terminated separately from server sessions.**
- **L2 OSI level request forwarding mode.**
- **L3 OSI level request forwarding mode.**
- **L4 OSI level requests forwarding.**
- **HTTP requests forwarding.**
- **Packet protocol balancing mode.**

10.2. Load balancing methods

10.2.1. The system must support balancing methods both per application balancing and/or per server.

10.2.2. A Round Robin balancing mechanism must be provided.

10.2.3. A Round Robin balancing mechanism should be provided with priority for server and/or load balanced app.

10.2.4. A balancing mechanism should be provided with performance tracking based on cpu, ram, disk utilization parameters with appropriate weighting for server and/or load balanced app.

10.2.5. A balancing mechanism should be provided to track the number of sessions for server and/or load balanced app.

10.2.6. A balancing mechanism should be provided, tracking the number of sessions and using priorities for server and/or load balanced app.

10.2.7. A balancing mechanism with server response time tracking must be provided.

10.2.8. A self-learning balancing mechanism must be provided.

10.2.9. It should be possible to connect backup servers for balancing.

10.2.10. A mechanism for creating custom load balancing algorithms must be supported.

10.3. Load balancing objects monitoring.

10.3.1. The following monitoring types for load balancing objects must supported:

- Diameter
- DNS
- FTP
- Gateway
- HTTP

- HTTPS
- ICMP
- IMAP
- LDAP
- MQTT
- In band
- LDAP
- MQTT
- MSSQL
- MySQL
- NNTP
- POP3
- Oracle
- PostgreSQL
- Radius
- Radius Account
- Real Server
- RPC
- SASP
- SIP
- SMB
- SMTP
- SNMP DCA
- SNMP DCA Base
- SOAP
- TCP
- TCP Echo
- UDP
- WAP
- WMI

10.3.2. Must support custom scripts for checking the status of the monitoring object (for example, using cURL or netcat to access the server)

10.3.3. Must support custom application monitoring methods.

10.3.4. The Must support administrator debugging to check monitoring operation of the monitor on any IP:PORT without apply it on the application/server.

10.3.5. A Graceful Shutdown mechanism should be provided for active user sessions when load balancing object need to be removed from the balancing process.

10.4. Sessions bind to a load balanced server.

10.4.1. Must support binding sessions to the server using source and recipient IP addresses.

10.4.2. Must support binding sessions to the server using the session identifier.

10.4.3. Must support binding sessions to the server using an SSL session ID.

10.4.4. Must support binding to the server using the Cookie mechanism.

10.4.5. Must support binding sessions to the server using the SIP.

10.4.6. Session-to-server binding functionality must be provided for MSRDP sessions.

10.4.7. Must support custom created algorithms for binding user to the balanced server.

10.5. Traffic optimization

10.5.1. Must support HTTP traffic compression mechanisms.

10.5.2. Must support HTTP traffic optional compression coprocessor for hardware level compression.

10.5.3. Must support request aggregating from different users into one session to the load balanced server.

10.5.4. Must support SPDY.

10.5.5. Must support caching for frequently used content.

10.6. Setup, management and traffic management flexibility

10.6.1. All load balancing settings must be applied based on FQDN and/or IP and/or payload information.
10.6.2. Must support mechanism for creating and managing custom rules and scenarios for traffic processing.
10.6.3. Must support mechanism for creating and managing specialized load balancing rules and scenarios.
10.6.4. Must support mechanism for creating and managing specialized bindings of sessions to servers.
10.6.5. Must support specialized sets of traffic manipulation technics and traffic content.

11. Solution must support functional upgrade for GSLB level load balancing. Upgrade reequipments.

11.1. DNS relay

11.1.1. DNS database caching mechanism in RAM must be supported.

11.1.2. The DNS caching mechanism in transparent mode must be supported.

11.1.3. A mechanism for delegating the parent DNS zone to child sub-domains must be supported.

11.1.4. The automatic DNS reverse lookup mechanism must be supported.

11.1.5. The NAPTR record management mechanism must be supported.

11.1.6. Should support DNS64 "out of the box" without needing to use scripts.

11.2. ISP links check

11.2.1. The following mechanisms for checking should be supported:

- **SNMP**
- **Gateway ICMP**

11.3. GSLB (global server load balancing)

11.3.1. The following mechanisms for checking connection status should be supported:

- **Round robin**
- **Ratio**
- **Statically specified server.**
- **First available server.**
- **LDNS binding to a specific server.**
- **Based on physical location.**
- **Based on the available number of servers in the pool.**
- **Server selection based on the least number of failed responses**
- **Selection of the server with the lowest CPU load.**
- **Selection of the server with the least number of hops from LDNS.**
- **Selection of the server with the lowest kilobyte/s load.**
- **Selecting the server with the least number of connections.**
- **Selection of the server with the lowest packet/s load.**
- **Selecting the server with the fastest RTT.**

11.3.2. The solution should have a built-in system of health check services for making a balancing decision.

11.3.3. The solution should have a mechanism for calling a health check both inside and outside the data center.

11.3.4. The solution should support such mechanisms of health check services Gateway ICMP

- ICMP
- TCP Echo
- TCP Half Open
- TCP
- UDP
- HTTP
- HTTPS Diameter
- Inband
- NNTPMSSQL
- MQTT
- MySQL
- Oracle
- PostgreSQL
- RADIUS
- RADIUS Accounting
- RPC
- SASP
- SIP
- SMB

- SOAP
- DNS
- LDAP
- SMTP
- POP3
- WAP
- Ability to create a non-standard monitor

11.4. A mechanism for incrementally updating the GSLB configuration must be supported.

11.5. A mechanism for selecting a backup server pool should be provided if the primary server pool is unavailable.

11.6. Availability of a geographic database of IP addresses.

11.7. The mechanism of management by regional polily should be supported, with the possibility of building the topology of the internal infrastructure based on traffic routes.

11.8. A mechanism for finding single points of failure should be supported to redirect traffic from more loaded DC/servers to less loaded ones.

11.9. The following set of records must suport: A, AAAA, CNAME, MX, NAPTR, SRV.

11.10. Binding of a session to a balancing object using: TTL, CIDR (IPv4 and IPv6) must be supported.

11.11. The session binding state must be synchronized between GSLB devices.

11.12. In case of unavailability of the main balancing rule, there must be a mechanism for selecting a backup.

11.13. Security

11.13.1. A DNSSEC security mechanism must be provided.

11.13.2. A DNS over TLS security mechanism must be provided.

11.13.3. The DNS Offload functionality must be supported.

11.13.4. A mechanism for signing DNS records must be provided.

11.13.5. Automatic updating of rules of reputation databases and cleaning of duplicate rules should be ensured.

11.13.6. Verification of DNS requests against RFC standards should be ensured.

11.13.7. Filtering of damaged packets, as well as UDP, DNS query and NXDOMAIN flood attacks should be ensured.

11.13.8. The solution must be able to extend the license to a full proxy DNS firewall (requires an additional license)

11.14. Monitoring

11.14.1. A mechanism for checking the availability of DNS zones during the configuration process should be provided.

11.14.2. A mechanism for importing DNS zones from a file or third-party DNS servers must be provided.

11.14.3. A mechanism for graphing application availability and performance using various metrics (source address, sender address, performance, etc.) should be provided.

11.14.4. A mechanism for creating groups for monitoring should be provided.

11.14.5. Both local and remote DNS query logging should be provided.

11.14.6. The solution must support high speed logging

11.14.7. The solution should support the following types of DNS query logging:

- the pool selected to answer the DNS query and the reason the pool was selected.
- the pool member selected to answer the DNS query and the reason why this member was selected.

მოთხოვნები ქსელის კომუტატორების მიმართ:

A ტიპის კომუტატორი - არანაკლებ 4 ცალი

- 48 x 1/10/25-Gbps fiber ports and 6 x 40/100-Gbps QSFP28 ports

- CPU 6 cores
- System memory Up to 32 GB
- SSD drive 128 GB
- System buffer 40 MB
- Management ports 1 RJ-45 port
- USB ports 1
- RS-232 serial ports 1
- Power supplies (up to 2) 500W AC
- Maximum number of IPv4 Longest Prefix Match (LPM) routes 1,792,000
- Maximum number of IPv4 host entries 1,792,000
- Maximum number of IPv6 Longest Prefix Match (LPM) routes 896,000
- Maximum number of IPv6 host entries 1,792,000
- Maximum number of MAC address entries 512,000
- Maximum number of multicast routes 128,000
- Number of Internet Group Management Protocol (IGMP) snooping groups
  Shipping: 8,000
- Maximum: 32,000
- Maximum number of Cisco Nexus 2000 Series Fabric Extenders per switch 16
- Maximum number of Access Control List (ACL) entries
- Single-slice forwarding engine:
  5000 ingress
  2000 egress
- Maximum number of VLANs
  4096
- Number of Virtual Routing and Forwarding (VRF) instances
  Shipping: 1,000
- Maximum: 16,000
- Maximum number of ECMP paths 64
- Maximum number of port channels 512
- Maximum number of links in a port channel 32
- Number of active SPAN sessions 4
- Maximum number of VLAN's in Rapid per-VLAN Spanning Tree (RPVST) instances 3,967
- Maximum number of Hot-Standby Router Protocol (HSRP) groups 490
- Number of Network Address Translation (NAT) entries 1,023
- Maximum number of Multiple Spanning Tree (MST) instances 64
- Number of Queues 8

B ტი პ ი ს კ ომ უტა ტორი - ა რა ნ ა კ ლ უ ბ 4 ც ა ლ ი

24 fixed SFP+ ports (1 or 10 Gbps); expandable to 48 ports

- Dual redundant hot-swappable power supplies
- Four individual redundant hot-swappable fans
- One 1-PPS timing port, with the RF1.0/2.3 QuickConnect connector type
- One 10/100/1000-Mbps management port
- One RS-232 serial console port
- Two USB ports
- 480-Gbps switching capacity
- Forwarding rate of 360 mpps
- Line-rate traffic throughput (both Layer 2 and 3) on all ports
- Configurable MTUs of up to 9216 bytes (jumbo frames)
  - Number of MAC addresses 64,000
  - Number of IPv4 unicast routes 24,000
  - Number of IPv4 hosts 64,000

- Number of IPv4 multicast routes 8000
- Number of VLANS 4096
- Number of ACL entries 4096
- Number of spanning-tree instances
  Rapid Spanning Tree Protocol (RSTP): 512
  Multiple Spanning Tree (MST) Protocol: 64
- Number of EtherChannels 24
- Number of ports per EtherChannel 24
- Buffer size 6 MB shared among 16 ports; 18 MB total
- System memory 16 GB
- Boot flash memory 16 GB
- Number of power supplies 2 (redundant)

Thin Client - ე ბ ი - 500 ც ა ლ ი

Processor	Intel® Celeron (2.0 GHz base frequency, up to 2.6 GHz burst frequency, 1.5 MB L2 cache, 4 cores, 4 threads)
Graphics	Integrated, [Intel® UHD Graphics]
Memory	8 GB DDR4-3200 MHz RAM (1 x 8 GB)
Memory Slots	1 SODIMM
Internal Storage	64 GB eMMC
Software included	Device Manager; Easy Shell; Easy Tools; Smart Zero Client Services; Thin Update; True Graphics; Microsoft SCCM/EDM Agent
Protocols	Citrix® HDX; Citrix® ICA; VMware Horizon® View™ through RDP/PCoIP, and Blast Extreme; Remote Desktop Services Remote FX (RFX), RDP
Browser supported	Mozilla Firefox, Microsoft Edge
Keyboard	USB 320K wired keyboard
Audio	Wired 320M Mouse
Ports	Front 1 SuperSpeed USB Type-A 5Gbps signaling rate; 1 3.5 mm headphone/microphone combo; 2 SuperSpeed USB Type-A 5Gbps signaling rate Back 1 RJ-45; 1 AC power; 2 USB 2.0 Type-A; 2 SuperSpeed USB Type-A 10Gbps signaling rate; 2 DisplayPort™ 1.4
Power	Smart 45 W External AC power adapter
გ ა რ ა ნ ტ ი ა	ა რ ა ნ ა კ ლ ე ბ 1 წ ე ლ ი

ზ ო გ ა დ ი მ ო თ ხ ო ვ ნ ე ბ ი :

- A და B ტიპის სერვერები უნდა იყოს ერთი და იგივე მწარმოებლის.
- A და B ტიპის კომპიუტერები უნდა იყოს ერთი და იგივე მწარმოებლის.
- ყველა მოხსენიებულ პარამეტრზე მომწოდებელმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form).
- მომწოდებელს უნდა გააჩნდეს ISO 27001:2013 და ISO 9001 - ის აქტიური სერთიფიკატები.
- მომწოდებელმა უნდა უზრუნველყოს აპარატის ფიზიკური დეფექტისგან საჭიროყველი პასიური კომპონენტის (რეკი,ოპტიკური გამსხივებელი, სპილენძის პაჩკორდი, ოპტიკური პაჩკორდი) მოწოდება.

ს ა ი ნ ტ ე გ რ ა ც ი ო ს ა მ უ შ ა ო ე ბ ი :

• Full VSAN and VDI deployment.
• Configure datastores.

• Existing service migration.
• vGPU configuration for vdi pools.
• Application server deployment
• Join active directory groups and users
• Configure user deaktop managment system
• Configure and deployment printers and usb redirections.
• Configure sandblast protocol for horizon client.
• Integrate vdi connection servers to load balancer